European Commission

Joint Research Centre

Digital sovereignty metrics

A multi-layer approach

Thabit Gonzalez, S., Isaraj, L., Kotsev A., Friis-Christensen, A., Passero, A., Minghini, M., Fabiani, J., Signorelli, S., Cerulli, G., Elmallakh, N., Walczak, N., Pagano, A, Di Girolamo, F., Cosgrove, J., López Cobo, M., Di Marco, D.

2026

This document is a publication by the Joint Research Centre (JRC), the European Commission's science and knowledge service. It aims to provide evidence-based scientific support to the European policymaking process. The contents of this publication do not necessarily reflect the position or opinion of the European Commission. Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use that might be made of this publication. For information on the methodology and quality underlying the data used in this publication for which the source is neither Eurostat nor other Commission services, users should contact the referenced source. The designations employed and the presentation of material on the maps do not imply the expression of any opinion whatsoever on the part of the European Union concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

Contact information
Name: Sara Thabit Gonzalez
Address: Joint Research Centre, Via Enrico Fermi 2749, TP 261, 21027 Ispra (VA), Italy
Email: sara.thabit-gonzalez@ec.europa.eu

Joint Research Centre
https://joint-research-centre.ec.europa.eu

JRC148221
EUR 40898

Print	ISBN 978-92-68-44594-5	ISSN 1018-5593	doi:10.2760/5753565	KJ-01-26-476-EN-C
PDF	ISBN 978-92-68-44593-8	ISSN 1831-9424	doi:10.2760/7132257	KJ-01-26-476-EN-N

Luxembourg: Publications Office of the European Union, 2026

© European Union, 2026

Some content was created using GPT@JRC.



The reuse policy of the European Commission documents is implemented by the Commission Decision 2011/833/EU of 12 December 2011 on the reuse of Commission documents (OJ L 330, 14.12.2011, p. 39). Unless otherwise noted, the reuse of this document is authorised under the Creative Commons Attribution 4.0 International (CC BY 4.0) licence (https://creativecommons.org/licenses/by/4.0/). This means that reuse is allowed provided appropriate credit is given and any changes are indicated.

For any use or reproduction of photos or other material that is not owned by the European Union permission must be sought directly from the copyright holders.

How to cite this report: Thabit Gonzalez, S., Isaraj, L., Kotsev, A., Friis-Christensen, A., Passero, A. et al., *Digital sovereignty metrics - A multi-layer approach,* Thabit Gonzalez, S., Isaraj, L., Kotsev, A. and Friis-Christensen, A. (eds.), Publications Office of the European Union, Luxembourg, 2026, https://data.europa.eu/doi/10.2760/7132257, JRC148221.

Contents

Abstract 2

Foreword 3

Acknowledgements 4

Executive summary 5

Introduction A multilayer approach to quantifying Digital Sovereignty 9

Section A **Digital Governance** 14

1. Mapping Science, Innovation and Technology Policies: Protection, Promotion and Projection in the Digital Domain 15

Section B **Digital Infrastructures, Software, and Data** 32

2. Substitutability of the European Digital Offer: A Digital Sovereignty Perspective 33

3. Observing Europe's open source ecosystem: community, activity and cross boarder collaboration 50

4. From research to scale-up: insights from the Cloud computing and Data Technologies domain 70

Section C **Digital Products and Markets** 81

5. Corporate Control in Digital Production Networks: Power and Interconnectedness Position 82

6. Asymmetric dependence in products underpinning digital sovereignty 110

Section D **People** 138

7. Digital sovereignty skills: Emerging perspectives 139

Conclusions and takeaways for policymakers 151

References 157

List of figures 164

List of tables 167

Annexes 169

Abstract

As digital sovereignty becomes increasingly central to the European Union's economic resilience, security, and democracy, this report introduces a holistic empirical framework to measure it across four layers: (i) digital governance, (ii) infrastructures, software and data, (iii) markets, and (iv) people. By providing empirical evidence to overcome the lack of unified metrics, the report supports existing and upcoming EU sovereignty initiatives by revealing critical facts, such as only 20% of European software alternatives offering exit mechanisms, and foreign investors supplying 43% of late-stage scale-up capital in the cloud computing and data technologies domain. It demonstrates that sovereignty is a highly complex, multidimensional phenomenon that extends beyond protectionism, highlighting the importance of an “open but not powerless” approach. In a world of interconnected production markets, the findings evidence the importance of the collective weight of the EU for global leverage, balancing concentrated supply-chain vulnerabilities (EUR 18.6 billion) with potential asymmetric strengths (EUR 72.8 billion) to address dependencies while scaling core competitive advantages. While this report establishes a crucial empirical foundation, significant measurement gaps remain across the digital sovereignty framework, representing a key need for future research.

Foreword



Francesca Campolongo
Director JRC.T Digital Transformation, AI and Data

The ability of our societies and economies to develop and use digital technologies in line with our societal values, legal frameworks and political priorities has emerged as one of the defining challenges of the past decade. In a geopolitical context in which dependencies on products and bottlenecks along value chains are increasingly being exploited, it is essential to identify and operationalise EU policy pathways towards digital sovereignty. This agenda is both urgent and strategically important. It offers a timely opportunity not only to address persistent vulnerabilities, but also to rethink how Europe can strengthen its capacity to shape the digital transformation on our own terms.

Yet such policy pathways can only be credible if they are grounded in solid scientific evidence. In this regard, qualitative evidence has an important role to play, but quantitative indicators are indispensable in enabling policymakers, industry and researchers to assess, prioritise and ultimately implement approaches that support a resilient and European-centred digital stack.

While public debate is rich in anecdotal evidence, there is, paradoxically, still only limited quantitative data available on digital sovereignty. Against this context, I am proud that the work of our Joint Research Centre helps to fill this gap through a set of carefully selected and curated digital sovereignty metrics. With its multidisciplinary expertise, world-class research infrastructures, and ready access to data and methods, our institution is well equipped to carry out such a complex task. The work presented here spans a broad range of interconnected dimensions, from trade dependencies, skills and innovation policies to open source technologies. This report forms an integral part of a broader package, which also includes a data bundle made available for reuse through our JRC Open Data Catalogue, and an interactive dashboard, available in our Knowledge for Policy platform, enabling users to explore the richness of the underlying evidence in greater depth.

In closing, I am confident that this work will provide valuable insights for policymakers, researchers and other stakeholders, contributing to a stronger understanding of Europe's digital position and economic security.

Francesca Campolongo

Acknowledgements

The authors express their sincere gratitude to the following JRC colleagues for their advice, review and an early reading of the report: Margherita Di Leo, Edoardo Ramalli, George Breyiannis, Andrea Ciani, Alice Bertoletti, Daniel Villar Onrubia, Luca Tangi, Francesca Campolongo, Ana Boskovic, Matthew King, Per Loekkemyhr, Michele Vespe, and Olivier Eulaerts, as well as to colleagues from Directorates General CNECT, TRADE, COMP, and DIGIT.

We also wish to thank Raffaella Manfredi who designed the cover page of the report, and Carmen Capote de la Calle (ABDE Business Consulting) for the graphic layout in Chapter 4.

The views expressed are purely those of the authors and may not in any circumstances be regarded as stating an official position of the European Commission. All errors remain the sole responsibility of the authors.

Editors

Sara Thabit Gonzalez, Loreta Isaraj, Alexander Kotsev, Anders Friis-Christensen

Authors per chapter

— *Mapping Science, Innovation and Technology Policies: Protection, Promotion and Projection in the Digital Domain*

Loreta Isaraj, Alexander Kotsev, Anders Friis-Christensen

— *Substitutability of the European Digital Offer: A Digital Sovereignty Perspective*

Loreta Isaraj

— *Observing Europe' open source ecosystem: community, activity and cross boarder collaboration*

Alessia Passero, Marco Minghini

— *From research to scale-up: insights from the Cloud computing and Data Technologies domain*

Josefina Fabiani, Serena Signorelli

— *Corporate Control in Digital Production Networks: Power and Interconnectedness Position*

Loreta Isaraj, Sara Thabit Gonzalez, Giovanni Cerulli

— *Asymmetric dependence in products underpinning digital sovereignty*

Nevine Elmallakh, Noemi Walczak, Andrea Pagano, Francesca Di Girolamo, Loreta Isaraj, Alexander Kotsev

— *Digital sovereignty skills: Emerging perspectives*

Judith Cosgrove, Monserrat Lopez Cóbo, Diletta Di Marco

Executive summary

Policy context

In an era of geopolitical tension and rapid technological acceleration, digital sovereignty is a crucial element of the European Union's economic resilience, security, and democratic agency. Currently, the EU relies on foreign sources for over 80% of its digital products, services, infrastructure and intellectual property (Draghi, 2025), marking the need to lowering its exposure in terms of strategic dependencies, and strengthening the EU's capacity to develop, control and scale critical digital technologies. This report supports current policy instruments—such as the "Tech Sovereignty package" (2026), including the Chips Act 2.0, the Cloud and AI Development Act (CADA), and the EU Open Source Strategy—as well as potential future policy interventions aiming towards reducing dependencies and seeking opportunities in the digital sovereignty realm. Produced by the Joint Research Centre (JRC) to assist policymakers, it addresses the persistent lack of unified, scientifically-sound empirical measurement for tracking various digital sovereignty aspects. By moving beyond abstract debates to actionable data, this work is essential for informing upcoming political decisions on balancing global integration with internal resilience.

Key conclusions

- **Digital sovereignty necessitates multidimensional metrics:** Achieving sovereignty in the digital domain requires a holistic approach spanning four interconnected layers: (i) Digital Governance, (ii) Infrastructures, Software and data, (iii) Markets, and (iv) People. Combining metrics across these layers provides critical analytical value by distinguishing policy intentions from strategic outcomes. For example, governance indicators reveal which strategic technologies policymakers prioritise, while production, trade, and substitutability metrics assess whether these priorities correspond to actual observed capabilities or vulnerabilities.
- **Sovereignty extends beyond protectionism**: EU Digital sovereignty should not be treated merely as a question of technological protectionism; it also necessitates strong domestic capacity-building and strategic international projection. The importance of this "*open but not powerless*" approach is evidenced in global corporate production; where leading global actors combine domestic production autonomy with deep international interconnectedness. Digital governance policies reinforce this paradigm by demonstrating that protective measures must be paired with the capacity to innovate and collaborate internationally.
- **Availability does not guarantee substitutability:** Providing European digital alternatives is insufficient if users remain locked into incumbent systems. Policy options should consider exit mechanisms, interoperability, and data portability remedies.
- **Leveraging the collective weight of the EU:** The integration and scale of the EU single market are essential for achieving global leverage. In corporate production networks, individual Member States often have limited standalone power, but their collective weight elevates the bloc among the top world economies in terms of power and interconnectedness. The importance of a unified scale is equally evident in open source ecosystems; while the global network remains US-centric, considering the EU as a single entity reveals it as the second major pole of international open source collaboration in the world.

— **Closing the gap from research excellence to commercial scale-up:** While the EU maintains a strong scientific research base, it struggles to translate this into technological service. A critical problem identified in the cloud computing and data technologies domain is the severe scale-up funding gap; as European digital firms grow, their reliance on foreign (primarily US) capital surges. This highlights the importance of strengthening European scale-up financing to reduce potential dependencies affecting the development and control of strategic technological assets.

— **Identify and manage asymmetric dependencies while leveraging EU indispensability:** The EU is potentially vulnerable to at least one third-country supplier across 31 products, accounting for EUR 18.6 billion in EU imports, which may require targeted supply-chain resilience and diversification strategies. However, the EU also holds significant asymmetric strengths across a much broader and more diversified base of 125 core and broad products exported to 188 partners, accounting for EUR 72.8 billion. European trade and industrial strategy would benefit from combining actions to address EU's strategic exposure with protecting and scaling the EU's core competitive advantages (i.e., EU indispensability) as strategic leverage in international partnerships.

— **A foundation for continuous monitoring:** The proposed metrics are not intended to provide a definitive or exhaustive assessment of European digital sovereignty. Instead, they establish an empirical foundation that can progressively evolve as new data sources, methodologies, and technologies become available. This appears as a central question as significant measurement gaps remain across all the digital sovereignty framework; an aspect particularly relevant in the People layer, where people's competences for digital sovereignty remain undefined in official monitoring systems, despite being a fundamental aspect of digital sovereignty. Yet, this report represents a critical step towards a dynamic and replicable monitoring framework, capable of tracking shifts over time and identifying both emerging dependencies and areas of strategic strength.

Main findings

This report provides empirical findings across four foundational layers of digital sovereignty: (i) Digital Governance, (ii) Infrastructures, Software and data, (iii) Markets, and (iv) People. Within the **Digital Governance** layer, the study analyses policies across three distinct orientations: protection, domestic promotion (building research and business capabilities), and international projection. While protective measures to reduce dependency vulnerabilities are the most prevalent, national approaches remain highly heterogeneous. Some countries prioritise business promotion, others focus on research capacity, and some strongly emphasise protection, demonstrating that digital sovereignty requires a multidimensional policy mix rather than a universal template.

Regarding **Digital Infrastructures, Software, and Data**, the analysis of European alternatives suggests that the availability of alternative solutions does not guarantee technical independence. Among 1,593 European solutions analysed, only 20% explicitly report at least one exit mechanism, such as interoperability, deployment autonomy, or portability. While deployment autonomy is the most common feature, data portability remains rare. Furthermore, the analysis of the European open source ecosystem indicates strong developer-driven hubs in countries such as Germany, France, the Netherlands, and Estonia, despite the global network remains mostly US-centric. This structural challenge also extends to the analysis of investment flows within cloud computing and data technologies. While EU start-ups receive roughly two-thirds of their early-stage funding from domestic investors, this domestic share drops sharply to just one-third during the scale-up phase.

US investors currently supply 43% of the funding for European scale-ups in this domain, highlighting a severe dependency in late-stage capital.

In the **Digital Products and Markets** layer, structural challenges are evident in supply chains and global corporate networks. Crucially, assessing this layer requires both looking at traditional trade flows and examining who actually owns and controls the production within each country. In trade, the EU faces highly concentrated asymmetric vulnerabilities in 31 products underpinning digital sovereignty, valued at EUR 18.6 billion in 2024. These vulnerabilities are primarily found in essential and core products sourced from Taiwan, China, and Malaysia. Conversely, the EU maintains widespread strengths across 125 core and broad digital products, valued at EUR 72.8 billion, where foreign partners depend asymmetrically on European supply. Conducted across the nine layers of the digital stack, the trade analysis reveals that EU vulnerabilities are heavily concentrated in the foundational lower layers, such as hardware and components. In contrast, European asymmetric strengths are widely distributed across the upper layers, particularly in specialised equipment and broader industrial digital products. Furthermore, distinguishing where production takes place from who controls it in global corporate networks reveals that individual Member States often have limited standalone power; however, leveraging the collective weight of the EU single market elevates the bloc to a highly interconnected global influencer.

Finally, underpinning the **People** layer, the report illustrates that digital sovereignty extends beyond basic digital literacy. It requires the capacity to understand technological dependencies, exercise agency over personal data, and make informed strategic choices. These necessary competences are highly role-specific, differing significantly among the general population, non-technology decision-makers, and technology decision-makers. However, a severe measurement gap currently limits the assessment of these capabilities and consequently what capability gaps may exist.

Related and future Joint Research Centre work

Led and coordinated by the JRC *Digital and Data Sovereignty* (T4) Unit, this report results from a fruitful collaboration among two JRC directorates (JRC.B “Fair and Sustainable Economy” and JRC.T “Digital Transformation and Data”) spanning across three units and five teams, whose ongoing research activities are directly relevant to digital sovereignty. Future work can further develop some of the research activities initiated in each of the chapters as new data sources, methodologies, and technologies become available to inform upcoming policy initiatives.

Quick guide

This report constitutes an integral part of the broader **“Digital Sovereignty Metrics Package”** composed by an openly accessible dataset collection (Thabit Gonzalez et al., 2026, Data Collection: id-00468) and a series of online interactive dashboards[1]. The report introduces a multi-layer framework to measure European digital sovereignty—the EU’s capacity to remain independent yet globally connected in the digital domain. To overcome the lack of unified empirical metrics, the study applies a targeted deep-dive methodology across four interconnected layers: Digital Governance, Infrastructures, Markets, and People. Key concepts explored include "substitutability" (the technical ability to switch digital providers) and "asymmetric dependence" (vulnerabilities within

[1] https://knowledge-for-policy.ec.europa.eu/visualisation/digital-sovereignty-metrics-dashboard_en

global supply chains). Proceeding from the assumption that true sovereignty requires balancing domestic capacity with international projection, the approach leverages diverse data, including trade statistics, policy databases, and software platforms. However, significant uncertainties remain due to the reliance on self-reported product descriptions, platform-specific proxies (such as GitHub), and the inherent complexity of aggregating such diverse dimensions.

Introduction
A multilayer approach to quantifying Digital Sovereignty

Context and Purpose of this Report

In an increasingly fragmented geopolitical landscape defined by technological acceleration and intensifying strategic rivalry, digital sovereignty has become a direct element of economic resilience, security, and democratic agency. For the European Union, the current landscape of structural dependency—of over 80% of its digital products, services, infrastructure and intellectual property (Draghi, 2025)—marks the need to lowering its exposure in terms of strategic dependencies, and staying ahead in the development control, and scaling of critical technologies.

In this context, **EU digital sovereignty should not be understood as digital isolation or technological protectionism.** Rather, it is defined as "the EU capacity to exercise its independence in the digital domain while remaining open and connected to global networks" (Di Marco et al., 2025). It focuses on the ability to decide, invest, and innovate according to European values of democracy, openness, and the rule of law, by strengthening EU skills, infrastructures, and governance to ensure that digital transformation supports competitiveness, resilience, and trust.

Over recent years, the Union has advanced several policy initiatives to assert this vision, including the "Tech Sovereignty package" adopted in June 2026, introducing the Chips Act 2.0, the Cloud and AI Development Act (CADA), the EU Open Source Strategy, and the Strategic Roadmap for Digitalisation and AI in the energy sector. It builds on existing EU initiatives—such as the Digital Decade 2030, the AI Act (European Union, 2023), and the Cyber Resilience Act (European Union, 2024), among others—that together form the policy and regulatory foundations of a coherent framework for asserting technological sovereignty in the EU.

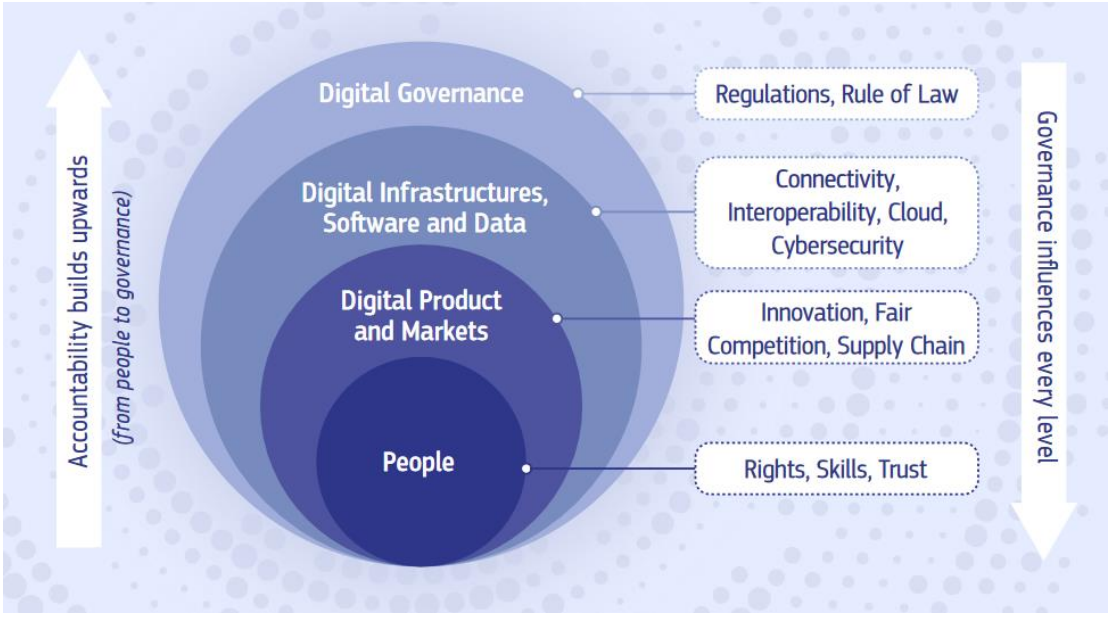
As the principle commonly attributed to Lord Kelvin states: "*If you can't measure it, you can't improve it*" (Thomson, 1883). This captures the core motivation behind this work: translating a complex, multidimensional policy concept such as digital sovereignty into empirical evidence that can inform policy decisions, identify vulnerabilities and opportunities, and monitor progress over time. However, translating these high-level policy ambitions into effective operational interventions reveals a persistent structural challenge: the **absence of unified, empirical measurement frameworks**. In the context of digital sovereignty, the lack of comparable data and reliable monitoring tools is even more prominent than in other traditional economic areas. This disparity stems from the very nature of digital services which makes them exceptionally difficult to track in terms of actual economic footprint and strategic dependency. Furthermore, this measurement challenge is exacerbated by the scope of digital sovereignty itself, which spans across different levels and scales.

Led and coordinated by the JRC *Digital and Data Sovereignty* (T4) Unit, this report aims to address this gap by bringing together two JRC directorates (JRC.B "Fair and Sustainable Economy" and JRC.T "Digital Transformation and Data"), three units, and five teams, whose ongoing research activities are directly relevant to digital sovereignty. Designed to ground strategic decision-making in reliable, actionable data, it constitutes an integral part of the broader **"Digital Sovereignty Metrics Package"** composed by an openly accessible dataset collection (Thabit Gonzalez et al., 2026, Data Collection: id-00468) and a series of online interactive dashboards[2].

Approach

This study is grounded in two primary methodological considerations designed to capture the full complexity of digital sovereignty. First, it adopts the JRC holistic approach that conceptualizes **digital sovereignty across four interconnected layers**: 1) Digital Governance; 2) Digital Infrastructures, Software, and Data; 3) Digital Products and Markets; and 4) People (see **Figure 1**). This multi-layered framework explicitly recognizes that digital sovereignty cannot be reduced to technological capacity or market dynamics alone, but also of legitimacy and democratic accountability (Di Marco et al., 2025). Combining indicators across these different layers provides crucial additional analytical value. While individual metrics are highly useful, their complementarity helps distinguish between policy intentions, observed capabilities, and strategic outcomes. For example, governance indicators can tell us which strategic technologies policymakers are prioritising, while production, trade, and substitutability indicators assess whether these priorities correspond to actual capabilities or vulnerabilities.

Figure 1. The Digital Sovereignty Framework: four layers shaping EU independence in the digital domain (Di Marco et al., 2025)



Source: Di Marco et al. (2025)

[2] https://knowledge-for-policy.ec.europa.eu/visualisation/digital-sovereignty-metrics-dashboard_en

Second, the analysis is grounded on a dual strategic approach to monitoring digital sovereignty. Rather than focusing solely on a reactive, mitigation-based assessment of strategic vulnerabilities and critical dependencies, it also addresses a proactive evaluation of potential areas of opportunity. Identifying domains where the EU can achieve technological leadership and become broadly indispensable to other global actors is essential. This dual lens is critical for **understanding and strengthening the EU's role as a key connector in the global digital ecosystem**—a technological node that other countries rely upon. By balancing the tracking of external dependencies with the measurement of outbound indispensability, this report aims to guide policies that keep the EU globally integrated, yet protected and strong enough to ensure internal resilience against potential geopolitical or supply chain shocks.

Building on these considerations, **the different chapters of this report present the results of independent, complementary studies addressing specific, highly relevant topics across the four interconnected layers**. This approach was chosen because constructing a single, all-encompassing digital sovereignty index encounters significant practical constraints. The persistent lack of access to granular, proprietary data and the inherent methodological complexity of aggregating such fundamentally diverse dimensions mean that developing a monolithic composite score would require considerable time. By offering these targeted deep-dives instead, the report responds directly to the urgent need policymakers face for actionable insights today, collectively building a nuanced and practical measurement foundation.

Furthermore, recent advances in Artificial Intelligence, particularly large language models and multimodal models, are creating new opportunities to measure dimensions of digital sovereignty that have traditionally been difficult to capture with conventional statistics. An increasing amount of relevant information is available in unstructured formats, including policy documents, technical descriptions, online repositories, corporate disclosures, and potentially visual materials such as images or diagrams. These sources can complement structured statistical data to provide a more comprehensive picture of digital capabilities, dependencies, and strategic positioning. Importantly, this is not merely a future opportunity: some of the analyses presented in this report already demonstrate the value of AI-assisted processing of textual information, expanding the boundaries of what and how we measure.

Ultimately, the proposed metrics are not intended to provide a definitive or exhaustive assessment of European digital sovereignty. Instead, they establish an empirical foundation that can progressively evolve as new data sources, methodologies, and technologies become available, serving as a critical step towards a dynamic and replicable monitoring framework capable of tracking changes over time and identifying emerging dependencies and strengths.

Contents of the report

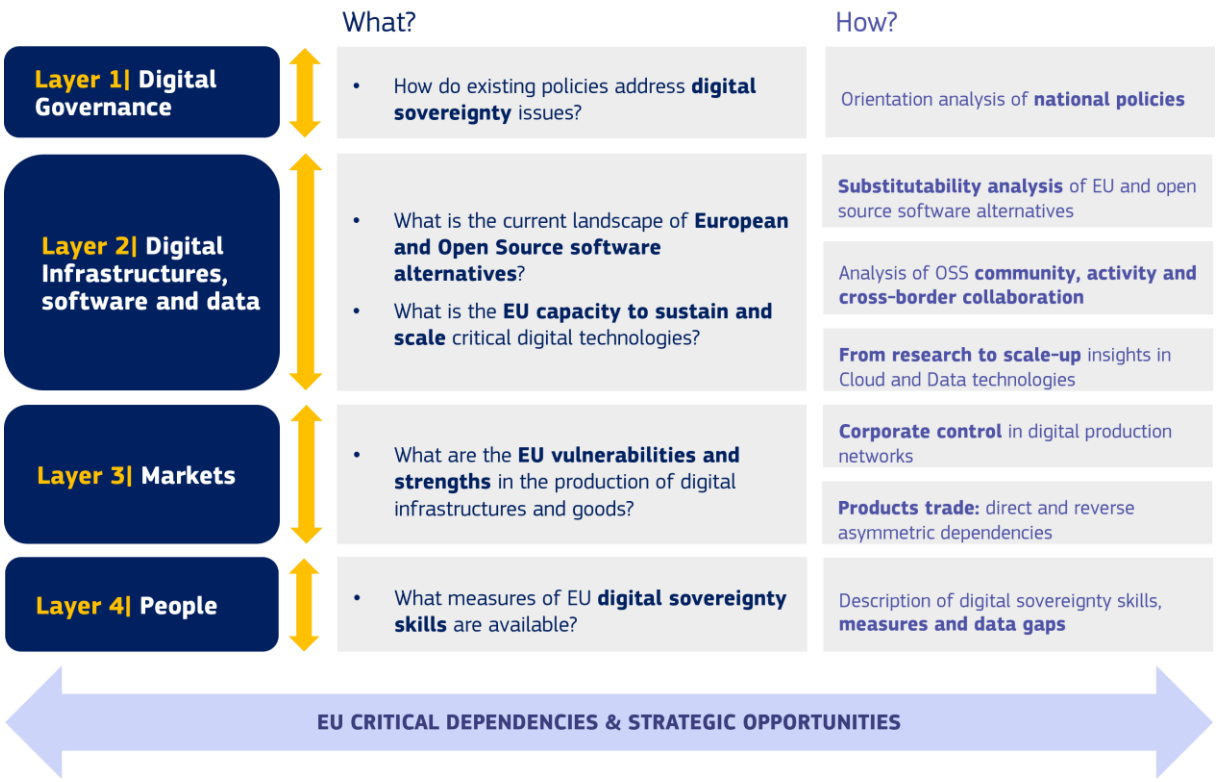
The report is structured around seven main chapters tackling different aspects of each of the four layers of the digital sovereignty framework (see **Figure 2**) followed by a general conclusions chapter and main takeaways for policymakers. The seven chapters do not provide a comprehensive analysis of each of the four digital sovereignty layers. Rather, they address specific issues that are highly relevant to the topic of analysis, considering both data limitations and replicability potential for future monitoring and comparative future analysis.

Addressing the Digital Governance layer, **Chapter 1** examines how digital sovereignty considerations are reflected in public science, technology, and innovation (STI) policies. The approach relies on a textual analysis and mapping of national policies using the EC-OECD STIP

policy database for the 2014–2025 period, applying an adapted Protection, Promotion, and Projection framework alongside large language model-based classifications.

Focusing on Digital Infrastructures, Software, and Data, **Chapter 2** investigates the technical substitutability of European digital alternatives. The methodology evaluates 1,593 solutions from the EuroStack Directory to measure reported technical exit mechanisms, including Interface compatibility, Deployment autonomy, and Portability. Following this, **Chapter 3** explores the Capacity, Activity intensity, and Interconnectedness of the open source software developer ecosystem. The analysis uses country-level GitHub Innovation Graph data for 2025, applying clustering and network analysis to assess cross-border collaboration flows. Additionally, **Chapter 4** traces the transition from research to scale-up in strategic domains, such as cloud computing and data technologies. The approach uses the JRC Digital Techno-Economic ecoSystem framework to track scientific publications, patents, and venture capital flows through micro-level databases like Scopus, Patstat, and Crunchbase.

Figure 2. Multidimensional analysis across four layers of digital sovereignty



Source: JRC

Within the Digital Products and Markets layer, **Chapter 5** assesses the power and interconnectedness of multinational enterprises within global production networks. It analyses bilateral gross-output data from the OECD Analytical AMNE database across key digital sectors for the 2000–2023 period to map corporate production power and structural network positions. **Chapter 6** conducts a product-level trade analysis to identify bidirectional asymmetric dependencies in global supply chains, combining information on production and international trade statistics to assess external exposure and bilateral trade relationships.

Finally, addressing the People layer, **Chapter 7** examines the role-specific competences required by individuals, non-technology decision-makers, and technology decision-makers to navigate, govern, and shape digital environments. The methodological approach involves desk-based research, conceptual mapping grounded in the JRC four-layer model, and an assessment of the viability of existing cross-national indicators to measure these digital sovereignty capabilities.

Section A

Digital Governance



1. Mapping Science, Innovation and Technology Policies: Protection, Promotion and Projection in the Digital Domain

1.1. Approach, methodology and data limitations

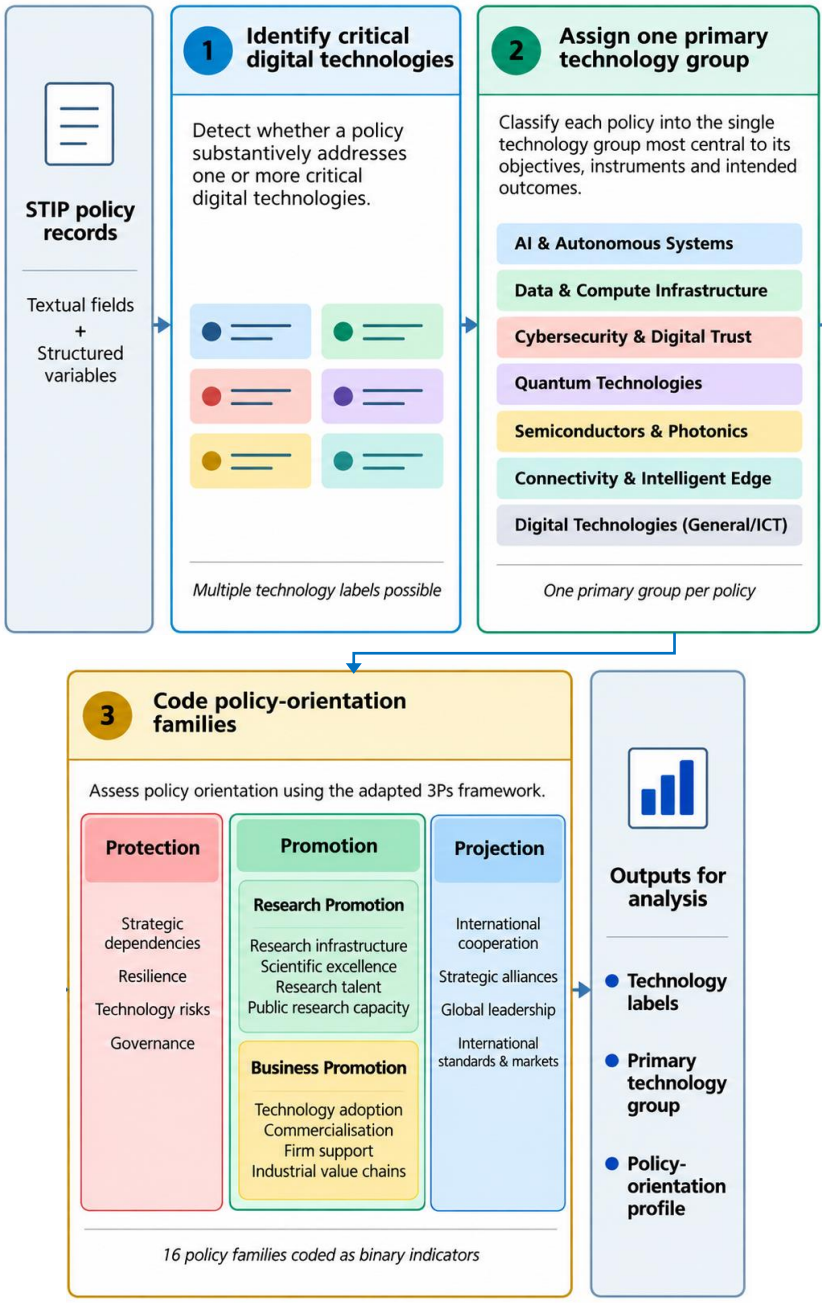
1.1.1. Analytical purpose and context

This analysis builds on the governance layer of the *Digital Sovereignty Metrics framework* (see **Introduction**). In the report, digital sovereignty is understood as the capacity to exercise independence in the digital domain while remaining open and connected to global networks (Di Marco et al., 2025). In recent years, technological sovereignty has become an increasingly prominent concern in innovation policy debates, reflecting intensified technology-based competition, geopolitical tensions and strategic dependencies (Edler et al., 2023; Timmers, 2024). Technological sovereignty concerns the capacity to develop or secure reliable access to technologies considered critical for economic competitiveness, societal welfare and the ability to act, while avoiding one-sided structural dependencies (Edler et al., 2023). From this perspective, innovation policy is not only a means of supporting technological advancement and economic growth, but also an instrument for strengthening strategic capabilities, addressing dependencies and preserving room for autonomous action. This understanding is consistent with a broad conception of innovation policy encompassing public interventions that influence innovation processes and outcomes (Edler and Fagerberg, 2017).

Against this background, this chapter examines how considerations related to digital sovereignty are reflected in public science, technology and innovation (STI) policies. Drawing on the EC–OECD STIP policy database (EC–OECD, 2026), it develops a policy-level mapping of strategic digital technologies and policy orientations, complemented by an assessment of the scope and intensity of policy instruments. The resulting analytical dataset is available through the JRC Open Data Catalogue (Isaraj, 2026a).

As illustrated in **Figure 3**, the classification procedure comprises three steps. *First*, policy initiatives are screened to identify whether they substantively address one or more critical digital technologies and label them accordingly. Multiple technology labels may be assigned to the same policy. *Second*, each identified initiative is assigned to one primary technology group, reflecting the technology that is most central to its objectives, instruments, and intended outcomes. *Third,* policy objectives are classified using an adapted Protection, Promotion and Projection (3Ps) framework (OECD, 2023). This framework is operationalized through 16 policy families organized under Protection, Projection, Research Promotion, and Business Promotion. Each family is coded as a binary indicator, and a policy may address multiple families. The resulting classifications provide the basis for the subsequent analysis of national policy portfolios, including the scope- and intensity-weighted comparisons presented later in the chapter. Together, these dimensions provide a structured view of how national STI policy portfolios are oriented towards strengthening digital sovereignty.

Figure 3. Workflow for classifying STIP policies



Source: JRC

The classification combines textual and structured information contained in the policy records and is implemented using GPT@EC[3], accessed via API using GPT-5.4. The approach applies a predefined

[3] GPT@EC is a generative AI platform developed by the European Commission's Directorate-General for Digital Services (DG DIGIT), providing Commission staff with access to large language models in a secure environment compliant with institutional data protection and governance requirements. For further information, see European Commission (2024), *Commission launches a new general-purpose AI tool – GPT@EC*, 22 October 2024.

classification prompt, giving greater weight to textual evidence while using structured policy variables to corroborate and contextualize the assessment. The procedure is deliberately conservative: incidental references to technologies or policy objectives are not sufficient for classification. The detailed input fields, classification prompt, definitions and decision rules are reported in **Annex 1.1**.

The first stage identifies 821 policies involving at least one critical digital technology out of a total of 8,820 STI policies recorded over the entire period 1990–2025. For comparative analysis, the detailed technology labels are organised into six strategic groups: *AI & Autonomous Systems; Data & Compute Infrastructure; Cybersecurity & Digital Trust; Quantum Technologies; Semiconductors & Photonics; and Connectivity & Intelligent Edge.* A residual *Digital Technologies (General/ICT)* category captures substantively digital policies for which no single strategic technology group can be identified as the primary focus. These classifications provide the technological basis for the subsequent analysis of policy orientations and instruments.

1.1.2. Policy orientation: adapting the 3Ps to digital sovereignty

A useful way to introduce the 3Ps is to connect them to the recent evolution of the STIP Survey itself. The OECD's Science, Technology and Innovation Outlook 2023 framed policy responses to technological strategic autonomy around three broad types of intervention - **protection, promotion and projection (the "3Ps")** - as illustrated in **Figure 4**. Protection concerns restricting technology flows and reducing dependency vulnerabilities; promotion focuses on strengthening domestic innovation capabilities and performance; and projection refers to extending and deepening international STI linkages, including alliances and participation in international standard-setting (OECD, 2023).

This perspective was subsequently incorporated more explicitly into the 2025 EC–OECD STIP Survey, which introduced a new survey question on "*Strategic autonomy and promotion of critical technologies*" to reflect recent shifts in STI policy agendas (EC-OECD, 2025). In the current STIP Compass taxonomy, this is represented by the theme TH111[4], which captures initiatives aimed at reducing foreign technology dependencies, strengthening domestic capabilities and improving resilience in critical technology sectors. Earlier techno-nationalist approaches emphasized strengthening domestic technological capabilities and protecting strategic industries from external competition, while subsequent debates on digital protectionism highlighted restrictions on cross-border technology and data flows (Chiang, 1990; Aaronson, 2019). The OECD's 3Ps framework offers a broader perspective by explicitly combining Protection with Promotion and Projection (OECD, 2023). Against this background, **the present analysis uses the 3Ps as an analytical framework for distinguishing the different ways in which STI policies can contribute to digital sovereignty, rather than treating sovereignty solely as a question of protection**. A

https://commission.europa.eu/news-and-media/news/commission-launches-new-general-purpose-ai-tool-gptec-2024-10-22_en

[4] See the official EC–OECD STIP Compass thematic dashboard, "Strategic Autonomy and Promotion of Critical Technologies" (TH111): https://stip.oecd.org/stip/interactive-dashboards/themes/TH111.

resilient digital position may require domestic capability-building and international embeddedness alongside risk mitigation (March and Schieferdecker, 2023).

For this chapter, the promotion dimension is further separated into *Research Promotion* and *Business Promotion*. This distinction reflects a well-established feature of STI policy: strengthening technological capabilities requires both the creation of new knowledge and research capacity, and the diffusion, adoption and commercial application of knowledge and technologies across firms and the economy (OECD, 2010; OECD, 2025). *Research Promotion* therefore captures policies directed towards the knowledge-creation side of the innovation system—research infrastructure; scientific excellence and frontier research; research talent and scientific skills; and universities and public research capacity. *Business Promotion* captures policies oriented towards the application and diffusion of technological capabilities—technology adoption and diffusion; commercialisation and scale-up; SMEs, innovation hubs and firm support; and industrial deployment and value chains. The distinction is analytical rather than implying a separation between the two processes: knowledge creation, transfer, adoption and commercialisation are closely interconnected within innovation systems (OECD, 2019).

Figure 4. 3Ps Framework



Source: (OECD, 2023)

The resulting framework comprises four policy orientations—Protection, Projection, Research Promotion and Business Promotion—each operationalised through four more specific policy families, for a total of 16 families: **Protection** encompasses technological sovereignty and autonomy, cybersecurity and secure infrastructure, strategic dependencies and resilience, and trust, risk and technology governance. **Projection** includes international cooperation, strategic partnerships and alliances, global technological leadership, and international standards and markets. Promotion is divided into two dimensions: **Research Promotion**, covering research infrastructure, scientific excellence and frontier research, research talent and scientific skills, and universities and public research capacity; and **Business Promotion**, covering technology adoption and diffusion, commercialisation and scale-up, SMEs, innovation hubs and firm support, and industrial deployment and value chains. These 16 families capture distinct but potentially overlapping policy objectives and mechanisms, with their full definitions and classification criteria provided in **Annex 1.1.**

These orientations are not mutually exclusive at the policy level: a single initiative may, for example, simultaneously support research infrastructure, industrial deployment and international partnerships. The analysis therefore codes each of the 16 families as binary indicators (1 when substantively addressed, 0 otherwise) and subsequently aggregates them into the four broader orientations to examine policy profiles across technologies and countries.

1.1.3. Scope and intensity of policy instruments

To account for the fact that the number of policies alone does not capture differences in the reach and intensity of government intervention, each policy instrument type is therefore assigned researcher-defined scores of *Scope* and *Intensity*. Drawing on the EC-OECD STIP instrument taxonomy and established approaches to policy instruments (Howlett, 2000; Eliadis et al., 2005), scope captures the expected breadth or reach of an instrument, ranging from targeted interventions to system-wide measures whileintensity captures the strength of its intervention mechanism, ranging from information and coordination activities to regulatory and institutional measures and direct resource commitments. Both are measured on three-point scales. The detailed definitions, scoring criteria and instrument-level assignments are provided in **Annex 1.2.**

These scores are analytical constructs and should not be interpreted as measures of policy quality or effectiveness. Instead, they provide alternative weights for assessing whether the composition of digital-sovereignty policy portfolios changes when greater importance is attached to interventions with broader reach or to instruments involving more direct resource commitments, regulatory obligations or institutional measures.. This distinction is particularly relevant because the STIP data contain a heterogeneous mix of strategies, grants, infrastructures, regulatory measures, collaborative platforms, and other instruments. Consequently, the number of recorded initiatives provides information about the presence and composition of policy activity, but not about its financial scale or implementation intensity.

1.1.4. Country analysis and limitations

Given the marked increase in the number of recorded initiatives in recent years (Figure 3), the country-level analysis focuses on the 2014–2025 period, which captures the most recent and policy-relevant phase of activity while providing a sufficiently consistent basis for cross-country comparison. EU-level initiatives are excluded from the national comparison, and only countries with at least ten eligible policies are retained for the positioning charts. This minimum threshold is applied to reduce the sensitivity of country-level policy profiles to individual initiatives and to avoid drawing comparisons from very small numbers of reported policies. The dataset combines the original STIP policy information with the LLM-generated classifications across the 16 policy families. Country cells report weighted means of standardized policy-level family indicators. Positive values indicate that a family is relatively more prevalent than the cross-country average; negative values indicate relative under-representation. They are portfolio orientations, not country performance scores.

Several limitations follow. *First*, STIP is a reporting database: cross-country differences can reflect reporting practices, administrative granularity, and update cycles as well as genuine policy differences (EC-OECD, 2025). *Second*, the policy descriptions vary in detail, affecting text classification. *Third,* start-year analysis does not capture implementation duration or discontinuation consistently. *Fourth*, the scope and intensity weights are based on instrument type rather than observed budgets, enforcement strength, or implementation quality. *Fifth*, standardization makes country values relative to the sample and period; a positive score does not

imply adequacy against an external benchmark. *Sixth*, small national samples remain sensitive to a few broad initiatives even with a ten-policy threshold. *Finally*, the final 2023–2025 cohort is provisional. For these reasons, the analysis is best used to identify patterns and questions for policy review, not to rank countries or infer causal effects.

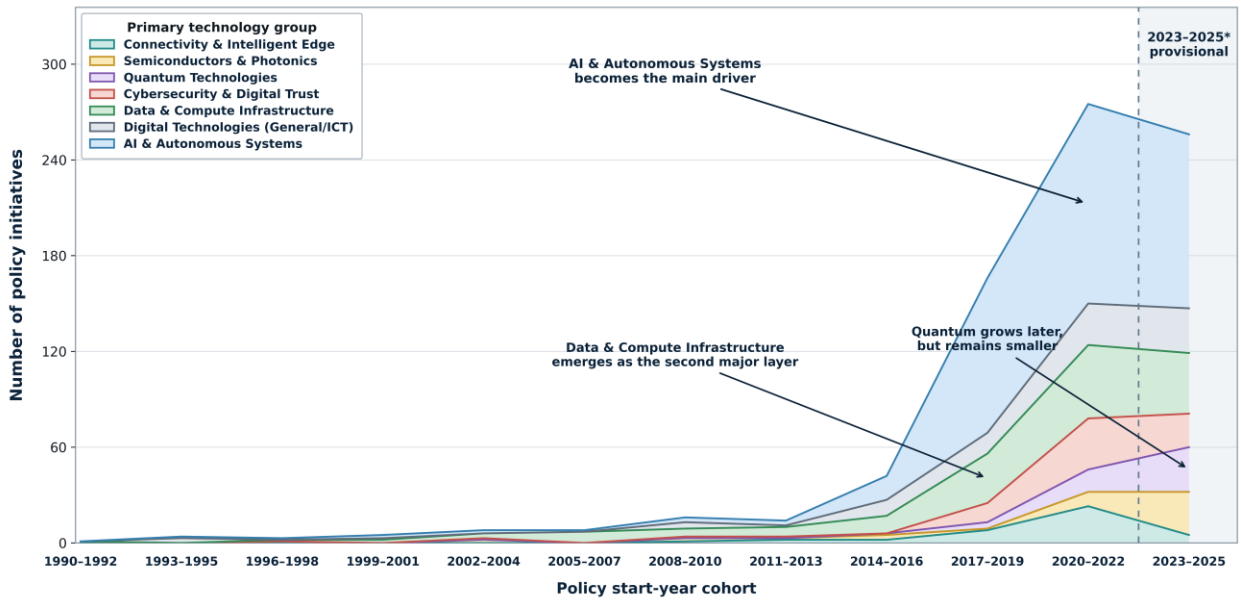
1.2. Results

1.2.1. Evolution of STI policies addressing strategic digital technologies

The clearest temporal signal is the expansion of strategic digital technology policy after the mid-2010s (**Figure 5**). While the number of recorded initiatives remains relatively limited in the earlier cohorts, activity increases substantially from 2017 onwards, particularly during 2017–2022. The growth is not confined to one technology, but AI is the dominant driver. In the full classification, AI & Autonomous Systems is associated with 419 policies, compared with 187 for Data & Compute Infrastructure and 117 for Cybersecurity & Digital Trust. Quantum accounts for 72 policies, while Semiconductors & Photonics and Connectivity & Intelligent Edge each account for 61. These counts are not mutually exclusive at the initial technology-identification stage, because policies may address several technologies; Figure 3 resolves this by assigning one primary technology per initiative.

The time profile should be read as evidence of policy attention, rather than as a direct measure of policy effort, since the number of recorded initiatives does not capture the financial resources committed, the scale of investment or the intensity of policy implementation. The apparent decline in the final cohort should not be interpreted as a reversal: the underlying material explicitly notes incomplete reporting for 2025. More generally, start-year counts are sensitive to how long-running strategies, programme renewals and successor initiatives are recorded in STIP.

Figure 5. Evolution of STI policies for strategic digital technologies by primary technology group



Source: JRC

Notes: Areas show the absolute number of unique initiatives starting in each three-year cohort. Each initiative is assigned to one primary technology group. The 2023–2025 cohort is provisional because 2025 reporting is incomplete.

For policymakers, the important point is not so much the precise ordering but the change in the policy agenda. Strategic digital technologies are increasingly embedded in mainstream STI portfolios. This is consistent with **a shift from a generic "digitalization" agenda towards more explicit strategic positioning around capabilities, dependencies and technological control.** At the same time, the strong concentration of policy attention around AI raises a measurement question for future monitoring: whether governance attention is keeping pace with enabling layers—compute, data, connectivity, cybersecurity and components—on which AI capability itself depends (Edler et al., 2023).

1.2.2. Policy orientations across strategic digital technologies

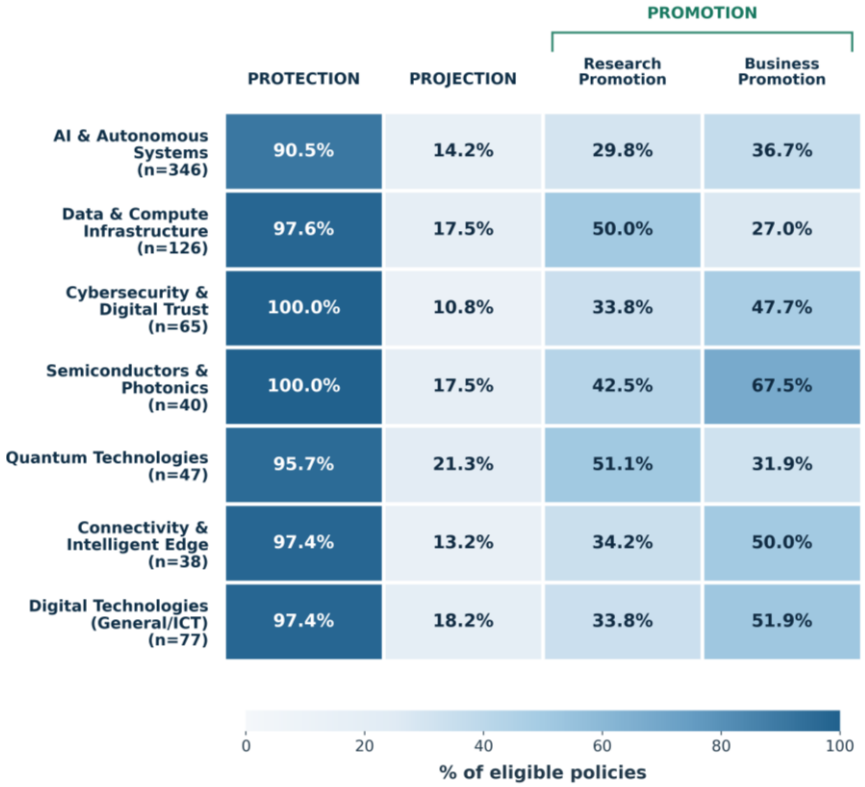
Protection is the most prevalent policy orientation across all digital technology groups, appearing in more than 90% of eligible initiatives in each domain (**Figure 6**). Panel A reports the share of policy initiatives within each technology group addressing each of the four policy orientations. Since multiple orientations can be assigned to the same initiative, percentages do not sum to 100 across orientations. Panel B presents an *Orientation Specialization Index*, calculated as the prevalence of a given orientation within each technology group divided by its prevalence across all eligible digital policy initiatives. A value of 1 indicates prevalence equal to the overall digital policy portfolio; values above or below 1 indicate relative over- or under-representation, respectively.

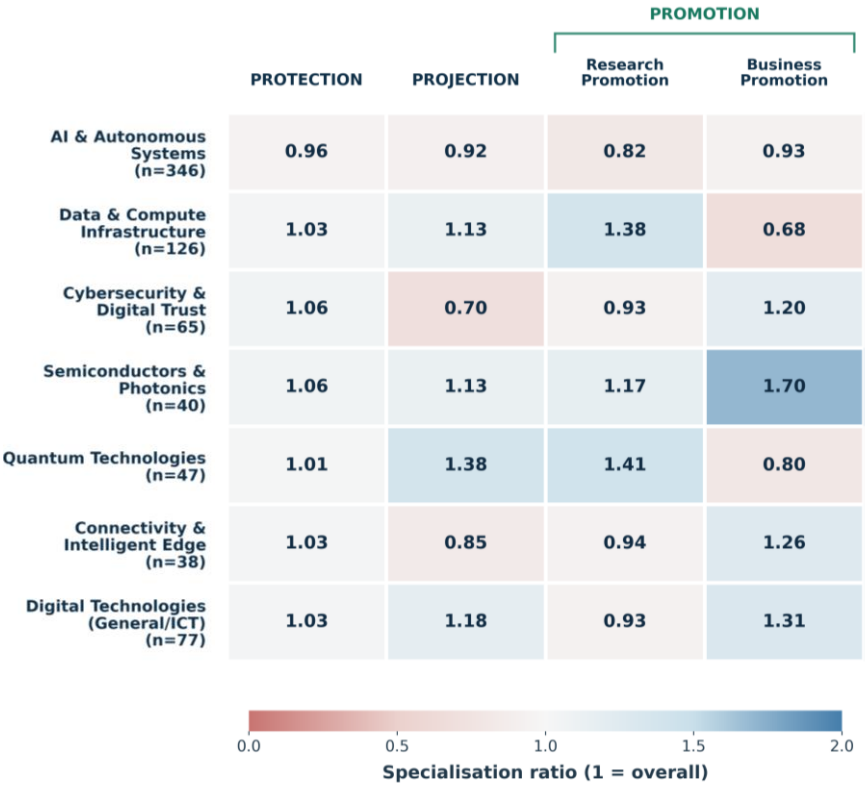
This common emphasis reflects the prominence of technological autonomy, security, resilience and risk governance in digital STI policy portfolios. However, because Protection is widespread across technologies, the *Specialization Index* shows relatively limited differences between groups. The more distinctive patterns emerge in the relative emphasis placed on Promotion and Projection.

Within *Promotion*, the distinction between research and business objectives reveals different technology-specific priorities. ***Semiconductors & Photonics* stands out for Business Promotion**, which is present in 67.5% of its initiatives and is 70% more prevalent than in the overall digital policy portfolio (*Specialization Index* of 1.70). *Connectivity & Intelligent Edge* and *General/ICT* also show above-average *Business Promotion*, suggesting a comparatively greater emphasis on commercialization, technology adoption and industrial deployment. By contrast, ***Quantum Technologies* and *Data & Compute Infrastructure* are more strongly oriented towards *Research Promotion***, with prevalence rates of 51.1% and 50.0%, respectively, and specialization indices of 1.41 and 1.38. These patterns are consistent with differences in technological maturity and capability requirements, particularly the importance of scientific knowledge and research infrastructure in emerging and infrastructure-intensive domains.

Projection is the least prevalent orientation across all technology groups, ranging from 10.8% of initiatives in *Cybersecurity & Digital Trust* to 21.3% in *Quantum Technologies*. Nevertheless, *Quantum Technologies* also exhibits the highest relative specialization in *Projection* (1.38), indicating a comparatively greater presence of international cooperation, partnerships and other outward-facing objectives.

Figure 6. Prevalence (up) and specialization (down) of policy orientations across digital technologies, 2014–2025





Source: JRC

The policy implication is one of portfolio coherence rather than a preferred universal mix. A protection-heavy profile may be appropriate in cybersecurity, while semiconductors may require stronger industrial instruments and quantum a deeper research base. **The 3Ps logic is useful precisely because it discourages a one-dimensional view of sovereignty.** Policy design should connect the dominant sovereignty risk in each technology to the instrument mix used to address it and should examine whether protective measures are accompanied by sufficient capacity to innovate, scale and collaborate internationally.

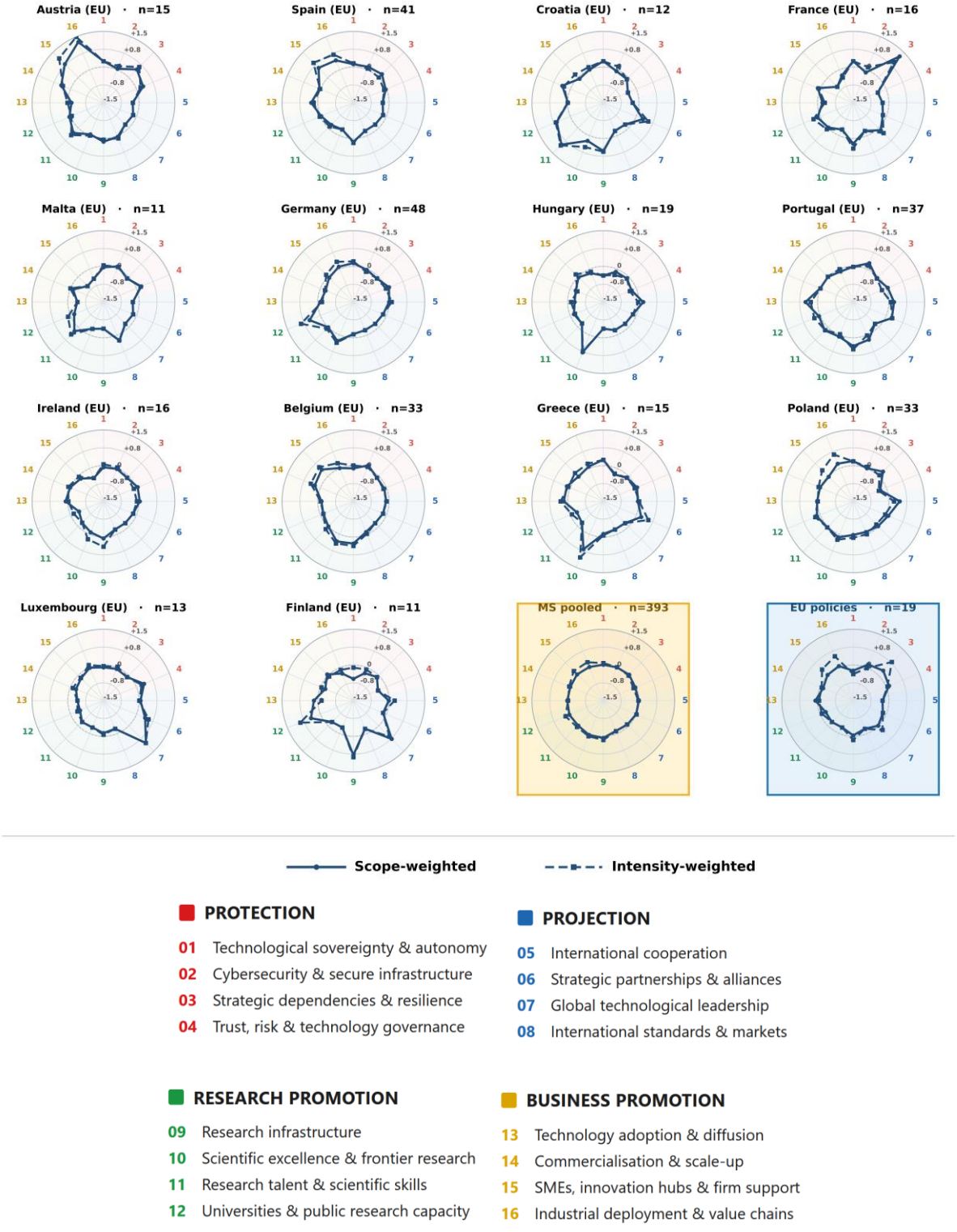
A further implication concerns sequencing. Technological orientations should not be read as static targets: *research promotion, business promotion* and *protection* may become important at different stages of technological maturity. Frontier domains can require sustained research infrastructure and talent before large-scale deployment instruments become effective; more mature or infrastructure-intensive domains may require procurement, scale-up finance, standards and supply-chain measures. Similarly, *projection* can support both early knowledge access and later market or standards influence. For monitoring purposes, this means that changes in the policy mix over successive STIP waves may be as informative as the level observed in a single year. A shift from research towards deployment may indicate maturation, while a rise in protection may reflect newly recognized vulnerabilities or a change in the external risk environment. These interpretations would, however, need to be tested against technology-specific evidence rather than inferred from the portfolio alone.

The distinction between research and business promotion also helps make a practical governance issue visible: the transition from capability creation to diffusion and scale. A policy system can be strong in frontier research but weak in commercialization, adoption or industrial deployment, or it can support firm adoption without building sufficient domestic knowledge and infrastructure. Digital sovereignty requires attention to both research capabilities and their translation into innovation and industrial development. While the STIP analysis identifies the policy orientations supporting these different stages, it cannot assess whether the transition is successful. Complementary insights are provided by the Digital Techno-Economic ecoSystem (DGTES) analysis (**Chapter 3**), which examines scientific publications, patenting, startup activity and scale-up financing, including international dependencies along this development pathway. Together, these perspectives can help policymakers assess whether policy priorities are aligned with observed technological and economic capabilities.

1.2.3. Country-level patterns in strategic digital policy orientations

Country-level results reveal differentiated strategic emphases rather than a single model of digital sovereignty policy. **Figure 7** and **Figure 8** present the scope- and intensity-weighted profiles of the 16 policy families for EU Member States and non-EU countries, respectively, over the 2014–2025 period. The analysis includes countries with at least ten eligible initiatives to limit the sensitivity of the results to individual policies. For Belgium, federal and regional initiatives are aggregated into a single national profile. The EU comparison is further complemented by two aggregate profiles: **MS pooled**, which combines all recorded national initiatives across the 27 EU Member States, and **EU policies**, which represents initiatives recorded directly at EU level.

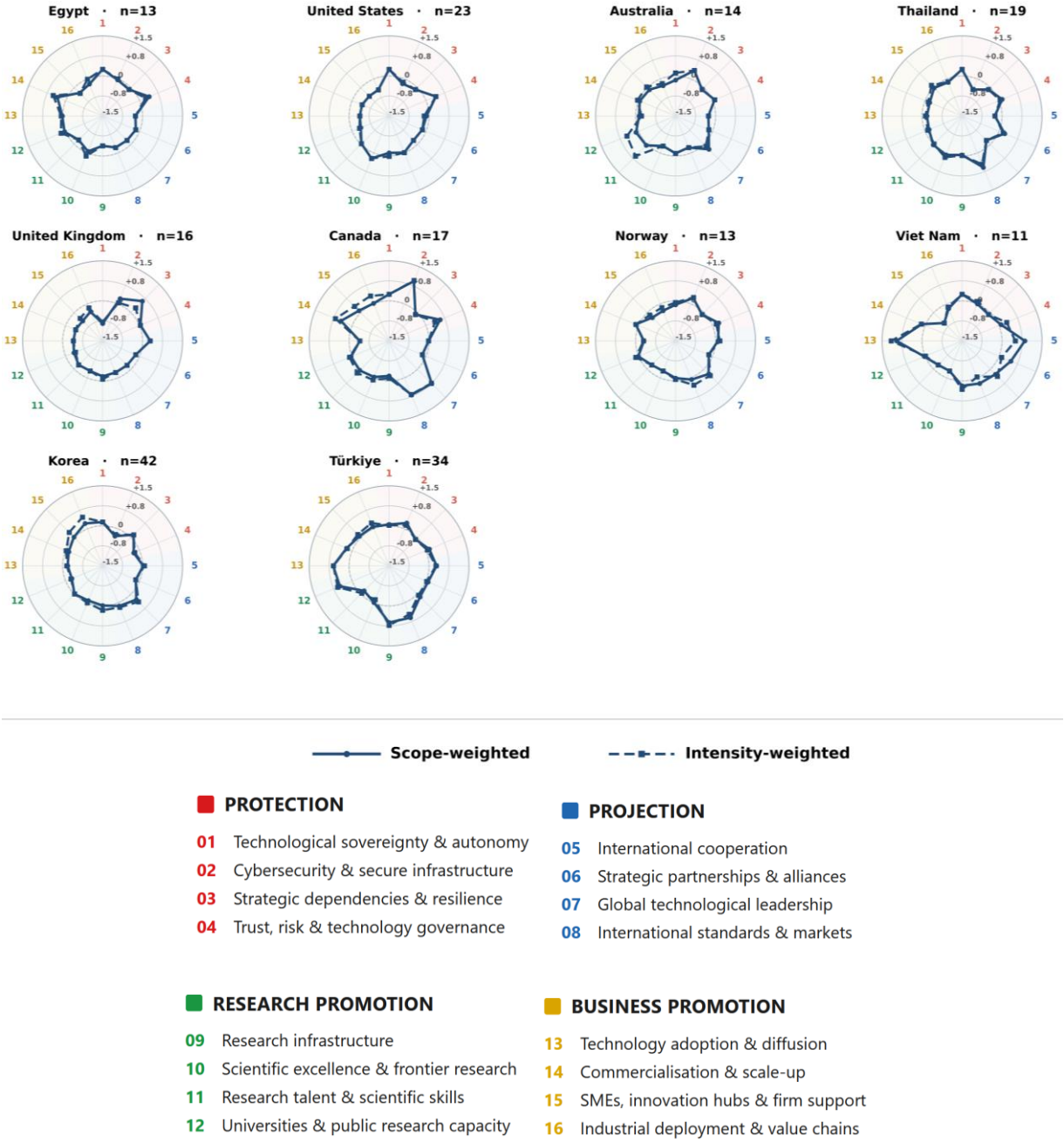
Figure 7. Strategic digital technology policy orientations across EU Member States, 2014–2025



Source: JRC

Notes: Radar charts show the 16 standardised policy-family indicators, weighted by scope (solid line) and intensity (dashed line). Countries with at least 10 policies are displayed individually. MS pooled includes all recorded national policies from the EU-27, while EU policies represent initiatives coded at EU level. Positive (negative) values indicate above-average (below-average) emphasis relative to the reference sample.

Figure 8. Strategic digital technology policy orientations across non-EU countries, 2014–2025



Source: JRC

Notes: Radar charts show the 16 standardised policy-family indicators, weighted by scope (solid line) and intensity (dashed line). Only countries with at least 10 policies are included. Positive (negative) values indicate above-average (below-average) emphasis relative to the reference sample.

The radar charts display weighted averages of standardised policy-family indicators, allowing the identification of relative emphases in national policy portfolios. Positive values indicate that a given family is more prevalent than in the reference policy sample, whereas negative values indicate relative under-representation. The four orientations—Protection, Projection, Research Promotion and Business Promotion—are represented through four specific policy families each, reflecting the

multidimensional nature of STI policy interventions. Importantly, these results describe the composition of reported policies rather than their effectiveness, financial scale or contribution to achieved digital sovereignty.

Across the countries examined, considerable heterogeneity emerges in the balance between protective measures, international projection and domestic capability-building. Some countries place relatively greater emphasis on strengthening research capacity and scientific infrastructure, while others prioritise business development, industrial deployment or the management of strategic dependencies. These differences suggest that digital sovereignty objectives are pursued through distinct combinations of policy instruments rather than through a common national policy model. They also demonstrate the importance of examining individual policy families, as aggregate orientations may conceal more specific areas of relative emphasis.

Several country profiles illustrate these differences. Among EU Member States, Austria displays a relatively strong Business Promotion orientation, with a scope-weighted summary score of +0.58, driven particularly by industrial deployment and value chains (+1.26) and support for SMEs and innovation hubs (+0.80). Spain also shows a positive Business Promotion profile (+0.33), particularly in support for SMEs, innovation hubs and industrial deployment. By contrast, Croatia stands out in Research Promotion (+0.59), with comparatively high scores for research talent and scientific skills (+0.99), universities and public research capacity (+0.62), and research infrastructure (+0.52). Finland similarly shows a positive orientation towards research infrastructure and public research capacity, alongside a relatively strong emphasis on global technological leadership. France is particularly distinctive within Protection, with a high relative score for strategic dependencies and resilience (+1.25). These results illustrate different national approaches to strengthening strategic digital capabilities, ranging from scientific capacity-building to industrial support and dependency management.

Among non-EU countries, Canada combines relatively strong Protection (+0.41) and Projection (+0.32) orientations, notably through cybersecurity and secure infrastructure, global technological leadership, and international standards and markets. Viet Nam displays a comparatively strong Projection profile (+0.46), particularly in international cooperation and strategic partnerships, alongside a strong emphasis on technology adoption and diffusion. Türkiye presents a comparatively diversified profile, with positive relative scores in Projection, Research Promotion and Business Promotion, reflecting a combination of outward-oriented objectives, research infrastructure and industrial capability-building. These examples reinforce the finding that the policy approaches associated with digital sovereignty differ substantially across national contexts. The observed differences are descriptive of the recorded policy portfolios and should not be interpreted as evidence that particular approaches are more successful in achieving digital sovereignty.

From an EU perspective, the distinction between national and aggregate policy orientations provides an additional layer of interpretation. The MS pooled profile combines all 393 national policy initiatives recorded across the 27 Member States, including countries with fewer than ten initiatives that are not displayed individually. Each policy contributes according to its scope or intensity score, rather than giving each Member State equal weight. This therefore represents the aggregate composition of the recorded national EU policy portfolio, with greater influence from countries accounting for larger numbers of initiatives. It is distinct from a simple average of national profiles and should be interpreted in light of potential differences in reporting coverage across countries.

The pooled Member State profile is relatively close to the overall reference distribution across most policy families, indicating that positive and negative national deviations partly offset each other when aggregated. Nevertheless, some differences emerge between the two weighting approaches. Under scope weighting, the pooled portfolio displays modest positive relative values for Research Promotion (+0.04) and Business Promotion (+0.03), while Projection remains slightly below the reference average (−0.05). Under intensity weighting, the emphasis on Research Promotion (+0.14) and Business Promotion (+0.13) becomes more pronounced. At the family level, this reflects comparatively stronger signals for universities and public research capacity, SMEs and innovation hubs, and industrial deployment and value chains. These differences suggest that the combined national policy portfolio gives greater relative weight to research and business capability-building when instruments involving stronger intervention mechanisms are emphasised. However, the relatively modest aggregate scores should not be interpreted as an absence of strategic policy activity, since standardisation measures deviation from the reference distribution rather than the absolute prevalence of policy objectives.

The EU policies profile provides a complementary perspective by considering the 19 initiatives recorded directly at EU level, separately from national Member State policies. Compared with the pooled national portfolio, EU-level initiatives show a particularly strong relative emphasis on strategic dependencies and resilience, especially under intensity weighting (+0.80). They also display positive intensity-weighted signals for industrial deployment and value chains (+0.52), and support for SMEs and innovation hubs (+0.35). By contrast, international cooperation and international standards and markets are relatively under-represented in this specific sample of EU-level initiatives. These results suggest a stronger relative emphasis on selected dependency-management and industrial capability-building objectives among the EU-level initiatives recorded in STIP. However, given the limited number of observations and the database's coverage characteristics, this profile should not be interpreted as a comprehensive representation of EU digital sovereignty policy, particularly in areas such as regulatory governance, international partnerships or the wider EU legislative framework.

Heterogeneity is relevant because it suggests that "digital sovereignty policy" is being assembled through national STI systems with different institutional legacies and strategic priorities. Countries may arrive at similar high-level objectives through different combinations of research funding, business support, governance, regulation, infrastructure and international engagement. For EU-level monitoring, this argues for a dashboard approach that preserves the underlying dimensions rather than collapsing them into a single league table. It also points to the value of linking policy-orientation data with outcome indicators in other layers of the report—for example, whether a research-oriented semiconductor portfolio is accompanied by domestic production capability, or whether protection-oriented cloud policy is associated with reduced concentration or dependency (Edler et al., 2023).

1.2.4. Country policy orientations under scope and intensity weighting

National policy portfolios combine instruments that differ substantially in their reach and intervention mechanisms, from targeted advisory programmes to system-wide strategies and major infrastructure investments. A key robustness question is whether the country patterns identified above remain consistent when greater weight is assigned to different characteristics of these instruments. Scope weighting emphasises the breadth of an intervention, whereas intensity weighting emphasises the resource commitments and regulatory or institutional mechanisms

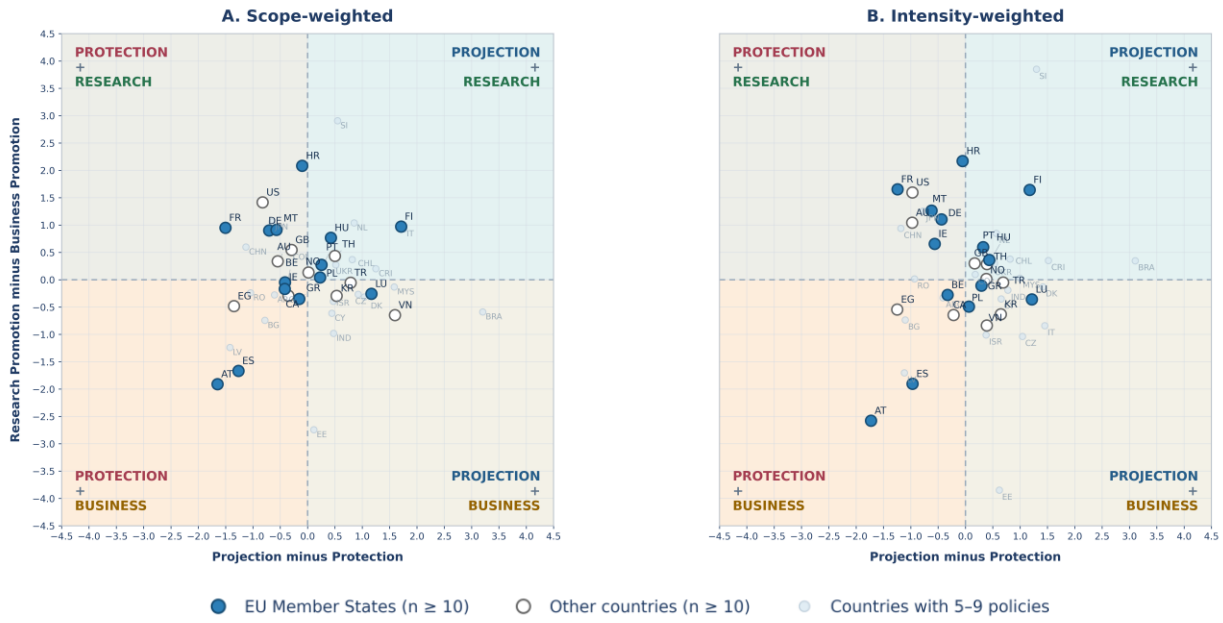
associated with the instrument type. Comparing the two approaches therefore assesses how sensitive the observed national orientations are to these alternative ways of weighting policy initiatives.

The comparison covers the period 2014–2025 and uses two complementary representations of national policy portfolios, each displaying scope-weighted positions in the left-hand panel and intensity-weighted positions in the right-hand panel. Both share the same horizontal axis, calculated as Projection minus Protection. Countries positioned to the right have higher relative scores for Projection than for Protection, while those to the left show the reverse. Since the underlying indicators are standardised against the reference policy sample, these positions describe relative policy emphases; they do not indicate the absolute number of initiatives devoted to either orientation.

Figure 9 combines this horizontal contrast with the balance between Research Promotion and Business Promotion. Countries above the horizontal axis have a stronger relative orientation towards research, while those below it have a stronger relative orientation towards business support. The resulting positions distinguish how national portfolios combine protective or outward-facing objectives with different approaches to developing technological capabilities.

For the 24 countries with at least ten eligible policies, both contrasts show a strong correspondence across weighting schemes. The Pearson correlation for Projection minus Protection is 0.923, and the Spearman rank correlation is 0.959. For Research Promotion minus Business Promotion, the corresponding values are 0.946 and 0.921. These results indicate that both the relative positioning of countries and their ordering along the two axes are broadly preserved. Individual positions may nevertheless shift as the weights attached to different instruments change, particularly where a country's portfolio includes measures with contrasting scope and intensity scores.

Figure 9. Country positioning under scope weighting (left) and intensity weighting (right). Projection versus Protection and Research versus Business Promotion, 2014–2025

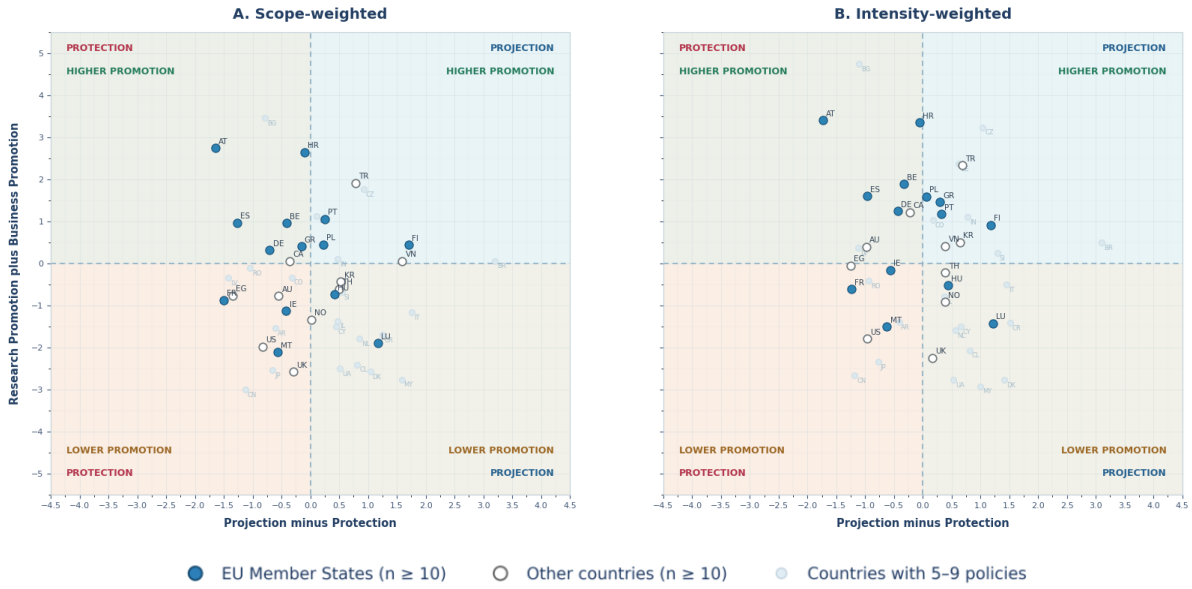


Source: JRC

Figure 10 provides a complementary perspective by replacing the research–business difference with the sum of Research Promotion and Business Promotion. Its vertical axis therefore captures the combined relative emphasis on capability-building. Positive values indicate a combined emphasis above the reference level, while negative values indicate a combined emphasis below it. A negative score does not imply an absence of research or business support, just as a positive score does not necessarily mean that both components individually exceed their reference levels.

This additional perspective helps distinguish portfolios that would otherwise appear similar when assessed only through the research–business balance. A country may have a score close to zero on that balance because research and business objectives are both strongly represented, or because both receive relatively limited emphasis. The combined measure makes this distinction visible. Austria and Croatia illustrate its value: although their portfolios lean towards Business Promotion and Research Promotion, respectively, both display a comparatively strong combined Promotion emphasis under both weighting schemes. Different balances between research and business objectives can therefore coexist with a similarly pronounced orientation towards capability-building.

Figure 10. Country positioning under scope weighting (left) and intensity weighting (right), Projection versus Protection and overall Promotion emphasis, 2014–2025



Source: JRC

1.2.5. What the STIP evidence can and cannot say about digital sovereignty?

The results provide a structured overview of how governments prioritize strategic digital technologies and the policy instruments they use to address them. They show where digital sovereignty concerns are linked to STI policy, which technologies receive attention, whether the policy logic is protective, promotional or outward-facing, and how national portfolios differ. This is valuable because **governance itself is a component of sovereignty: the ability to identify dependencies, set priorities, mobilize resources and coordinate institutions establishes whether technological and market capabilities can be built or protected.**

However, the evidence should not be used to infer achieved sovereignty. A country may report many policies but still depend heavily on external suppliers; conversely, a country with fewer recorded innovation policies may possess strong incumbent capabilities. The STIP data also does

not reveal whether programmes are fully funded, whether regulation is enforced, whether procurement reaches domestic firms, or whether international partnerships generate durable capability. The chapter therefore treats policy orientation as an input-side metric. Its strongest use in the broader Digital Sovereignty Metrics report is in combination with the infrastructure, market and people layers, where observed dependencies and capabilities can be compared with the policy response.

1.3. Conclusions

The STIP Survey analysis provides a replicable way to observe the shift in digital STI policy towards a more strategic focus on critical technologies, technological capabilities and dependencies. Using a conservative classification of reported initiatives, it identifies a substantial policy universe around critical digital technologies and shows a pronounced expansion of activity from the mid-2010s onwards. AI & Autonomous Systems is the most prominent technology group, but the policy landscape extends across data and compute, cybersecurity, quantum, semiconductors and connectivity. The result is a governance picture in which digital sovereignty is increasingly addressed through technology-specific policy portfolios rather than through generic digitalization measures alone.

Three conclusions are particularly relevant for policy monitoring. *First*, **sovereignty STI policy is multidimensional. Protection is prominent, but business promotion, research promotion and projection remain integral parts of the portfolio**. Technology domains display different combinations, reflecting different underlying risks and capability requirements. This supports a targeted approach: the appropriate balance of protection, domestic capability-building and international engagement should be assessed against the characteristics of each technology rather than imposed through a common template.

Second, **EU Member States display differentiated policy orientations, highlighting the diversity of national approaches to digital sovereignty.** While some countries, such as Austria and Spain, place comparatively greater emphasis on business-oriented support, others, including Croatia and Finland, show stronger relative orientations towards research promotion. France, meanwhile, stands out for its emphasis on strategic dependencies and resilience. These differences suggest that digital sovereignty is being pursued through distinct combinations of policy instruments, rather than through a common national policy model. From an EU perspective, this heterogeneity is particularly relevant. Different national policy portfolios may reflect complementary approaches to strengthening European technological capabilities, but they may also reveal potential imbalances between research, commercialization, industrial deployment and protection. The STIP analysis cannot determine whether these differences represent effective specialization or gaps in the collective European policy response. However, it provides a structured basis for identifying such questions and examining how national policy priorities relate to broader EU objectives and strategic dependencies.

Third, **considering both the reach and the intensity of policy interventions provides a more complete picture of national digital strategies.** These two perspectives highlight different aspects of government action, from the breadth of policy interventions to the strength of the instruments used. However, the overall strategic orientations of countries remain broadly consistent across both approaches. Together, they offer complementary insights into national policy priorities, while recognizing that the scores do not measure actual public spending or policy effectiveness. For future iterations of the Digital Sovereignty Metrics, the priority should be to

connect this governance evidence to outcome and dependency measures in other layers. The following questions could be explored:

- Is policy attention aligned with observed strategic dependencies?
- Are research-oriented policy portfolios followed by increased scale-up and production capability?
- Do protection-oriented interventions coincide with greater diversification or resilience?
- Is projection associated with greater influence in standards, alliances or international technology networks?

Repeated STIP waves could also support monitoring of policy rebalancing over time, provided reporting completeness and changes in database coverage are explicitly controlled.

The chapter therefore positions the STIP Survey as a structured "policy response" layer within a broader measurement architecture. It is suited to tracking strategic attention, policy mix and institutional orientation, but not to producing a stand-alone sovereignty score. Used in this way, it contributes to the report's broader objective: **moving from an abstract debate on digital sovereignty towards an evidence base that can distinguish vulnerabilities, capabilities and policy responses, while preserving the openness and international connectedness that are central to the EU approach.**

Section B

Digital Infrastructures, Software, and Data



2. Substitutability of the European Digital Offer: A Digital Sovereignty Perspective

2.1. Approach, methodology and data limitations

2.1.1. Introduction

This chapter operationalises one component of digital sovereignty as technical substitutability: the extent to which an organisation can replace a digital solution without being technically locked into the incumbent through proprietary interfaces, a deployment model controlled solely by the supplier, or an inability to move data and workloads. The conceptual motivation is established in the economics of switching costs and compatibility. Incompatible products and accumulated switching costs can bind customers to vendors and weaken competitive pressure, while interoperability and portability can reduce such lock-in (Farrell and Klemperer, 2007; Krämer and Stüdlein, 2019; Jeon et al., 2023). This framing is also consistent with the EU Data Act, which places switching and interoperability requirements on data-processing services, and with recent Commission work on interoperability specifications for cloud and edge services (European Parliament and Council, 2023; European Commission, 2026).

The metric is deliberately narrower than a general assessment of "European", "open source" or "sovereign" technology. Digital sovereignty is a multidimensional capacity involving governance, infrastructures, markets and products, and people; substitutability addresses only the technological and market-facing ability to change supplier or operating arrangement (Di Marco et al. 2025; Bryson et al., 2026). A solution may therefore contribute to European digital sovereignty through various characteristics, independently of the extent to which it offers technical substitutability. Conversely, strong technical substitutability does not necessarily imply European origin, open source licensing or broader sovereignty characteristics. **This distinction is important for policy measurement because provider origin, licensing model and technical exit options capture related but conceptually distinct dimensions of technological autonomy and dependency** (Gineikytė-Kanclerė and Eggert, 2025).

The chapter is structured as follows. **Section 2.2.1** presents the data, methodological approach and measurement limitations. **Section 2.2** examines reported substitutability across the European digital offer, including differences across technological layers, incumbent target groups and open source status, and discusses the implications for digital sovereignty metrics. **Section 2.3** summarizes the main findings and identifies directions for further measurement development.

2.1.2. Data source and unit of analysis

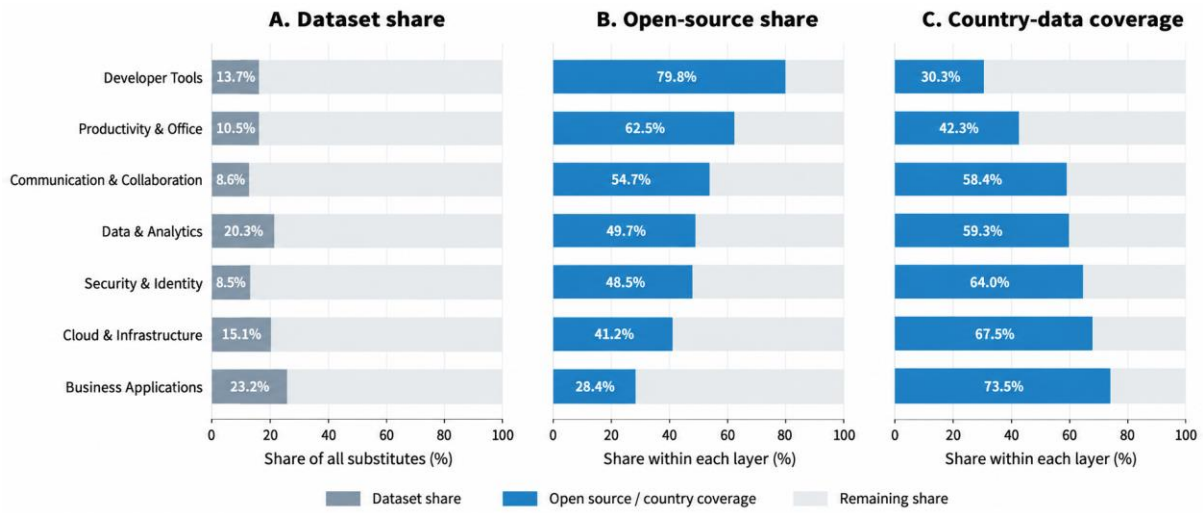
The empirical source is the EuroStack Directory Project[5], a curated catalogue of digital solutions aimed at supporting European digital sovereigntyspanning cloud services, open source technologies

5 https://euro-stack.com/

and other components of the digital stack. Its scope includes both European-developed solutions and globally developed technologies that are substantially supported or considered relevant within the European ecosystem. The analysis uses a snapshot of web-scraped data collected on 6 July 2026. The dataset follows the directory's original classification structure, comprising seven top-level layers—*Business Applications, Cloud & Infrastructure, Communication & Collaboration, Data & Analytics, Developer Tools, Productivity & Office, and Security & Identity*—and 64 lower-level layers. Accordingly, the dataset should be interpreted as a structured snapshot of available and relevant digital alternatives rather than as a representative census of European firms or software products (EuroStack Directory Project, 2026). The resulting analytical dataset, including the indicators of interface substitutability, deployment autonomy and portability, is available through the JRC Open Data Catalogue (Isaraj, 2026b).

The unit of analysis is a EuroStack solution entry. The analysis relies on the "Description", "Features" and "Benefits" textual fields for scoring the three substitutability indicators (see **Sub-section 2.1.3**), while structural fields such as "*Open Source*", "*Country*", "*Layer*" and "*Alternative to*" are used only for stratification and descriptive comparison. The "Country" field records the geographical association assigned to each solution by EuroStack, without systematically distinguishing between the provider's location, the solution's origin or, particularly for open source projects, the geographical location of developers, maintainers or project governance.

Figure 11. Overview of substitutes, open source share and country-data coverage by layer



Source: JRC

After concatenation, the analytical dataset contains 1,593 solutions: 23% Business Applications, 15% Cloud & Infrastructure, 9% Communication & Collaboration, 20% Data & Analytics, 14% Developer Tools, 11% Productivity & Office, and 9% Security & Identity. Open source Solutions (OSS) accounts for 80% of Developer Tools, 63% of Productivity & Office and 55% of Communication & Collaboration. Data & Analytics and Security & Identity are close to 50%, while the OSS share falls to 41% in Cloud & Infrastructure and 29% in Business Applications (see **Figure 11**). The availability of country information varies considerably across layers. A broadly inverse association emerges between open source prevalence and country-data coverage, with layers characterized by higher shares of open source solutions generally exhibiting lower availability of country information. This pattern may reflect the nature of open source solutions, which are often developed and maintained by decentralized, internationally distributed communities rather than

organizations associated with a single country, making geographical attribution less straightforward.

2.1.3. Substitutability indicators

As shown in **Table 1**, each solution is evaluated on three binary indicators: *Interface, Autonomy deployment*, and *Portability*. The indicators are scored using an LLM-based prompt applied to the information provided in three textual fields of the EuroStack Directory: "Description", "Features" and "Benefits". The prompt, reproduced in **Annex 2.1**, assigns a score of one only when the available text explicitly reports the relevant capability. By contrast, a score of zero indicates that the available text does not provide sufficient evidence to confirm the capability under the scoring criteria. It should therefore be interpreted as an absence of documented evidence, not as proof that the capability itself is absent. This distinction is essential when interpreting the results, as **the indicators measure the visibility of substitutability-enabling features in the available text rather than the full set of technical characteristics of each solution**.

Table 1. Substitutability indicators

Indicator	Criterion	What does not qualify
Interface (I)	1 only when the text reports a **replacement-relevant** interoperable interface, protocol, format, API compatibility or drop-in interface; 0 otherwise.	Generic integration claims, generic API availability, or inferred compatibility.
Deployment autonomy (D)	1 only when the text explicitly reports **customer-run** installation, self-hosting, on-premises operation or deployment on customer-controlled infrastructure; 0 otherwise.	Cloud availability, privacy, sovereignty language, or open source status by itself.
Portability (P)	1 only when the text reports a concrete mechanism for moving data, workloads or configuration, or **for switching provider**; 0 otherwise.	Bare "no lock-in" claims, interoperability without movement, or self-hosting alone.

Source: JRC

2.1.4. Comparison groups

The comparison groups are derived from the EuroStack "Alternative to" field, which identifies the incumbent products or services that a listed solution is presented as capable of replacing. Google, Microsoft and Amazon/AWS are treated as a distinct comparison group because a consistent body of evidence identifies these firms as holding structurally important positions in Europe's digital economy. Their prominence is most clearly documented in cloud infrastructure, where AWS, Microsoft Azure and Google Cloud together account for around two thirds to 70% of the European market, but their relevance extends beyond cloud to enterprise software, productivity applications, analytics and public-sector digital services. **The literature also points to the reinforcing role of ecosystem integration, switching costs and dependency on non-EU providers in**

sustaining these positions (Gineikytė-Kanclerė and Eggert, 2025; European Parliament, 2025; Synergy Research Group, 2025; European Commission, 2026).

To capture competition with these incumbent ecosystems more accurately, the classification maps each named alternative to a provider-family dictionary covering Google, Microsoft and Amazon/AWS products and brands. The procedure is deliberately rule-based and auditable. Where an "Alternative to" cell contains several products, the field is first split into the individual named alternatives. Each item is then normalised for case and punctuation and compared against an explicit lookup dictionary of unambiguous product and brand aliases. For example, the Microsoft family includes terms such as Microsoft 365, Office 365, Azure, Azure DevOps, SharePoint, OneDrive, Power BI, Dynamics 365, GitHub and GitHub Actions; the Google family includes Google Workspace, Google Drive, Google Cloud Platform, GCP, Google Meet, BigQuery, Firebase and related services; and the Amazon/AWS family includes Amazon Web Services, AWS, S3, RDS, CloudFront, Route 53, Cognito, EC2, Lambda and Redshift. Matching is based on the complete normalised product name rather than loose substring matching. The rule-based procedure assigns the large majority of product and brand aliases automatically to the relevant provider family. A small number of cases that remained ambiguous after this automated step were reviewed manually and, where necessary, corrected before the final classification was produced.

On this basis, three mutually exclusive analytical groups are constructed. "Big Three targets" comprises solutions for which at least one named alternative can be mapped to the Google, Microsoft or Amazon/AWS provider family. "Other named targets" comprises solutions with a non-empty field for which none of the named alternatives maps to those three provider families. "No named target" comprises solutions for which the "Alternative to" field is empty. In this specific context, this does not imply that the solution has no potential substitute; rather, it means that EuroStack does not explicitly identify a specific incumbent product or service that the solution is presented as replacing. The fourth group, "All", is the full sample. The first three groups are mutually exclusive, while the fourth is the overall reference population.

This approach allows the market-positioning variable to reflect the broader incumbent ecosystem rather than only explicit occurrences of the parent-company name. It also preserves reproducibility: the dictionary can therefore be updated transparently if additional aliases are identified in future versions of the directory.

For descriptive provider-specific insights, Google, Microsoft and Amazon/AWS classifications are non-exclusive. A solution may, for example, be presented as an alternative to both Microsoft Teams and Google Meet and will therefore contribute to both provider profiles. For the inferential comparisons, however, the hierarchy is mutually exclusive: the presence of at least one "Big Three" match takes precedence, ensuring that each solution enters only one comparison group. This distinction avoids double counting in the statistical analysis while retaining the richer multi-provider information for descriptive diagnostics.

Table 2 summarizes the composition of the four groups. Solutions without a named target represent the largest group, while the remaining solutions are relatively evenly distributed between "Big Three" and "Other named" targets. Open source prevalence is highest among solutions targeting other named providers and lowest among those without a named target. Country-data coverage is highest for "Big Three targets" and lowest for "Other named targets", highlighting differences in licensing characteristics and geographical information availability across groups.

Table 2. Comparison groups derived from "Alternative to"

Comparison group	N	Open source (%)	Country data (%)
Big Three targets	461	**53.6**	**65.7**
Other named targets	430	**61.6**	**48.8**
No named target	702	**38.9**	**59.4**
All	1593	**49.3**	**58.4**

Source: JRC

2.1.5. Data limitations

Several limitations should shape interpretation. *First*, the metric measures reported substitutability mechanisms, not latent capability. Sparse product descriptions can create false negatives, while well-documented products have more opportunities to provide qualifying evidence. *Second*, the "Alternative to" field is a directory classification rather than observed switching behaviour; it indicates intended substitutability, not realised migration. It does not provide evidence that replacing the named incumbent is technically feasible or that such a replacement has occurred in practice. *Third*, the catalogue is curated and continuously updated, meaning that the dataset does not necessarily represent the full range of digital solutions available in Europe. y. The current EuroStack site lists more solutions than this fixed snapshot here, highlighting the importance of specifying the data collection date when updating the metric (EuroStack Directory Project, 2026). *Fourth*, country information is not consistently available across solutions, with coverage varying by layer and comparison group. This uneven availability limits geographical comparisons, as the solutions with recorded country information may not be representative of the full dataset. Country-based results are therefore used descriptively and interpreted alongside data coverage rates, as further discussed in Section 2.4. *Fifth*, binary indicators compress heterogeneous mechanisms: an interface based on an open standard and a narrow compatibility layer both score one if they meet the textual criteria, although their practical effects on substitutability may differ.

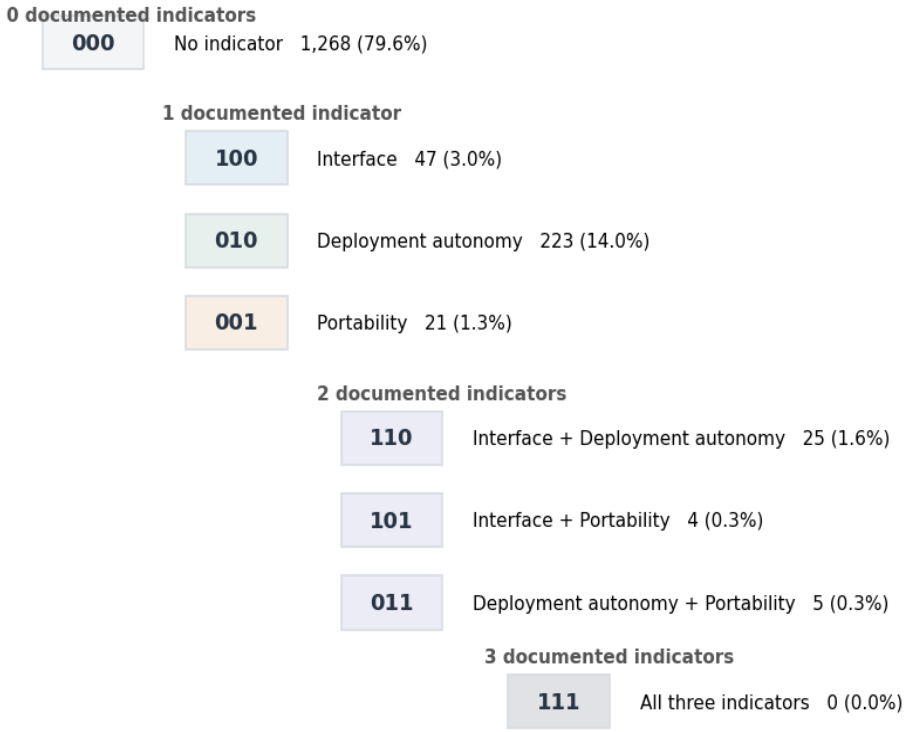
These limitations do not invalidate the metric. Rather, they define its policy use: it is best treated as a transparent, reproducible signal of reported exit-enabling mechanisms. This is particularly relevant because portability and interoperability are not merely technical properties; they interact with incentives, network effects, entry conditions, security and privacy (OECD, 2021; Jeon et al., 2023; Kim, 2026). For monitoring purposes, the key value is comparability over time and across groups under a stable scoring protocol.

2.2. Insights

For each solution, the three indicators, *Interface* (I), *Deployment autonomy* (D) and *Portability* (P), take values of either 0 or 1. The total substitutability score is calculated as the sum of these indicators (S = I + D + P), ranging from zero to three. **Figure 12** presents the distribution of solutions across the eight possible combinations of the three indicators. Three cumulative measures are also defined, capturing solutions reporting at least one, at least two or all three

mechanisms. These measures describe the breadth of reported exit mechanisms rather than stages of technological maturity. **The central empirical result is the contrast between the availability of European digital alternatives and the limited reporting of technical exit mechanisms**. Of 1,593 solutions analysed, only 20% report at least one technical exit mechanism, while the remaining 80% provide no explicit evidence of the three. exit mechanisms considered. Most positive cases report only one mechanism, and fewer than 3% report two. No solution reports all three exit mechanisms.

Figure 12. Eight-state ladder of documented technical substitutability



Source: JRC

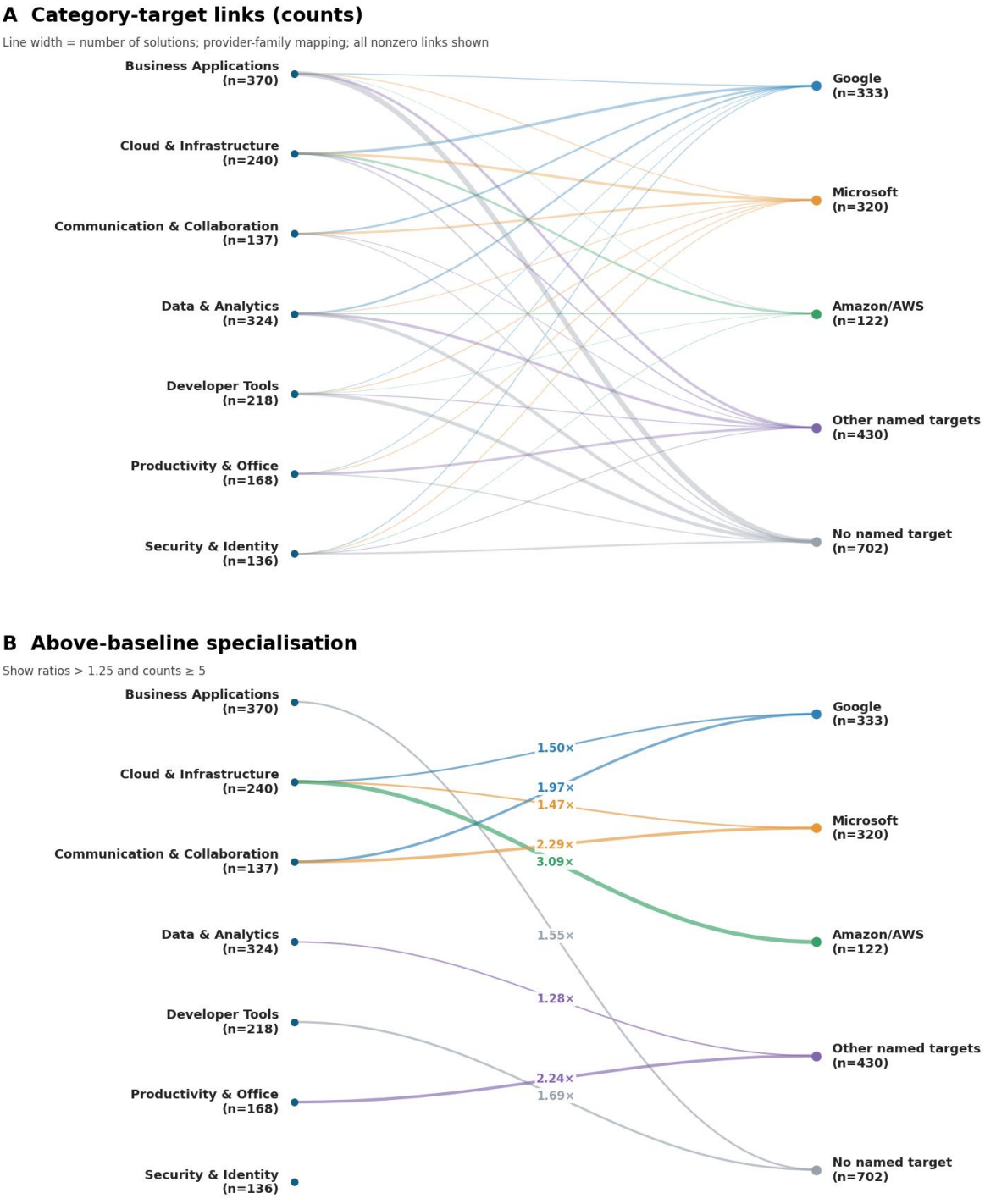
***Deployment autonomy* is the dominant documented mechanism**: appearing in 253 solutions (16%), followed by *Interface substitutability* in 76 solutions (5%) and *Portability* in 30 solutions (2%). Among solutions reporting two mechanisms, the most common combination is *Interface substitutability* and *Deployment autonomy* (25 solutions), followed by *Deployment autonomy* and *Portability* (5) and *Interface substitutability* and *Portability* (4). For a digital-sovereignty metric, this pattern suggests that European supply-side availability should not be equated with technical substitutability. A purchaser may have access to an European alternative yet still facing switching costs if interfaces, deployment control and migration mechanisms are not explicitly established. Importantly, **the result should not be read as evidence that four fifths of the analysed solutions are technically non-substitutable; it means that** available descriptions **do not report exit mechanisms.** The distinction is crucial for potential applications such as procurement and policy dashboards.

2.2.1. Substitutability across digital layers

Figure 13 shows that the seven layers classifying the type of solutions - *Business Applications, Cloud & Infrastructure, Communication & Collaboration, Data & Analytics, Developer Tools, Productivity & Office, and Security & Identity* - differ not only in the number of solutions associated with particular incumbent targets, but also in the extent to which those associations are stronger than expected from the overall target distribution. Panel A reports the absolute number of category-target links, allowing to see where solutions are most frequently positioned as alternatives to Google, Microsoft, Amazon/AWS, "Other named" providers, or "No named" target. Panel B complements this by reporting above-baseline specialisation ratios: for each layer, the share of links directed to a given target group is compared with that target group's share across all links in the dataset. Ratios above one therefore indicate that a layer is disproportionately oriented towards that target relative to the catalogue as a whole; the figure displays only stronger specialisations, above 1.25 and with at least five observations.

This distinction between volume and specialisation is important. A target may attract many links simply because it is common across the catalogue, whereas the specialisation ratio identifies where a layer is unusually concentrated on that target. Cloud & Infrastructure, for example, is markedly specialised towards Amazon/AWS and also shows above-baseline orientation towards Google and Microsoft. Communication & Collaboration is similarly specialised towards Google and Microsoft, while Productivity & Office is relatively more concentrated on other named targets. *Business Applications* and *Developer Tools*, by contrast, show above-baseline association with solutions for which no specific incumbent target is named. These patterns suggest that the competitive and replacement context varies systematically across the digital stack.

Figure 13. Category-target links (A) and above-baseline target specialization (B)



Source: JRC

Notes: Provider classifications are non-exclusive: a solution may be listed as an alternative to products or services from more than one provider (e.g. both Google and Microsoft) and is therefore counted in each relevant provider category.

The layer-specific substitutability results in **Table 3** are consistent with this **heterogeneity in market positioning**. *Communication & Collaboration* records the strongest overall profile, with more than two fifths of solutions reporting at least one indicator, driven especially by *Deployment autonomy*. *Cloud & Infrastructure* also performs comparatively strongly and has the highest incidence of *Interface substitutability*, which is consistent with the greater importance of compatibility and interoperability in infrastructure-level replacement. *Security & Identity* also shows a relatively high prevalence of reported substitutability, again largely through *Deployment autonomy*. At the other end of the distribution, *Business Applications* exhibits the weakest profile, with very limited evidence of interface-based replacement and no solutions documenting two or more indicators. These differences may also reflect the distinct technical characteristics and deployment requirements of solutions across layers, rather than market positioning alone. Across all layers, the general pattern is that *Deployment autonomy* is much more commonly reported than *Portability*, while evidence of multiple substitutability dimensions remains uncommon.

Table 3. Indicators by layer

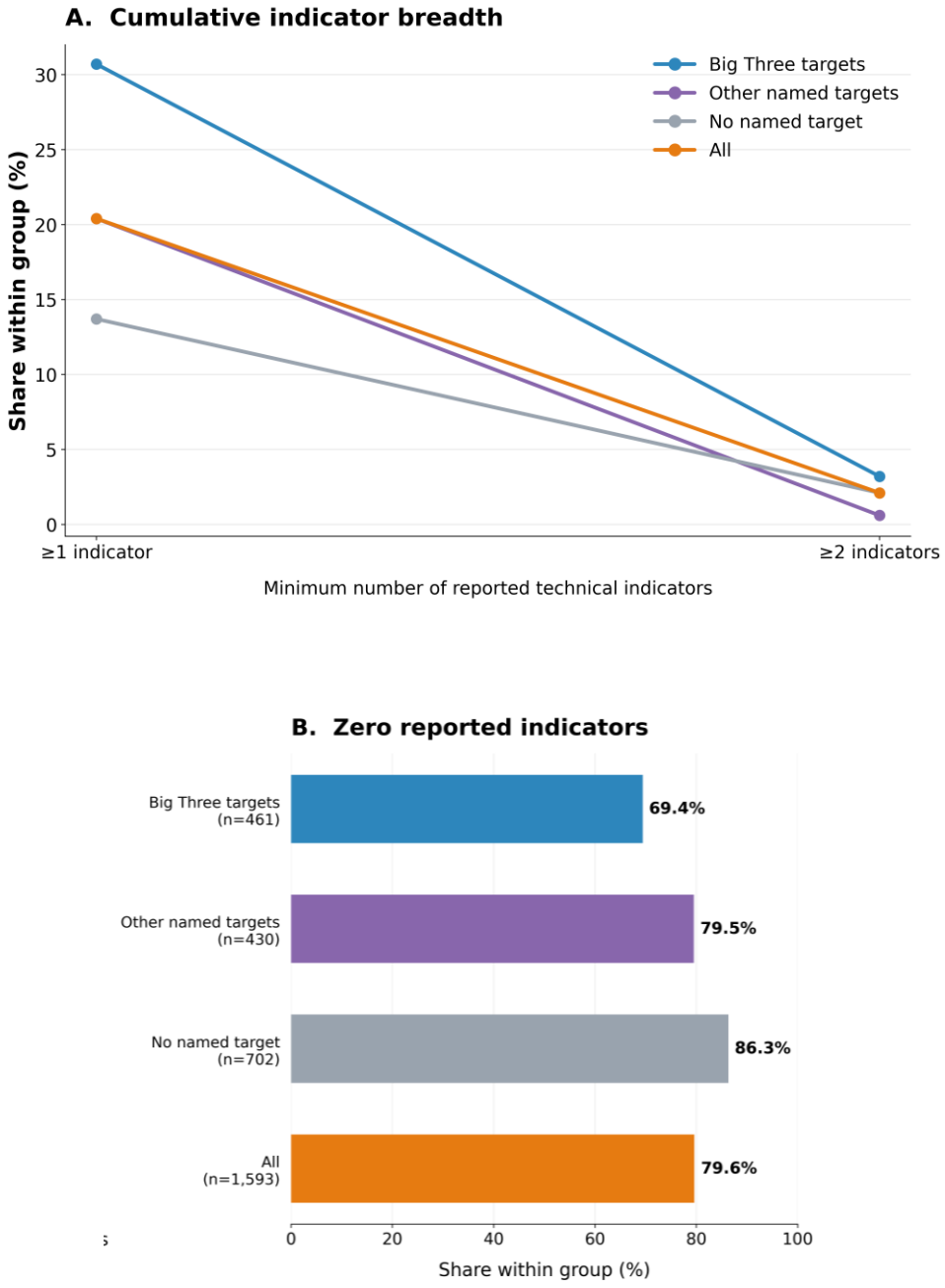
Layer	Interface (%)	Deployment (%)	Portability (%)	Any indicator (%)	2 or more indicators (%)
Business Applications	0.3	8.4	1.9	10.5	0.0
Cloud & Infrastructure	12.1	16.2	2.5	26.7	4.2
Communication & Collaboration	10.2	38.0	0.7	42.3	6.6
Data & Analytics	3.1	12.0	2.5	16.3	1.2
Developer Tools	3.7	15.1	0.9	17.4	2.3
Productivity & Office	1.8	16.7	3.6	20.2	1.8
Security & Identity	8.1	22.8	0.0	28.7	2.2

Source: JRC

2.2.2. Substitutability among the main incumbents

Across the three groups, 31% of solutions positioned as alternatives to the "*Big Three*" report at least one substitutability mechanism, compared with 21% targeting "*Other named*" providers and 14% of solutions with "*No named*" target. The corresponding zero-mechanism shares are 70%, 80% and 86%. Two-mechanism documentation remains uncommon in all groups: 3% for "*Big Three*" targets, 1% for "*Other named*" targets and 2% for solutions with no named target (see **Figure 14**).

Figure 14. Cumulative breadth of reported substitutability mechanisms by target group



Source: JRC

The gradient is consistent with a plausible market mechanism: products explicitly positioned as replacements for large incumbent ecosystems may have stronger incentives to document compatibility, migration or deployment control, because reducing buyer switching costs is part of the value proposition. This interpretation is consistent with research work linking compatibility and portability to switching costs and competition (Farrell and Klemperer, 2007; Jeon et al., 2023). However, the result is descriptive. The “Alternative to” field itself may be more completely populated for mature or strategically positioned products, which may also provide more detailed information on their technical capabilities.

2.2.3. Open source and Deployment autonomy

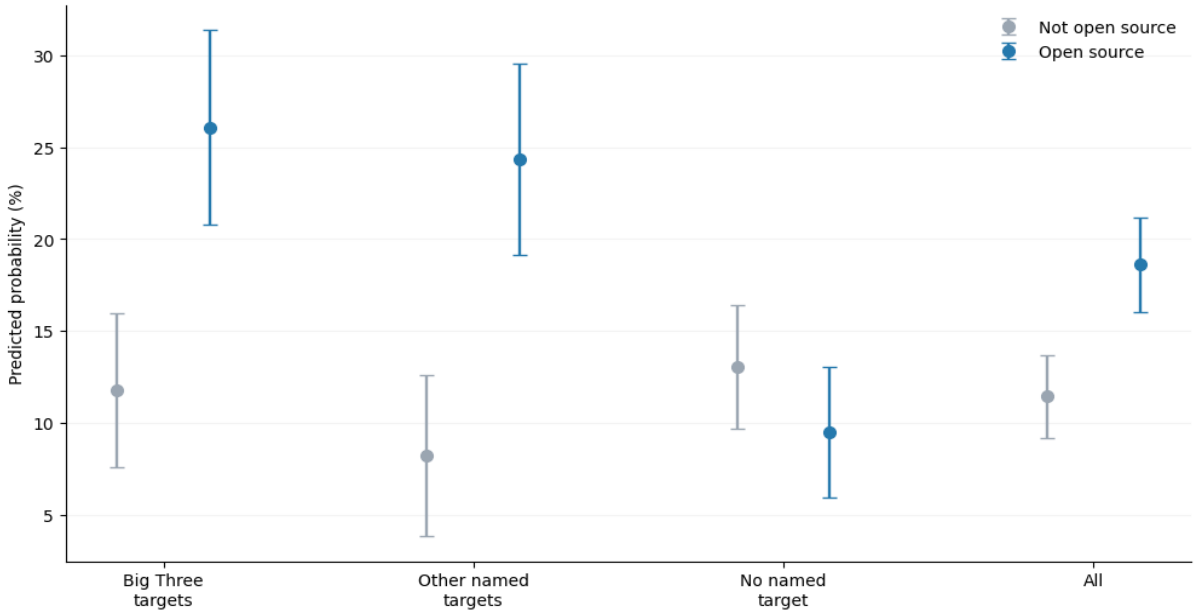
Open source status is common but not universal in the catalogue, and it should not be treated as a substitute for an exit mechanism. The scoring approach (see the prompt in **Annex 2.1**) does not assume that open source solutions can be self-hosted or transferred to another provider unless these capabilities are explicitly reported. Among the three substitutability indicators, *Deployment autonomy* is particularly relevant to open source solutions, as open source licensing may facilitate independent deployment without necessarily guaranteeing it. Building on the earlier finding that *Deployment autonomy* is the most frequently reported mechanism, the analysis examines its association with open source status across the different technological layers and comparison groups. The results show a positive association for solutions targeting named providers, but not for those without a named target (**Figure 15**). To assess this relationship while accounting for differences across technological layers and comparison groups, a binomial generalised linear model with a logit link is applied:

$$\text{logit } Pr(D_i=1) = \alpha + \beta \cdot OpenSource_i + \gamma \cdot TargetGroup_i + \delta \cdot (OpenSource_i \times TargetGroup_i) + \theta \cdot Layer_i$$

Predicted probabilities are standardised over the observed distribution of the seven layers; 95% confidence intervals use the delta method. Here, D_i indicates whether solution i reports *Deployment autonomy*, $OpenSource_i$ identifies open source solutions, $TargetGroup_i$ refers to the three comparison groups defined in Section 1.4, and $Layer_i$ identifies the seven technological layers. The interaction term ($OpenSource_i \times TargetGroup_i$) allows the association between open source status and *Deployment autonomy* to differ across comparison groups, while $\alpha, \beta, \gamma, \delta$ and θ represent the model parameters.

The analysis identifies statistical associations between variables but does not establish cause-and-effect relationships. This is because open source status may be related to other characteristics, such as product type, business model, documentation practices or solution maturity, which may also influence the results.

Figure 15. Predicted probability of reported *Deployment autonomy*, by target group and open source status



Source: JRC

Notes: Predicted probabilities are marginally standardised over the observed distribution of the seven layers.

For "*Big Three targets*", the predicted probability of *Deployment autonomy* is 11.8% (95% CI 7.6–16.0) among non-open source solutions and 26.1% (95% CI 20.8–31.4) among open source solutions. For *"Other named targets"*, the corresponding estimates are 8.2% (3.8–12.6) and 24.3% (19.1–29.6). For solutions with "No named target", the relationship reverses numerically—13.1% (9.7–16.5) versus 9.4% (5.9–12.9)—and the open source contrast is not statistically distinguishable from zero (p=0.15). Across the full catalogue, standardised deployment rises from 11.4% among non-open source to 18.5% among open source solutions.

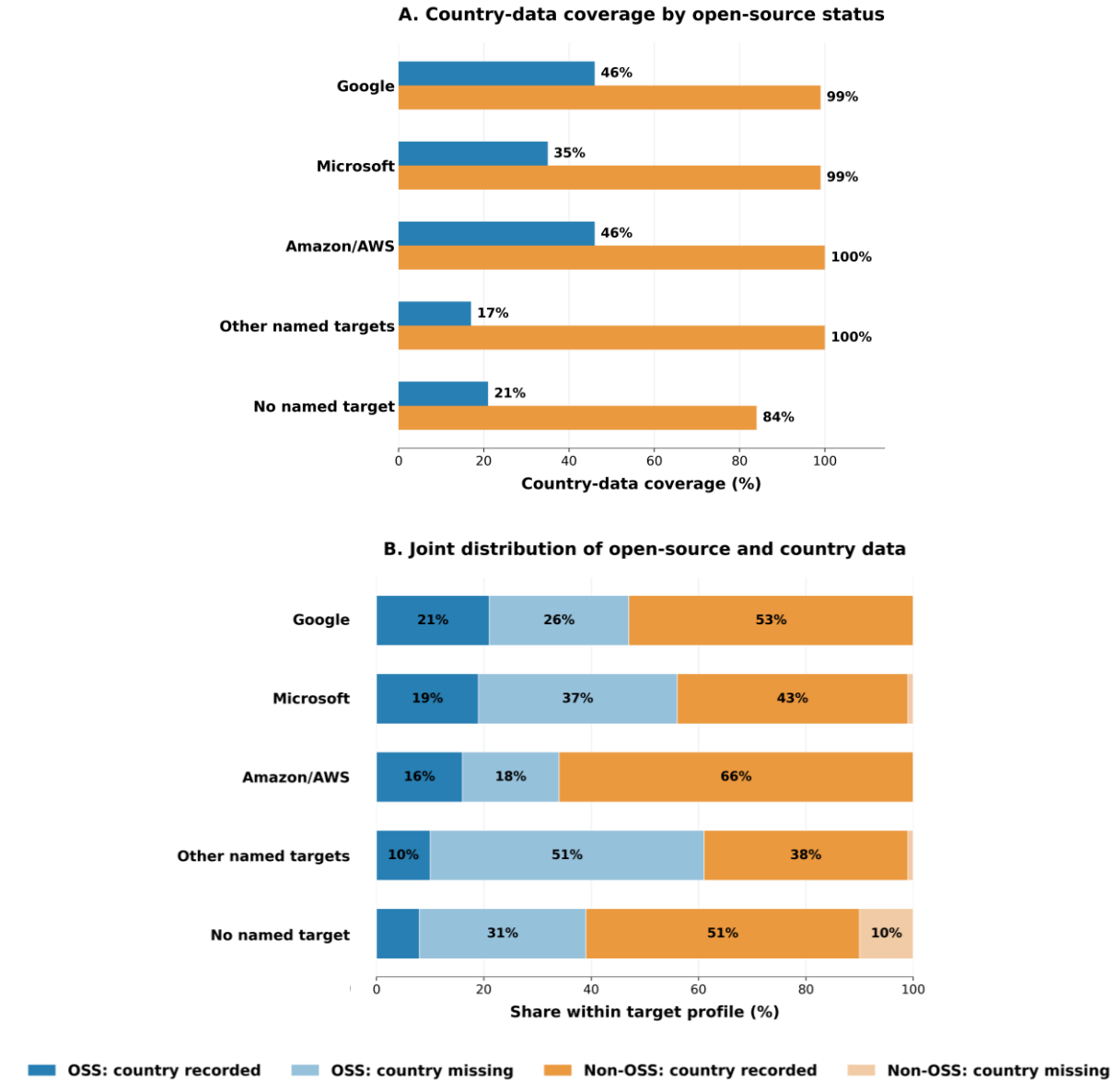
The group-specific open source association is statistically strong for "*Big Three targets*" (odds ratio 2.76; p<0.001) and "*Other named targets*" (odds ratio 3.78; p<0.001), but not for the "No-target" group. These findings suggest that the relationship between open source licensing and *Deployment autonomy* varies depending on how solutions are positioned in the market. While open source licensing may facilitate *Deployment autonomy*, it does not necessarily guarantee it. **These findings highlight the importance of assessing open source licensing and reported deployment capabilities separately when evaluating technical substitutability.**

2.2.4. Open source and country profiles

The descriptive analysis reveals differences in open source prevalence and country-data availability across target profiles. As shown in **Figure 16**, country information is substantially less frequently recorded for open source than for non-open source solutions across all groups. Coverage among open source solutions ranges from 17% for "*Other named targets*" to 46% for Google and Amazon/AWS targets, whereas it reaches 84% or more among non-open source solutions. This confirms that the inverse association observed at the aggregate level is also present when comparing solutions by open source status within each target profile.

This pattern should be interpreted cautiously. As discussed in **Section 2.2,** the internationally distributed nature of many open source projects may make geographical attribution less straightforward. Differences in organisational structures and directory documentation practices may also contribute to the observed gaps. Importantly, the "Country" field does not consistently distinguish between provider location, solution origin and other geographical attributes. Country-data availability should therefore not be interpreted as an indicator of the geographical origin or distribution of the solutions.

Figure 16. Open source share and country-data coverage by target profiles

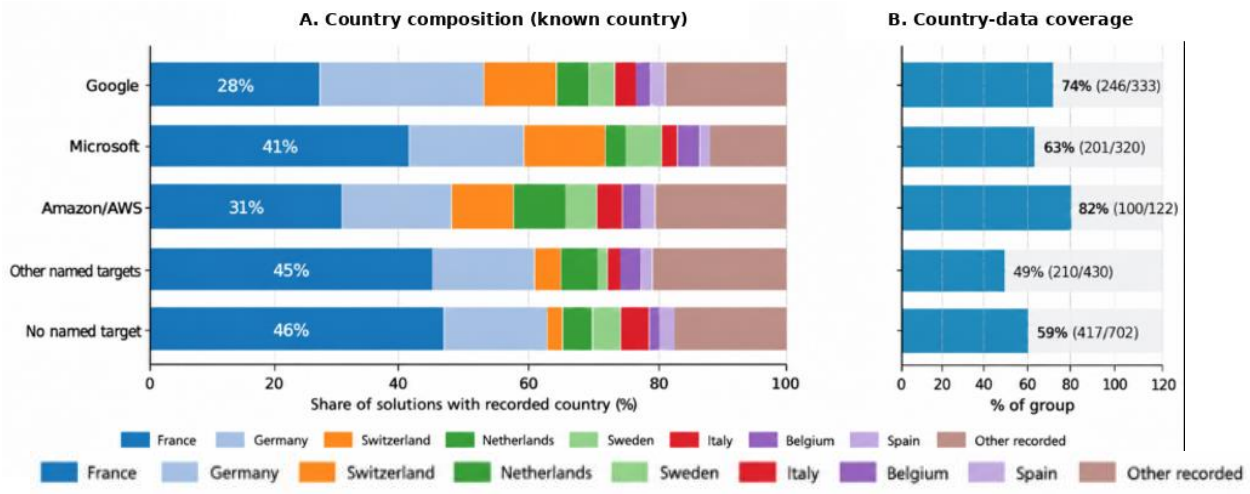


Source: JRC

Figure 17 examines the geographical composition of solutions for which country information is recorded. As shown in Panel A, France and Germany account for substantial shares across most target profiles, although the composition varies between groups. These distributions should be interpreted alongside the corresponding coverage rates in Panel B, given substantial differences in missing country information. For future monitoring, distinguishing provider headquarters, project

governance, development location, and hosting arrangements would provide a more informative basis for geographical comparisons.

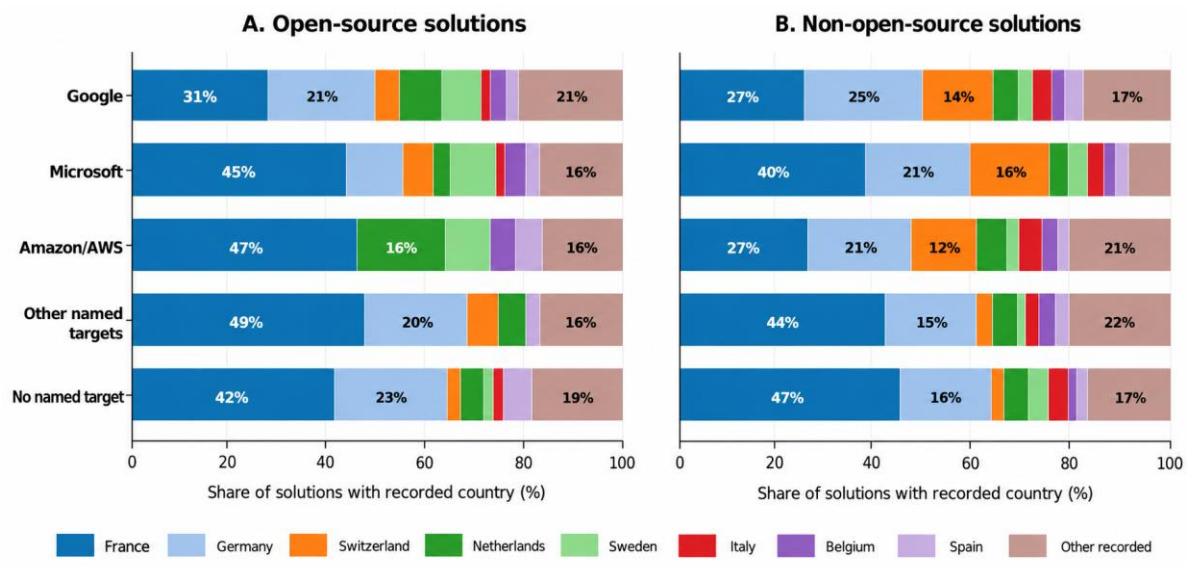
Figure 17. Country composition among solutions with recorded country information



Source: JRC

Figure 18 further compares the geographical composition of open source and non-open source solutions across target profiles. France accounts for the largest share of recorded countries in most groups, particularly among open source solutions targeting Microsoft, Amazon/AWS and "*Other named providers*", where it represents nearly half of observations. Germany also contributes substantially, especially among Google-targeting open source solutions. While geographical distributions differ by open source status, no consistent pattern emerges across target profiles. These comparisons should be interpreted cautiously, given the considerably lower country-data coverage among open source solutions (Figure 6).

Figure 18. Country composition of open source and non-open source solutions by target profile



Source: JRC

These country-related evidence complements the analysis of open source development capacity presented in Chapter 3.EuroStack records a concentration of solutions associated with France and Germany, and the GitHub-based indicators highlight that France stands out for its strong Intensity in terms of conde contributions, whereas Germany demonstrates a high-degree of international connectedness trough cross-border collaboration. . This distinction underscores the importance of considering both the availability of digital alternatives and national capabilities to develop, maintain, and foster collaboration around them.

2.2.5. Policy interpretation for Digital Sovereignty Metrics

Digital sovereignty is a multidimensional concept that remains challenging to define and measure. However, it includes specific technical characteristics that can be assessed, one of which is substitutability. This chapter contributes to its measurement by identifying whether digital alternatives explicitly report mechanisms that facilitate switching between solutions or providers. Three policy-relevant messages emerge. *First*, the availability of digital alternatives does not necessarily imply technical substitutability, as only one in five solutions describes at least one exit mechanism. This supports a metrics approach that asks whether exit paths are actually specified. *Second*, *Deployment autonomy* is more frequently reported than interoperability or portability, highlighting that the ability to operate a solution independently does not necessarily ensure the possibility of switching providers or transferring data and workloads. This distinction is also relevant to the EU Data Act's provisions on switching and interoperability (European Parliament and Council, 2023; European Commission, 2026). *Third*, reported substitutability varies according to the type of digital solution and the incumbent products or services it is positioned to replace. Open source licensing may support certain technical capabilities, particularly *Deployment autonomy*, but does not necessarily guarantee them.

These results suggest that digital sovereignty metrics could benefit from assessing substitutability through distinct technical indicators, alongside other characteristics such as licensing and geographical information. For a potential application of the measurement approach in procurement, the proposed indicators could help identify solutions requiring further verification of interoperability, customer-controlled deployment and data portability. For policy monitoring, applying the same scoring approach to updated datasets could help track changes in the reporting of technical exit mechanisms over time. However, the indicators rely on available product descriptions rather than technical testing and should therefore be interpreted as measures of reported capabilities, not verified substitutability. In this sense, the framework offers a transparent and reproducible contribution to the broader measurement of digital sovereignty.

2.3. Conclusions

This empirical analysis relies on the EuroStack Directory as an early example of efforts to bring information on European digital solutions together in a single, structured source. The methodological approach, however, could be applied to other comparable databases that compile sufficiently detailed information on digital solutions, their characteristics and the alternatives they are intended to replace. **In this 1,593-solution snapshot taken in July 2026, by looking at technical substitutability**. **(i.e., Inference, Deployment autonomy, and Portability mechanisms, only one in five solutions reports at least one explicit technical exit mechanism.** *Deployment autonomy* is the mostly documented route to autonomy; replacement-relevant interfaces are less common, and concrete portability mechanisms are rarely reported. The main limitation identified is therefore not necessarily the availability of alternatives or their

technical capabilities, but the limited evidence of exit-enabling mechanisms in the public information provided by the directory. This should not be interpreted as evidence that such mechanisms are absent or undocumented elsewhere.

The result is particularly relevant to policymakers and the broader debate around digital and technological sovereignty, as it highlights the importance of ensuring that digital solution catalogues provide clear and comprehensive information on technical switching mechanisms to support informed assessments of substitutability. Research based evidence shows why compatibility and portability can alter switching costs and competitive dynamics, while EU legislation increasingly makes switching and interoperability a policy objective (Farrell and Klemperer, 2007; OECD, 2021; Jeon et al., 2023; European Parliament and Council, 2023). The proposed indicators offer a framework for assessing technical substitutability at the solution level, which could be extended to other digital solution catalogues by adapting the scoring approach to their data structures and available information.

This analysis contributes to operationalising digital sovereignty by translating technical substitutability into measurable indicators, while highlighting the complexity and multidimensional nature of the broader concept. For a Digital Sovereignty Metrics framework, the three indicators should be retained separately and reported jointly through the eight-state and cumulative ladders. A single binary "sovereign/non-sovereign" label would discard precisely the information needed for intervention. For example, a product that can be self-hosted but cannot export data presents a different policy risk from one that supports standard interfaces but remains supplier operated. The four comparison groups derived from "Alternative to" add a market-positioning dimension and show that substitutability is substantially more frequent among solutions explicitly positioned against the largest incumbent ecosystems.

A next step would be to assess whether the switching mechanisms identified in the EuroStack Directory can be verified through more detailed technical information, given that the catalogue descriptions may also serve communication or marketing purposes. Future analyses could also incorporate complementary sources, such as user surveys and reviews, to capture users' experiences and evaluations of the solutions, as well as evidence from technical testing, migration case studies and independent assessments. Combining these sources would provide a more comprehensive understanding of the practical feasibility of switching between solutions and providers. This could be complemented by more detailed measures of portability quality, including the scope of exported data, configuration fidelity, downtime, transfer costs and destination neutrality. Future analysis could also consider maintenance and development activity to assess the long-term sustainability and viability of digital solutions, an aspect particularly relevant for open source projects, which may depend on the continued engagement of developer communities. These extensions would strengthen the assessment of effective switching capabilities, while preserving the transparent baseline established here.

In policy terms, the underlying principle is that technical substitutability is an important component of digital sovereignty, as it concerns users' ability to switch between solutions and providers. European origin, open source licensing and local hosting can contribute to technological autonomy, but none is sufficient on its own to ensure substitutability. A robust metric should therefore assess whether a solution supports interoperability, customer-controlled deployment and portability. The EuroStack analysis provides an initial assessment of how these mechanisms are reported across the European digital offer, highlighting the relevance of incorporating technical substitutability into broader digital sovereignty metrics.

Finally, these conclusions should be interpreted in light of the study's limitations. The analysis relies on a curated, non-representative catalogue of digital solutions, and the indicators capture reported substitutability mechanisms rather than independently verified technical capabilities. Moreover, the classification of solutions as alternatives to incumbent providers does not demonstrate actual switching possibilities, while incomplete and uneven country information limits geographical comparisons. The results should therefore be considered an initial assessment of reported technical substitutability rather than a comprehensive evaluation of the European digital offer or its effective switching capabilities.

3. Observing Europe's open source ecosystem: community, activity and cross boarder collaboration

3.1. Introduction

Digital sovereignty depends not only on technological infrastructures, software and data but also on the capacity of citizens, entrepreneurs, and workers not merely to use these assets, but also to understand and shape them (Di Marco et al., 2025). This is particularly relevant for open source software (OSS), where the availability of substitutive programmes can reduce certain technological dependencies, but does not itself guarantee the capacity to deploy, maintain or further develop a technology. OSS communities and developers represent therefore an important component of the capabilities associated with digital infrastructure and software.

Such communities are social groups of individuals and organisational contributors who participate in the collaborative production of public information goods. The outputs of these communities occupy a distinctive position in digital economies: they can simultaneously represent state-of-the-art technologies, commodities, and public goods (Böhm, 2022). Their strategic importance is reflected in the EU Open Source Strategy, which places empowered communities alongside open-science networks, standardisation bodies, data-stewardship initiatives, and GovTech innovators as a critical layer of Europe's digital capacity.

When looking at the enablers underlying digital sovereignty, the geographical distribution of open source human and technological capacity (e.g., to create, use and diffuse these technologies) becomes a highly useful insight to indicate a country's ability to develop and adopt technological alternatives. Accordingly, this chapter examines the geographical distribution of OSS activities, users, and cross-country collaborations, both at the EU and international levels. In addition, Chapter 8 *Digital sovereignty skills: Emerging perspectives* of this report, complements this view by considering the human competences underpinning digital sovereignty for various societal roles.

The present study analyses levels of OSS capacity, activity intensity, and interconnectedness, using GitHub Innovation Graph dataset[6] by linking indicators of developer activity and collaboration to the country level. GitHub's position as a primary web-based platform for hosting, managing, and collaboratively developing OSS through the Git version-control system makes these data particularly relevant[7].

Linking OSS development with geographical territories may initially appear at odds with the inherently distributed and, as the analysis below will show, highly international character of OSS communities. Yet the relevance of geography becomes clearer when **OSS is approached as a multidimensional phenomenon rather than solely as a coding activity**. Digital technologies

---

6 GitHub Innovation Graph

7 According to the latest figures reported by the respective platforms, GitHub hosts more than 180 million developers (GitHub Octoverse data, 2025), compared with over 50 million estimated registered users on GitLab (Gitlab by the numbers, 2026) and 15 million developers on Bitbucket (Bitbucket homepage, 2026). Gitee, the major Chinese code-hosting platform, reports a community of more than 14 million developers (Gitee "about us" section, 2026), while Codeberg report more than 200 thousand registered accounts (Letter from Codeberg PR team, 2025). Although these figures are not strictly comparable, as platforms employ different definitions and reporting periods between 2025 and 2026, they illustrate the substantial difference in scale.

facilitate collaboration across distance, but this does not necessarily eliminate the role of place in generating and concentrating knowledge, skills, and innovation. **Geographical concentrations of developers and OSS projects may generate positive local spillovers for firms, workers, universities, and other developers**. These effects may, in turn, attract further developers and firms or stimulate additional OSS activity. In this sense, open source activity, as captured through GitHub data, can be interpreted not only as a proxy for geographical innovation outcomes but also as a potential contributor to them (Wachs et al., 2022).

A geographical perspective can also reveal differences in how countries position themselves within the global OSS ecosystem. In particular, it can help identify concentrations of capabilities, differences in the development trajectories of national communities, patterns of cross-border collaboration.

Against this background, the analysis follows two complementary directions. First, section 3.1 examines the amount, geographical distribution and evolution of GitHub activity within the EU in order to identify differences across national OSS communities and highlight potential areas of emerging strength. Results are compared with the insights emerging from the Open Source Observatory (OSOR)[8] and with other relevant sources observing the OSS context from a geographical perspective.

Second, section 3.2 focuses on the interconnectedness of these communities. By reconstructing the most significant cross-country interactions, the analysis seeks to identify patterns of cooperation and the position of European OSS communities within wider international networks.

3.2. Methodology

This study examines the geographical structure of the OSS developers' community and activity in 2025 (the most recent complete year for which data are available), identifying the main dimensions that characterise each national ecosystem, delineating European clusters with similar profiles, and observing international collaboration networks. It addresses two research questions:

1. *How is the GitHub EU open source developer community geographically structured, and what patterns emerge across Member States' ecosystems in terms of capacity, activity intensity, and interconnectedness?*
2. *Focusing on the connections, which GitHub cooperation networks appear to be the most prominent within the EU Member States and between the EU and the rest of the world, and which national ecosystems appear to be the most interconnected?*

The empirical analysis uses 2025 country-level data derived from GitHub Innovation Graph, a publicly available dataset covering quarterly observations from Q1 2020 to Q1 2026. It provides near-global coverage of public GitHub activity and reports aggregate statistics at the country level.

[8] The Open Source Observatory (OSOR, Open Source Observatory (OSOR) | Interoperable Europe Portal) is a European Commission initiative hosted within the Interoperable Europe Portal. It includes an observatory that provides FOSS expertise and information as well as serves as middle-ground to connect European Public Administrations with other relevant stakeholders. To reach this objective, OSOR promotes the use of Free and Open Source software and supports the community.

Metrics for countries are only reported when there are 100 or more unique developers performing the relevant activity within the considered time period and only for public repositories.

The analysis centred on 2025, and the observed metrics are:

- **Developers**. Number of developer accounts located in a given country based on statistical mode daily location, as of the last date of each quarter. Excludes users that are bots or otherwise flagged as "spammy". Includes developer accounts that may no longer be active[9].
- **Repositories**. Number of software projects in a given country based on the statistical mode location of all repository members with *triage*[10] and above roles, as of the last date of each quarter. Includes repositories that may no longer be actively developed or maintained.
- **Git pushes**. Number of times developers in a given country uploaded code to GitHub during each quarter. Changes to files made through GitHub's online platform automatically result in a push. Note that a single git push may contain one or multiple commits.
- **Country collaborators**. Volume of collaboration on software projects based on the sum of git pushes sent and pull requests opened by a developer to a repository owned by another developer or organization during each quarter. A country acts as a source when its developers contribute to repositories attributed to other countries, and as a destination when repositories attributed to it receive contributions from developers located abroad.

Developers and repositories are measured as stocks observed in each quarterly snapshot, whereas git pushes represent activity flows. Three dimensions are constructed to capture distinct features of national OSS ecosystems:

- **Capacity**, measured as developers per million inhabitants. It refers to the relative size of a country's developer community in relation to its population and provides an indication of the diffusion of software development participation within the population.
- **Intensity**, measured through repositories per developer and git pushes per developer. The former indicator captures the relative prevalence of repositories associated with the developer base, while the latter reflects the frequency of code contributions. Together, they provide an indication of how intensively the observed developer community engages in software-development activity;
- **Connectedness**, measured as the sum of incoming and outgoing cross-border collaborations per developer, using git pushes and pull requests between developers and repositories located in different countries. It refers to the degree to which a country's developer community is integrated into cross-border OSS development networks.

---

9 The metrics of activity are assigned to a location based on the relevant user as determined by their IP address when interacting with GitHub. If a user changes locations in the time period, the location for all user-relevant activity would be determined by the statistical mode of location sampled daily in the period (e.g. if a developer were contributing to open source projects in the United States for two months, but also made contributions while traveling in India, all activity from that developer during that quarter would be assigned to the United States).

10 Triage contributors can manage issues, discussions, and pull requests without write access. The above access are writer, maintainer and administrator. Repository roles for an organization - GitHub Docs

After constructing these substantive ratios, each indicator is independently min–max normalised on a 0–1 scale across the EU-27; single-indicator dimensions take the normalised value directly, while multi-indicator dimensions are computed as the equally weighted arithmetic mean of their normalised components. Consequently, single-indicator dimensions span the full 0–1 range, whereas multi-indicator dimensions may not, as their averages reach 0 or 1 only when the same country records the minimum or maximum across all constituent indicators. Once scores had been established for the three dimensions, countries were grouped using k-means clustering. The appropriate number and composition of clusters was assessed by comparing k-means solutions across different *k*, using the elbow method and silhouette analysis.

The data are subject to several important limitations. First, they rely on a broad definition of developers (for example, accounts that may no longer be active are included). Second, a single git push may contain one or multiple commits, making it impossible to quantify the volume of development activity represented by each push. The data also include repositories that may no longer be actively developed or maintained. Furthermore, VPNs and other mechanisms that alter or conceal IP addresses can introduce distortions into location-based metrics and, in general, countries should not be interpreted as developers' nationality, permanent residence or permanent place of employment. A further limitation concerns the fact that not all activity hosted on the GitHub platform necessarily qualifies as open source. For example, public repositories may completely lack a license (in which case there is no legal right to use the code), or may lack an explicitly open source licence. Finally, as already mentioned, other open source development platforms exist in addition to GitHub. Therefore, the GitHub-based indicators used in this analysis should be interpreted as proxies for OSS development and collaboration rather than as direct measures of OSS activity. We believe, however, that this qualifies as a reasonable assumption and anyhow, to the authors' knowledge, no better datasets exist that can satisfactorily answer the chapter's research questions.

To provide qualitative context for the patterns emerging from the quantitative analysis, the results are considered alongside evidence from the OSOR Country Intelligence Reports[11] and from other data sources observing the OSS ecosystem from a geographical perspective. This information is not used to establish causal relationships with the GitHub indicators, but rather to identify characteristics that may help contextualise differences observed across countries.

3.3. Findings

3.3.1. EU clusters and comparison with non-EU countries

To capture the scale of GitHub open source development in Europe, Innovation Graph data were analysed for the EU-27 using annual country-level data for 2025 to identify the three dimensions described in the methodology: **Capacity**, **Intensity** and **Connectedness**. The quantitative scores were then complemented by qualitative evidence from the OSOR Country Intelligence Reports[12], focusing specifically on initiatives engaging open source communities and wider public. While these

11 Open Source Software Country Intelligence | Interoperable Europe Portal

12 Open Source Software Country Intelligence | Interoperable Europe Portal

initiatives often involve public-sector actors, their scope extends beyond public administrations to engage broader open source communities, private-sector stakeholders and the general public.

In absolute terms, the European OSS developer landscape is dominated by a small number of countries, notably Germany (19.5% of the total number of developers, 18.5% of repositories and 19.1% of push share), France (15% of the developers, 15.2% of the repositories and 16.5% of the pushes), Spain (10.3% of developers, 10.7% of repositories, 10.7% of pushes) and the Netherlands (8% of developers, 8.5% of repositories, 8.2% of pushes). However, when the different dimensions are normalised by population or by developers[13], the scores provide a different narrative (**Figure 19**).

It should be emphasised that the clusters each country is assigned to do not constitute a ranking, a progression, or a performance hierarchy from best to worst. Rather, they represent four balanced groups of countries with similar score profiles. Although some clusters record higher scores than others, these results must be interpreted considering the data limitations set out above. They are not intended to capture the open source ecosystem in its entirety, but rather to provide an initial and exploratory perspective through which to examine it.

Cluster A – "Developer-driven Ecosystems" is characterised by high developer Capacity, particularly in the **Netherlands** (1.00) and **Estonia** (0.86), as well as high development Intensity, especially in Estonia (0.89) and **Finland** (0.84). Countries in this cluster also tend to have moderate-to-high international Connectedness. Its defining feature, however, is the combination of a large OSS developer base relative to population combined with intense developer activity.

The qualitative evidence points to several factors that may help explain this profile, including mature digital ecosystem, established OSS organisations and institutional support for open source development.

Estonia combines high Capacity and Intensity with a highly digitalised public sector and an established role for OSS in digital-government infrastructure. X-Road[14], jointly developed with Finland through the Nordic Institute for Interoperability Solutions (NIIS), illustrates how this strong domestic ecosystem is also linked to international OSS cooperation. Similarly, Finland combines relatively strong Capacity and Intensity with a long tradition of OSS development and adoption: the OSOR highlights an established ecosystem involving organisations such as Finnish Centre for Open Systems and Solutions (COSS)[15] and Open Knowledge Finland[16], suggesting that sustained organisational and community infrastructure may contribute to a high level of OSS activity. The Netherlands stands out above all for the highest developer presence and strong Connectedness. The Dutch Open Cloud Alliance[17] provides a more recent example of coordination among market actors around open and interoperable digital infrastructure, presenting broader forms of ecosystem-level cooperation. Sweden, meanwhile, combines high Capacity (0.75) with moderate-to-high Intensity (0.61), alongside initiatives spanning institutional ecosystem development through

---

13 See paragraph 3.*2. Methodology*

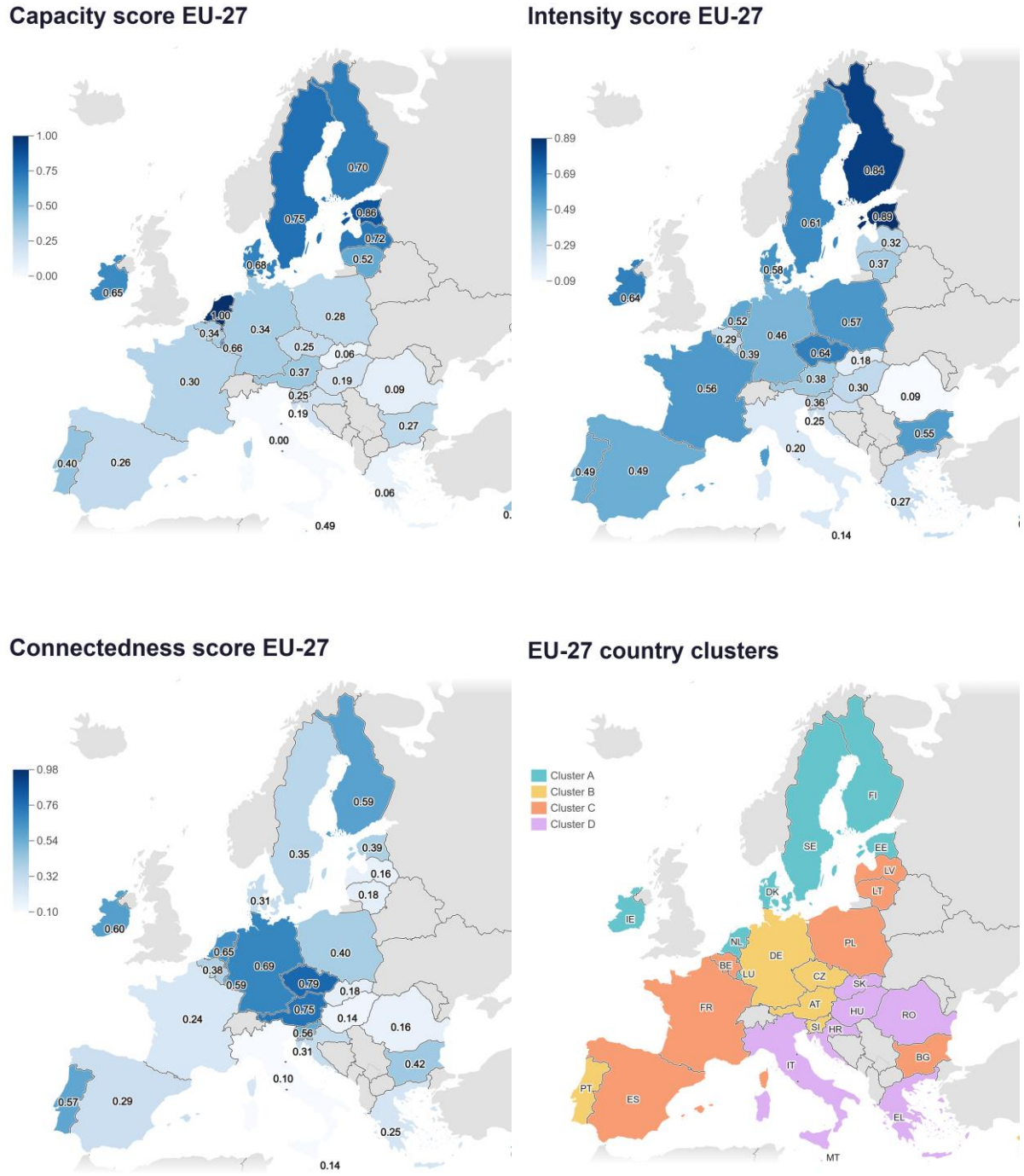
14 X-Road - e-Estonia

15 COSS – Finnish centre for Open Systems and Solutions

16 OKFI - Open Knowledge Finland

17 OCA—Manifest—Digitaal-2026.pdf

Figure 19. Maps illustrating Capacity, Intensity and Connectedness scores and Clusters, EU-27



Administrative boundaries: © EuroGeographics © OpenStreetMap
Cartography: Eurostat – IMAGE, 10/2026

Source: JRC

OSPO Sweden[18], and civic technology initiatives as Open Up![19], created to monitor procurement patterns.

Taken together, these cases suggest that the cluster's high Capacity and Intensity may be associated with mature domestic OSS ecosystems, where communities are supported by a broader organisational and institutional infrastructure. International collaboration is also present, but appears to complement (rather than define) the strong domestic developer base that distinguishes this cluster.

Cluster B – "Internationally connected Ecosystems" presents a medium-low Capacity (0.25–0.40), while Intensity is mostly moderate (0.36–0.64). What distinguishes this cluster is its high level of Connectedness, which ranges from 0.56 to 0.98.

The qualitative evidence provides some context for this pattern, pointing to several forms of cross-border OSS engagement. **Germany** has launched the Sovereign Tech Fund[20] that directly finances the maintenance and resilience of critical open source infrastructure at the global level.

Austria and **Czechia** have launched the Open Source Innovation Hubs[21], which provide a particularly close qualitative counterpart to the Connectedness dimension; they are meant to advance digital sovereignty and competitiveness through the strengthening of interregional cooperation on open source technologies. Austria also agreed with Germany to collaborate on and evaluate OpenDesk[22], an open source suite tailored for public services.

Taken together, these cases suggest that the cluster's high Connectedness may be associated with institutional mechanisms that actively support cross-border OSS cooperation, including interregional networks, joint public-sector initiatives, and investments in shared open source infrastructure. They also suggest that a country does not need an exceptionally large developer base to occupy a central position in international OSS collaboration.

Cluster C – "Mixed-profile Ecosystems" is the most heterogeneous group where generally the scores lie around the middle of the overall distribution. However, important differences emerge within the cluster. **Latvia** and **Lithuania** perform particularly well in terms of Capacity (0.72 and 0.52 respectively) indicating a relatively strong developer base. In contrast, **Poland**, **Bulgaria**, and **France** achieve higher scores in Intensity. Bulgaria and **Belgium** stand out for having the highest Connectedness scores within the cluster. Comparing these results with some qualitative OSOR findings, Latvia's high capacity occurs alongside an established open source community, Latvia's Technology Association (LATA)[23], which promotes open technologies through advocacy, training, conferences and hackathons.

France stands out for its institutionalised approach and many strategic players, such as the Union of Free Software and Open Digital Companies (CNLL)[24] that comprises more than 200 companies

18 https://ospo.se

19 Open Up! - Open Up!

20 Sovereign Tech Fund | Sovereign Tech Agency

21 Open Source Innovation Hubs

22 openDesk

23 Open technology | LATA | Riga

24 CNLL

that specialise in, or have significant activity in, OSS development and open digital technologies. In Poland, open source associations and companies came together to establish an alliance, called Alliance of Friends of the Open and Free Software (SPOIWO)[25], with the goal of uniting the Polish open source ecosystem and supporting public and private organisations' adoption of open source solutions and concrete development initiatives such as the Polish Large Language Model (PLLuM)[26], an open source Polish-language AI project developed by a research consortium for public- and private-sector use. Bulgaria presents a similar quantitative profile; here initiatives such as SIGMA[27], an open source public-procurement transparency platform, provide an example of domestic OSS development. Belgium combines strong Connectedness with weaker developer presence and Intensity; from the OSOR it emerges that its decentralised ecosystem includes internationally oriented communities and initiatives, most notably the annual Free and Open Source Software Developers' European Meeting (FOSDEM)[28]. The Intermunicipal Association for IT and Organisational Resource Sharingi (iMio)[29] is also a relevant example of collaboration between technological SMEs and open source communities, including the Odoo and Plone ecosystems.

All in all, this cluster reflects different pathways to OSS ecosystem development rather than a single common model.

Cluster D – "Emerging Ecosystems" scores relatively low across all three dimensions. Capacity is especially low (0.00–0.19), Intensity is also limited (0.09–0.30), and Connectedness remains modest (0.10–0.31). The qualitative evidence from the OSOR shows that these aggregate patterns coexist with specific but limited OSS communities and initiatives that sometimes are driven by other Member States.

Italy, for instance, participates in OpenEuroLLM[30], a cross-country consortium developing open source multilingual large language models, coordinated from Czechia. **Greece** and **Romania** participate as partners in the international Consul Democracy[31] ecosystem, an open source digital platform for citizen participation. Greece also hosts initiatives such as FOSSBot, an open source educational robotics project.

These cases suggest that the relatively low scores of Cluster D should not be interpreted as an absence of OSS activity, but in this cluster, OSS activity appears more selective and project-specific than broadly reflected across the three quantitative dimensions. While the mentioned initiatives do not directly explain the Connectedness scores, they illustrate mechanisms through which international integration can develop independently of the size of the domestic developer base.

Other sources beyond GitHub have been analysed to identify geographical patterns in open source activity, providing useful external points of comparison: Cloudflare[32] data on Linux desktop adoption place Finland and the Netherlands among the leading European countries, while the FOSS4G

---

25 SPOIWO - Alliance of Friends of Open and Free Software

26 PLLuM - Polish Large Language Model

27 СИГМА — Платформа за прозрачност на обществените поръчки

28 FOSDEM 2026 - Home

29 Intercommunale de Mutualisation informatique et organisationnelle — iMio

30 OpenEuroLLM

31 About us – CONSUL DEMOCRACY

32 Worldwide Overview | Cloudflare Radar

Observatory[33], which identified 5,714 European contributors to open source geospatial projects, shows Finland, Estonia, the Netherlands and Denmark among the top six countries when contributors are normalised by population. Similarly, according to European TechMap[34] data, Luxembourg, Estonia and the Netherlands record the highest numbers of identified open source companies per capita. The State of Public Code 2026 report[35], based on Software Heritage data, provides further complementary evidence: the Netherlands records the highest share of AI-related projects within government-associated open source activity. However, these sources also reveal differences across dimensions of OSS activity. Germany and France, for example, exhibit substantial open source activity despite belonging to different clusters. Overall, although these sources differ substantially in scope, methodology and coverage and are therefore not directly comparable, their results provide some external support for the recurrence of countries from Cluster A among Europe's relatively strong open source ecosystems.

At the same time, the comparison is not uniform across countries or dimensions: Germany, for example, emerges strongly in many of the external sources analysed but emerges in our analysis primarily by its high international Connectedness rather than by an exceptionally high developer Capacity. These differences highlight the value of considering multiple dimensions of OSS activity rather than interpreting ecosystem strength through a single aggregate measure.

3.3.2. Comparison with non-EU countries

To place the EU-27 results in a broader international context, the analysis was extended to a set of comparator countries (taking into account a combination of geographical relevance to EU and the relative weight of these countries in the global GitHub ecosystem): the United States, India, the United Kingdom, China, Japan, South Korea, Singapore, Hong Kong, Switzerland, and Norway. To ensure comparability with the original EU-27 results, the normalisation of the underlying indicators was anchored to the EU-27 distribution. Specifically, the minimum and maximum values used to construct the normalised indicators were estimated exclusively from the EU-27 sample. The same normalization parameters were then applied to the comparator countries.

As a result, scores of EU Member States remain unchanged relative to the EU-27 analysis, while the scores of comparator countries indicate their position relative to the EU range. Comparator country* values may therefore fall outside the 0–1 interval. The comparators were assigned to the existing EU-27 cluster using a k-nearest neighbours (KNN) classification approach (**Table 4**). Distance-weighted classification was applied so that closer EU-27 neighbours had greater influence on the resulting assignment. This approach preserves the original EU-27 cluster structure while positioning the international comparators according to their similarity to observed European profiles.

[33] FOSS4G Observatory

[34] Map of European Tech Companies | European Tech Map

[35] The State of Public Code

Table 4. Clustering of comparison countries and heatmap of the Capacity, Intensity and Connectedness scores

Country	Cluster	Capacity score	Intensity score	Connectedness score
United States	A - Developer driven	0.72	0.33	0.56
Hong Kong	A - Developer driven	5.06	0.63	0.22
Norway	A - Developer driven	0.67	0.78	0.84
Singapore	A - Developer driven	3.60	0.76	0.33
Switzerland	B - Internationally connected	0.60	0.97	2.08
United Kingdom	B - Internationally connected	0.55	0.29	0.63
South Korea	C - Mixed-profiles	0.31	1.17	-0.32
China	D - Emerging ecosystem	-0.29	-0.54	-0.37
India	D - Emerging ecosystem	-0.18	0.41	-0.28
Japan	D - Emerging ecosystem	0.12	0.26	-0.11

Source: JRC

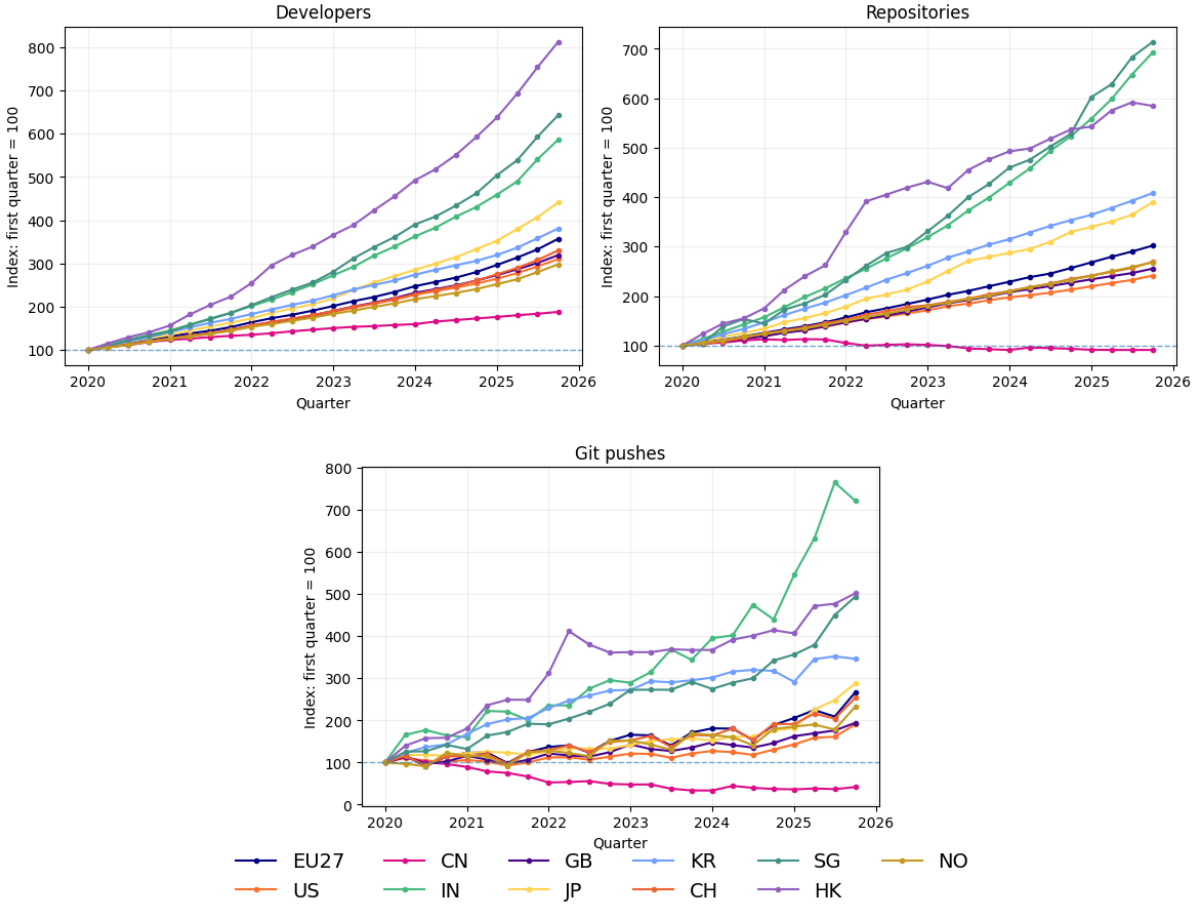
Hong Kong, **Norway**, **Singapore**, and the **United States** are assigned to *Cluster A – "Developer-driven Ecosystems"*, indicating similarity to EU countries characterised by good scores in all the dimensions. Norway displays a relatively strong and balanced profile, while Hong Kong and Singapore stand out for their exceptionally high Capacity. The United States presents a less extreme and more balanced profile. These patterns may reflect different structural characteristics of the countries. The US score may partly result from the scale and concentration of major technology companies involved in OSS development. Singapore and Hong Kong's high Capacity may reflect their role as international technology hubs attracting firms and developers, particularly relative to their small populations.

Switzerland and the **United Kingdom** are assigned to *Cluster B – "Internationally connected Ecosystems"*, reflecting their similarity to EU countries characterised particularly by stronger Connectedness. One possible explanation, requiring further investigation, relates to them being positioned outside the EU while remaining closely integrated with the European economy. This may translate into a high volume of cross-border interactions with EU developer communities.

South Korea is assigned to *Cluster C – "Mixed-profile Ecosystems"*, although its profile is difficult to compare directly with those observed within the EU-27. It combines exceptionally high Intensity with moderate Capacity and low Connectedness, making it a relatively distinctive case that does not fit neatly within the existing EU-derived typology.

China, **India**, and **Japan** are assigned to *Cluster D – "Emerging Ecosystems"*, corresponding to the comparatively lower-scoring EU profile. China is below the EU-27 range across all three dimensions. This is somehow reflected also in the evolution of the four main observed dimensions over the years (**Figure 20**):

Figure 20. Evolution of GitHub indicators in the EU and selected comparator countries (2020–2025)



Source: JRC

It is important to remind here that GitHub is not the only platform for Git-based version control. This is particularly evident in China, where a plausible explanation for the decline in traffic across all the dimensions observed above (in green) is the growing adoption of domestic Git hosting platforms such as Gitee[36] and the removal of repositories. This trend intensified after the geopolitical tensions with the United States and the 2019 sanctions against Huawei, which raised concerns that Chinese developers could lose access to foreign platforms such as GitHub (Pannier, 2022). Similar considerations may also apply in the European context, where some public administrations are exploring alternatives to GitHub, also through public procurement practices that may encourage the adoption of alternative platforms.[37]

Such concerns are relevant, given that GitHub itself notes that Specially Designated Nationals (SDNs), other denied or blocked parties under U.S. and other applicable law, and certain government officials, may be restricted from accessing or using GitHub.com[38].

36 https://gitee.com/

37 New paper on open source progress and trends published | Interoperable Europe Portal

38 GitHub and Trade Controls - GitHub Docs

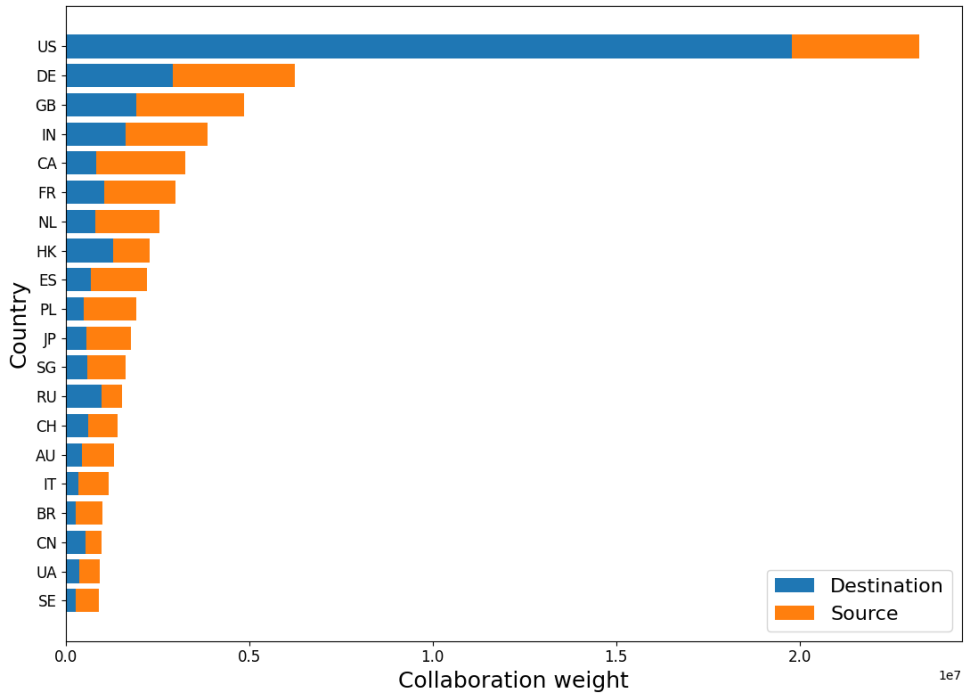
3.4. Interaction between GitHub communities in Europe and globally

This subsection observes more in detail the collaboration dynamics among countries with the highest total collaboration weight in 2025, **distinguishing between their roles as sources and destinations of collaboration in terms of git pushes and pull requests**. In practical terms, a source country represents where contributions originate (based on the location of the developer) and a destination country represents where the receiving OSS projects are based. These results differ from those obtained in paragraph 3.3.1 for the Connectedness score because the two measures capture different dimensions of international collaboration. The Connectedness score normalizes collaboration by the size of each country's developer community, allowing ecosystems of different sizes to be compared. By contrast, the analysis presented here considers absolute collaboration weights, as the objective is **to identify where the overall volume of international open source collaboration tracked by GitHub is concentrated**. Collaboration is measured by aggregating pushes and pull requests made by developers to repositories attributed to a different country. A country acts as a source when its developers contribute to repositories attributed to other countries, and as a destination when repositories attributed to it receive contributions from developers located abroad.

3.4.1. Countries by collaboration weight

While looking at the top 20 countries by collaboration weight, the **United States account for by far the largest collaboration weight and act predominantly as a destination** (see **Figure 21**), **suggesting that a substantial share of global OSS contributions on GitHub flows towards projects based in the US**. Germany ranks a distant second and displays a more balanced combination of source and destination links, followed by the United Kingdom and India. Among EU Member States, Germany, France, the Netherlands, Spain, Poland, and Italy appear among the leading countries, although at substantially lower levels than the United States. Several non-EU countries, including Hong Kong, Japan, Singapore, Switzerland, Canada, and Australia, also occupy visible positions in the international collaboration network. Some countries are predominantly recipients of collaboration links, while others exhibit a comparatively stronger outward collaboration component.

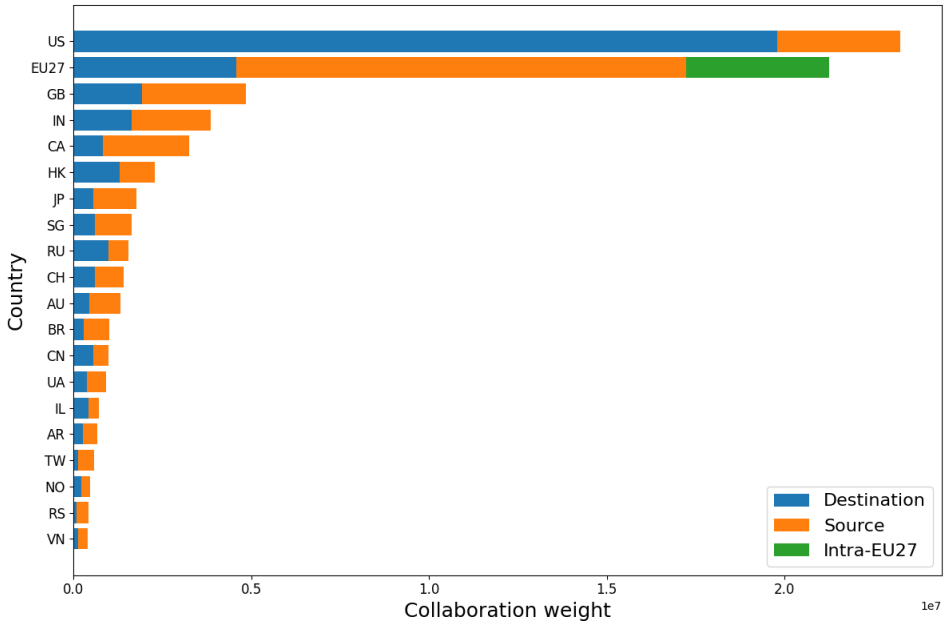
Figure 21. Top 20 countries by collaboration weight (EU27 disaggregated), 2025



Source: JRC

The picture changes when the EU27 is considered as a single aggregate and compared with the rest of the world (see **Figure 22**):

Figure 22. Top 20 countries by collaboration weight (EU27 aggregated), 2025



Source: JRC

For the EU27 aggregate, interactions between Member States were retained, as they represent relevant collaboration within the European ecosystem. The resulting EU27 total therefore comprises

intra-EU27 collaboration, counted once, plus incoming and outgoing collaboration with non-EU27 countries.

As shown in the Figure above, **when considered as a single entity, the European Union exhibits a relevant weight of GitHub interactions**. An important point to note, however, is that although it ranks second in terms of total weight, it remains far behind the United States as a destination for interactions, while functioning primarily as a source. In fact, all of the countries display a relatively balanced pattern between being the source and the destination of collaboration requests, with the notable exception of the United States, which is predominantly a destination, and **Hong Kong, Russia and China, which are the only countries where incoming activity exceed outgoing activity**. One possible explanation relates to the GitHub's data geographical attribution: globally distributed repositories may be attributed to the United States when US-members constitute the largest national group in terms of statistical modal location. Contributions from developers located elsewhere (including those working for the same organisations) would then appear as incoming interactions to the US.

3.4.2. Cooperation patterns

Figure 23. Top 20 countries by GitHub international collaboration with top 5 partnerships (EU-27 aggregated), 2025

Country	Total interactions	Top outgoing					Top incoming				
US	23,254,682	EU27	IN	GB	HK	CA	EU27	CA	GB	IN	AU
EU27	17,226,088	US	GB	RU	IN	CH	US	GB	IN	RU	CH
GB	4,854,127	US	EU27	IN	CA	RU	EU27	US	IN	CA	AU
IN	3,859,737	US	EU27	GB	CA	IL	EU27	US	GB	CA	UA
CA	3,267,795	US	EU27	IN	GB	HK	US	EU27	IN	GB	AU
HK	2,299,484	US	CN	SG	JP	EU27	US	JP	SG	CN	TW
JP	1,779,494	US	HK	EU27	CN	SG	US	HK	EU27	SG	CN
SG	1,642,921	US	HK	CN	JP	EU27	HK	US	JP	CN	EU27
RU	1,543,888	EU27	US	KZ	GB	BY	EU27	US	GB	RS	KZ
CH	1,416,284	US	EU27	GB	IN	RU	EU27	US	GB	IN	CA
AU	1,329,406	US	EU27	GB	CA	IN	EU27	US	NZ	GB	IN
BR	1,016,000	US	EU27	IN	GB	AR	EU27	US	CA	IN	AR
CN	989,389	HK	US	SG	JP	TW	HK	US	JP	SG	TW
UA	921,606	US	EU27	IN	RU	GB	EU27	US	GB	CA	BR
IL	720,639	US	EU27	IN	GB	RU	EU27	US	IN	GB	UA
AR	662,303	US	EU27	GB	CO	IN	EU27	US	CO	BR	GB
TW	592,669	US	HK	CN	EU27	SG	US	HK	JP	CN	SG
NO	466,072	US	EU27	GB	CA	RU	EU27	GB	US	IN	NP
RS	417,975	US	EU27	RU	GB	IN	EU27	US	BR	RU	BA
VN	405,009	US	EU27	SG	JP	IN	EU27	SG	US	JP	PH

Europe North America South America Asia Oceania

Source: JRC

Figure 24 Top 20 countries by GitHub International Collaboration with top 5 partnerships, 2025

Country	Total interactions	Top outgoing	Top incoming
US	23,254,682	IN DE GB HK CA	CA GB DE IN FR
DE	6,251,779	US GB RU FR IN	US GB FR NL ES
GB	4,854,127	US DE IN FR NL	US DE FR NL ES
IN	3,859,737	US DE GB BE CA	US DE GB CA ES
CA	3,267,795	US DE IN GB FR	US DE IN GB FR
FR	2,988,544	US DE GB CH IN	US DE GB ES NL
NL	2,557,987	US DE RU GB IN	DE US RU GB ES
HK	2,299,484	US CN SG JP TW	US JP SG CN TW
ES	2,224,872	US DE GB IN FR	US DE GB FR NL
PL	1,932,822	US DE GB UA IN	US DE UA GB ES
JP	1,779,494	US HK CN SG DE	US HK SG CN TW
SG	1,642,921	US HK CN JP IN	HK US JP CN TW
RU	1,543,888	US DE NL KZ FI	NL DE US FI GB
CH	1,416,284	US DE FR GB IN	DE FR US IT GB
AU	1,329,406	US GB DE CA IN	US NZ GB IN DE
IT	1,176,135	US DE GB CH FR	US DE GB FR ES
BR	1,016,000	US DE IN GB FR	US PL DE PT CA
CN	989,389	HK US SG JP TW	HK US JP SG TW
UA	921,606	US DE IN PL RU	PL DE US ES NL
SE	897,640	US DE GB RU NO	US DE GB DK FR

Europe North America South America Asia Oceania

Source: JRC

In the previous section the total weight of GitHub incoming and outgoing interactions between countries has been observed, but it is now interesting to link that weight to the geographical source of the requests. **Figure 23** provides an overview for each of the 20 countries which presented the highest amount of collaboration requests (with EU-27 aggregate weight), providing for each of them the 5 top partners in terms of outgoing and incoming collaboration requests, according to the data observed.

The figure suggests a **strongly international but highly concentrated collaboration structure, dominated by the United States and characterized by substantial integration among European countries**.

The US is the dominant hub by a very large margin. With more than 23 million interactions, it surpass by 5 million the volume of EU-27, the second-ranked economy. They appear among the leading outgoing and incoming partners of almost every other country. This suggests that international GitHub collaboration is organized around a strong US-centered, and partially EU-centered hub, rather than being evenly distributed across countries.

Asia shows a somewhat different regional structure. Hong Kong, Japan, Singapore and China have strong links with one another, alongside substantial interaction with the US. This suggests a recognizable Asian collaboration cluster embedded within a broader US-centered network.

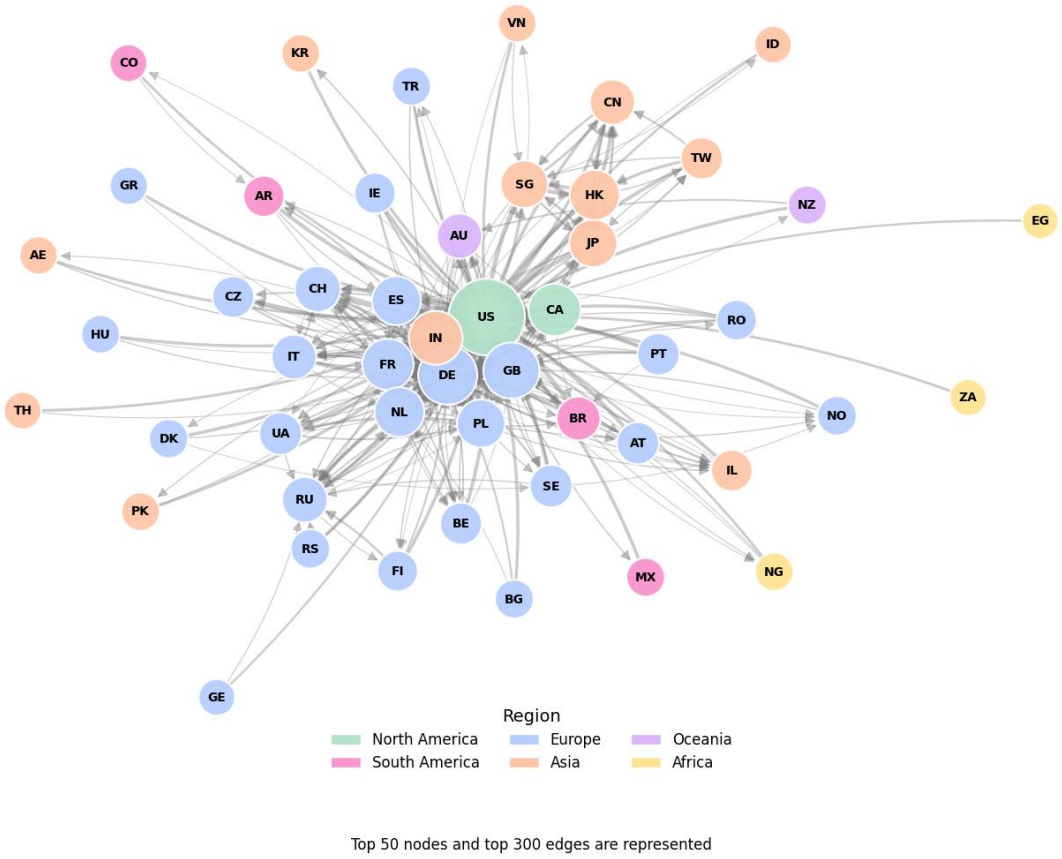
A more complete picture is provided by observing the global top 20 countries' interactions considering the single EU-27 countries (**Figure 24**).

Germany results the second country per wight of interactions, right after the United States. For countries such as Germany, France, Spain, Italy, Switzerland and Sweden, the leading partners include several other European countries, indicating substantial regional integration. At the same time, the US is generally their first or one of their most important partners.

Both the figures highlight **the EU-27 as second major pole of interaction of international GitHub collaboration, after United States. A strong reciprocal relationship between the two poles is particularly evident.** European collaboration is simultaneously intra-European and transatlantic, with the United States dominating for both outgoing and incoming collaborations, but also a strong presence of India and United Kingdom.

These findings are reflected also in the following visualization (**Figure 25**), which, in order to better identify geographical interactions, represents the top 50 nodes by collaboration volume and the top 300 edges by number of interactions.

Figure 25. International GitHub collaboration network, 2025

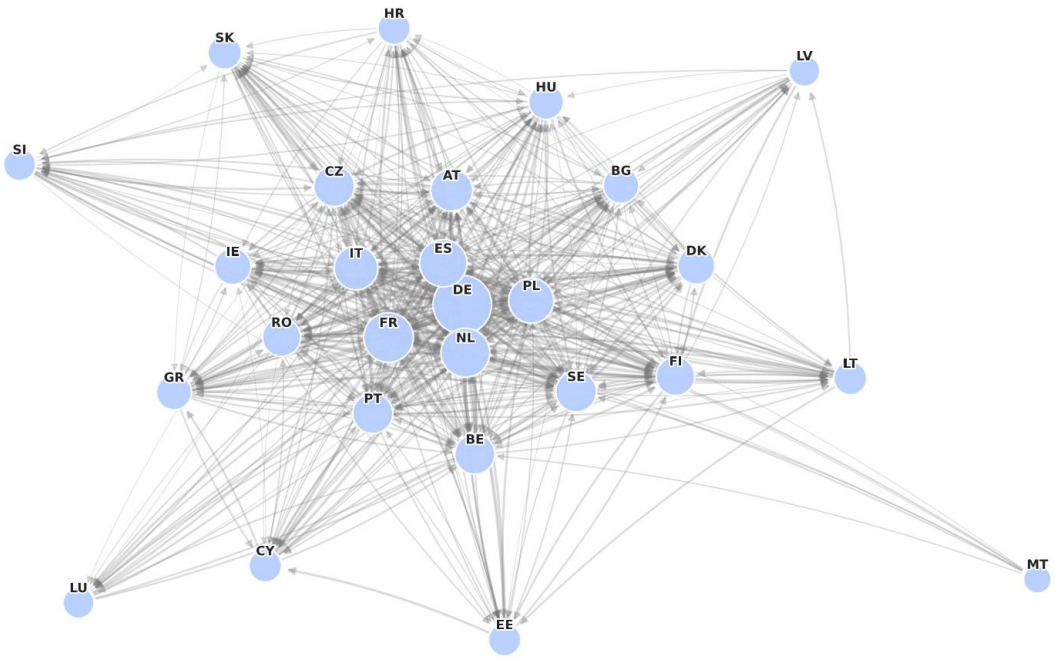


Source: JRC

The figure highlights the highly concentrated international GitHub collaboration network, with the United States acting as the dominant global hub. India, Germany, and the United Kingdom also occupy central positions, reflecting their strong integration into international collaboration flows. European countries (including here both EU and non-EU countries) form a dense and interconnected core, while distinct geographical clusters are also visible at the network's periphery, including a group of Eastern Asian countries and another one of Eastern European countries. Some of the international collaborations might reflect the fact that, despite the common beliefs that OSS collaboration can overcome geographical barriers, cultural affinities and shared historical experiences can be observed in the interactions between countries (Xu et al., 2025).

Considering the EU-27 dimension (**Figure 26**), the results show Germany clearly occupying the central position as the leading incoming or outgoing partner for most Member States. France and the Netherlands form a second tier of major collaboration hubs, followed by Spain and Poland. Smaller Member States tend to concentrate their interactions around these larger countries. Malta, Luxembourg, Latvia, and Cyprus are in fact located more toward the network periphery and display lower overall collaboration volumes.

Figure 26. EU-27 GitHub collaboration network, 2025



Source: JRC

Overall, the network indicates a strongly interconnected but uneven EU collaboration ecosystem, characterized by a dense central core and a less-connected periphery within the EU27 GitHub collaboration network.

The intra-EU network provides a complementary view of the Connectedness dimension, showing the absolute volume and structure of collaboration among Member States. Several countries belonging to the developer-driven (Cluster A) and internationally connected (Cluster B) clusters

appear strongly integrated into the network. However, in this figure the weights are not normalised by the number of developers, so the figure highlights only the overall scale of cross-border interactions.

3.5. Conclusions

The analysis identifies different geographical patterns in the OSS ecosystems captured by GitHub data, complemented by qualitative evidence from OSOR. These patterns should not be interpreted as a comprehensive assessment or ranking of national OSS performance. Not all activity on GitHub necessarily qualifies as open source, and GitHub itself captures only part of the broader OSS ecosystem. The indicators should therefore be understood as proxies for different dimensions of OSS development and collaboration.

Nevertheless, comparison with other geographically disaggregated sources provides some external support for the patterns identified. This is particularly evident for countries such as **the Netherlands, Finland, Estonia and Sweden, which repeatedly emerge as relatively strong OSS ecosystems**. At the same time, the analysis shows that this strength can take different forms: a large and active developer base, strong international integration, or different combinations of these dimensions. This suggests that there is no single pathway towards a strong OSS ecosystem and that policy interventions should take these different starting conditions into account.

From a digital-sovereignty perspective, the results suggest that **European OSS capacity should be considered not only in terms of the availability of open technologies, but also in terms of the capacity to develop, maintain and collaborate around them**. The combination of these dimensions can therefore contribute to reducing technological dependencies while preserving the benefits of participation in global open source networks.

The qualitative evidence also points to the **public sector as a potential driver of OSS ecosystem development**. Examples such as Germany's Sovereign Tech Fund, Estonia and Finland's cooperation around X-Road, and Germany and Austria's cooperation around openDesk illustrate different ways in which public intervention can support domestic capabilities while simultaneously strengthening European and international collaboration. These examples do not establish a causal relationship with the quantitative indicators, but they suggest mechanisms that warrant further investigation.

Finally, the comparison with non-EU countries demonstrates an important limitation of platform-specific measurement: **countries might be developing alternative infrastructure** and appear weaker when observed exclusively through GitHub. More broadly, it raises a strategic question for Europe concerning the appropriate balance between developing sovereign OSS infrastructure and remaining deeply integrated into global development communities.

Policy considerations

The results also suggest that a differentiated approach to public support may be more appropriate than uniform interventions across Member States. Given the concentration of commercial OSS

venture capital in the United States[39], strategically targeted European public investment could play an important role in strengthening areas where market investment alone may be insufficient. Identifying countries according to their Capacity, Intensity and Connectedness can help reveal existing strengths, complementarities and gaps across the EU. Rather than applying uniform interventions across Member States, public (including EU) investment could therefore be tailored to different ecosystem profiles to increase efficiency.

Once further validated, the cluster typology could therefore be used to construct and test policy directions. Rather than treating the clusters as fixed categories, such scenarios could ask how targeted interventions might change countries' ecosystem profiles.

In this perspective, the preliminary cluster profiles suggest different policy directions (see **Table 5**)

Table 5. Possible policy directions for each OSS cluster

Cluster	Ecosystem profile	Possible policy direction	Strategic objective
A – Developer-driven ecosystems	High Capacity and Intensity, with generally solid Connectedness	Support maintainers, scaling of successful projects and greater international reach	Consolidate strong domestic ecosystems and increase their European and global influence and export EU good practices
B – Internationally connected ecosystems	High Connectedness despite medium-low Capacity and mostly moderate Intensity	Use international networks to support domestic projects, maintainers and developer communities	Export EU good practices in initiatives towards international Connectedness
C – Mixed-profile ecosystems	Different combinations of Capacity, Intensity and Connectedness	Target the specific bottleneck identified in each national ecosystem rather than applying a uniform intervention	Build on existing strengths while addressing country-specific gaps
D – Emerging ecosystems	Relatively low Capacity, Intensity and Connectedness	Strengthen skills, developer communities, OSS adoption and contribution, and institutional and private-sector participation	Expand the domestic OSS base while providing an opportunity to pilot and scale training, capacity-building and other measures to support the ecosystem

Source: JRC

These scenarios should be understood as hypotheses for further analysis rather than policy prescriptions. Their value lies in providing a framework for examining how different forms of intervention could affect the components of an OSS ecosystem and where complementarities between Member States could be exploited.

Future work

This analysis is preliminary and exploratory, with the primary aim of demonstrating the value of identifying patterns that could inform future investment and policies to strengthen European OSS

[39] 65% of venture capital investment in commercial open source companies still goes to the United States (European Parliament, 2025)

ecosystems. Its main limitation is the reliance on GitHub as the principal quantitative source and on OSOR for much of the qualitative contextualisation.

Preliminary work has already explored other OSS-related data sources (including GitLab[40], Stack Overflow[41], Censys[42], Cloudflare[43], FOSS4G[44]) which could provide a more comprehensive representation of OSS ecosystems and reduce potential platform-specific biases.

A second direction for future work is to relate the identified profiles to broader socioeconomic, institutional and digital conditions. Potential indicators include GDP per capita, R&D expenditure, internet use, digital skills, STEM graduates, ICT specialists and regulatory quality. These variables could be used first to investigate whether contextual conditions are systematically associated with Capacity, Intensity or Connectedness. Where meaningful relationships emerge, they could subsequently inform an extended clustering framework.

Finally, the qualitative analysis should be expanded systematically to investigate which mechanisms may explain the quantitative patterns and the types of intervention that can strengthen European technological capacity and digital sovereignty.

40 REST API | GitLab Docs

41 Stack Overflow Survey - OECD.AI

42 Censys | The Authority for Internet Intelligence and Insights

43 Data Explorer | Cloudflare Radar

44 FOSS4G Observatory

4. From research to scale-up: insights from the Cloud computing and Data Technologies domain

4.1. Introduction: the DGTES approach

The metrics presented in this chapter focus on three fundamental layers of the digital ecosystem value chain that go from knowledge creation to market technology development. It comprises the sequence of research, innovation and business activities through which scientific knowledge of different technological domains is transformable into market-ready firms. By analysing emerging and strategic digital technologies, this framework allows mapping gaps and bottlenecks at different stages, highlighting EU strengths and dependencies.

Digital sovereignty is understood here not as technological self-sufficiency, but as the capacity to sustain and scale critical digital capabilities in line with European interests within an open global ecosystem. Accordingly, cross-border collaboration, co-invention and foreign investment are not treated as vulnerabilities per se. They become sovereignty-relevant only when they are combined with limited domestic capabilities, strong concentration on a small number of external partners, or persistent asymmetries that reduce the EU's room for manoeuvre across the research-to-scale-up chain.

The JRC's **Digital Techno-Economic ecoSystem (DGTES)** analytical approach allows mapping and exploring the complex dynamics of industry segments driven by rapidly evolving emerging technologies, which are challenging to characterise through traditional metrics or classifications (Calza et al., 2022, 2023). Based on micro-level data sources, the approach builds a network of players and activities connected through collaborative relations (**Figure 27**).[45] In this chapter, a player is defined as an organisation (academic institution, government body, or firm) that conducts research, innovates or runs a business related to the digital industry. These represent the research, (patent-driven) innovation and business activities of the ecosystem. Collaborations arise as players co-author, co-patent, or invest in the business, and represent the edges of the DGTES network. These connections are not limited to one geography but can also happen across borders: for instance, when foreign investors fund domestic businesses or two players file together an application for an invention.

[45] The methodology employs the following micro-level data sources: Scopus, EPO Patstat, Cordis, Moody's Orbis, Standard & Poor Capital IQ, Dealroom, Crunchbase, Pitchbook, and DowJones.

Figure 28. The DGTES analytical approach applied to measure EU's digital strengths and dependencies from research to scale-up.



Source: JRC

Thus, DGTES allows to analyse the roles of entities and regions are at the forefront of the different technologies and to the extent of the EU's involvement in comparison to other global regions. In the framework of the current study, we exploit these networks of research, innovation and business, and generate a series of indicators to analyse the competitiveness of the EU and the foreign dependencies in the digital ecosystem. In particular, the analysis develops and computes metrics to identify strategic dependencies in four areas:

— **research**, providing indicators on the number of scientific publications, degree of internationalisation and foreign collaborations of countries and geographical areas in the research realm in each technology domain;

— **innovation**, providing indicators on the number of patents filed, degree of internationalisation and foreign collaborations of countries and geographical areas in the innovation realm in each technology domain;

— **startups**, computing indicators that grasp the dynamics in the early stages of investment of startups, including the number of venture capital (VC) deals and their average size across geographical areas and investors;

— **scaleups,** computing indicators that grasp the dynamics in the late stage of funding of startups, once they grow, including the number of VC and private equity (PE) deals and their average size across geographical areas and investors

Covering the period 2009–2025, the analysis focuses on the EU while accounting for the roles of major global players. The technological scope includes the following domains: AI and GenAI; Cloud Computing and Data; Cybersecurity; Robotics; Semiconductors; Advanced computing and Quantum.

4.2. Insights: an analysis of Cloud Computing and Data Technologies

This section presents the selection of metrics by defining and applying them to the domain of **Cloud Computing and Data Technologies**. The aim is to get insights into the presence of possible foreign dependencies along the journey from research and innovation to venture funding and scaling of startups.

The proposed metrics (**Table 5**, **Table 7** and **Table 9**) include both a view on the volume of the (research, innovation, or investment) activity and the collaboration across borders to identify potential dependencies. The insights presented for each stage are drawn from the associated metrics computed on the whole DGTES ecosystem introduced in Section 1.1; the activity of each stage is captured through specific sources of data used in DGTES, as explained in each of the following subsections. These metrics represent an example of the type of insights that can be computed through the DGTES approach, which covers a broader set of technological domains over the digital ecosystem.

4.2.1. Research

Four main indicators have been defined for the analysis of research trends (**Table 5**).

The first two indicators (**share of research activities** and **number of research activities by year**) highlight the share of EU scientific publications *vis à vis* other geographical areas, both considering the whole analysis timeframe (2009-2025) as well as each year. By measuring the scale of a geographical areas' research output, they allow understanding which global players are strong in research by the size of their knowledge base or their capacity to generate scientific output at scale and how this position has evolved over time.

The third indicator (**research activities per capita**) is useful to measure the research intensity independently of the population size. This metric helps removing the advantage of large countries like China that produces a huge number of publications that appear to have a lower impact if re-sized considering its population.

While the first three indicators highlight the situation of each global player as standalone, the fourth one (**affinity matrix: research**) introduces the layer of collaborations between players, computing for each of them a bilateral affinity index with the share of collaborative publications

with each of the other global players. A high share of collaborations could be seen both under positive and negative lenses: if on one side having a collaborative network is for sure good for scientific excellence, it might also lead to possible dependencies from other global players.

All indicators are computed using Scopus data, Elsevier's multidisciplinary abstract and citation database. The DGTES curated list of keywords is run over a the text of a selection of around 150 journals around digital topics.

Table 6. Research metrics

Metric	Description
Share of research activities	EU share in total number of scientific publications in academic journals by technology areas *vis à vis* other geographical areas. An activity shared across more than one geographical area (i.e. owing to co-authorship) counts as 1 / n (where n = total number of players involved in the activity) for each player. An activity shared across more than one technological domain (i.e. having keywords linked to multiple technologies) counts as 1 / d (where d = total number of technologies linked to the activity) for each technological domain.
Number of research activities by year	Number of EU scientific publications in academic journals by technology areas by year *vis à vis* other geographical areas. An activity shared across more than one geographical area (i.e. owing to co-authorship) counts as 1 / n (where n = total number of players involved in the activity) for each player. An activity shared across more than one technological domain (i.e. having keywords linked to multiple technologies) counts as 1 / d (where d = total number of technologies linked to the activity) for each technological domain.
Research activities per capita	EU number of research activities for every million inhabitants by technology areas *vis à vis* other geographical areas.
Affinity matrix: research	EU's bilateral research collaboration with major global partners across the selected technological domains. It consists of two sub-indicators: i) The share of joint research activities (co-authored scientific publications) between the EU and a partner country, expressed as a proportion of all EU research activities (collaborative and non-collaborative ones); and ii) the same share expressed as a proportion of all research activities of the partner country (collaborative and non-collaborative ones).

Source: JRC

The **findings** in the Cloud and Computing and Data Technologies domain show that **EU-based authors contributed 22% of scientific publications between 2009 and 2025, with most foreign co-authors based in the US and China.**

This is almost the same share as China, that has been recently catching up and cumulated the highest number of scientific publications in 2025, challenging EU's historical leadership. The EU and US have been publishing a similar number of research articles annually, but since 2017 the gap began to widen, with the US accounting for 18% of global publications during the considered period (**Figure 28**). Still, in per capita terms, the US showed a clear advantage over the EU, both well above China. Research connections are useful to unveil potential asymmetries in collaboration patterns. For EU publications, 13% show a US-coauthor, 10% a Chinese co-author, and 9% a UK co-author. (**Table 6**). While with the US and China the relationship is balanced (EU authors participate in 15% of US publications and 9% of Chinese publications), there is an imbalance with the UK as 31% of UK publications have at least one EU co-author.

Figure 29. Share of research activities (left), number of research activities by year (centre), research activities per capita (right) in cloud computing and data technologies



Source: DGTES database.

Table 7. Affinity matrix: research in cloud computing and data technologies

Publications with authors from	Share with at least one co-author from: EU	US	CN	UK
EU	100%	13%	10%	9%
US	15%	100%	23%	4%
CN	9%	18%	100%	6%
UK	31%	12%	20%	100%

Source: DGTES database.

4.2.2. Innovation

Similarly to what proposed for the research trends, four indicators have been defined for the innovation stage (see **Table 7**) to reflect dependency interrelations regarding patent applications, and bilateral collaboration in innovation activities.

The first two indicators (**share of innovation activities** and **number of innovation activities by year**) highlight the share of EU priority patent applications *vis à vis* other geographical areas, both considering the whole analysis timeframe (2009-2025) as well as each year. By capturing the scale of inventive activity, they allow to understand which global players are strong in innovation in a technology given their patent portfolio and how this position has evolved over time.

The third indicator (**innovation activities per capita**) measures patenting intensity relative to the population size. It helps distinguish if a high volume of patents reflects an innovation-driven ecosystem or the scale of the country. This metric is particularly useful to rescale the activity of a player like China that produces a huge number of patent applications reflecting its sustained R&D investments but also industrial policies promoting innovation in strategic technologies.

While the first three indicators highlight the situation of each global player as standalone, the fourth one (**affinity matrix: innovation**) introduces the layer of collaborations between players, computing for each of them a bilateral affinity index with the share of collaborative priority patent application with each of the other global players. A high share of collaborations could be seen both under positive and negative lenses: if on one side having a collaborative network is for sure good for innovation excellence, it might also lead to possible dependencies from other global players.

All indicators are computed using Patstat data, the European Patent Office's Worldwide Patent Statistical Database.

Table 8. Innovation metrics

Metric	Description
Share of innovation activities	EU share in total number of priority patent applications by technological domains *vis à vis* other geographical areas. An activity shared across more than one geographical area (i.e. owing to co-application) counts as 1 / n (where n = total number of players involved in the activity) for each player. An activity shared across more than one technological domain (i.e. having keywords linked to multiple technologies) counts as 1 / d (where d = total number of technologies linked to the activity) for each technological domain.
Number of innovation activities by year	Number of priority patent applications by technological domains by year *vis à vis* other geographical areas. An activity shared across more than one geographical area (i.e. owing to co-application) counts as 1 / n (where n = total number of players involved in the activity) for each player. An activity shared across more than one technological domain (i.e. having keywords linked to multiple technologies) counts as 1 / d (where d = total number of technologies linked to the activity) for each technological domain.
Innovation activities per capita	EU number of innovation activities for every million inhabitants by technology areas *vis à vis* other geographical areas.
Affinity matrix: innovation	EU's bilateral innovation collaboration with major global partners across the selected technological domains. It consists of two sub-indicators: i) The share of joint innovation activities (co-application of patents) between the EU and a partner country, expressed as a proportion of all EU innovation activities (collaborative and non-collaborative ones); and ii) the same share expressed as a proportion of all innovation activities of the partner country (collaborative and non-collaborative ones).

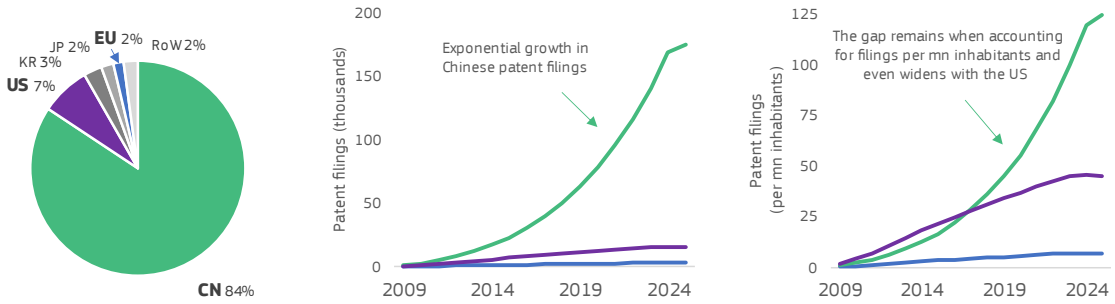
Source: JRC.

The main **findings** in the Cloud and Computing and Data Technologies domain show that **during the 2009-2025 period, only 2% of global patent filings involved at least an EU applicant, with a widening gap with both China and the US.**

This is below half the same share for the US and well below the 84% held by Chinese applicants (**Figure 29**). Cloud computing and data technologies patenting activity recorded the fastest acceleration from the mid-2010s onwards, particularly in China, turning the country into the largest source of patent filings by volume in recent years. Chinese applicants filed 55 times more patents in cloud and data technologies than EU applicants over 2009-2025, with a widening gap against the EU and US over the years. Adjusting for population does not change the picture: unlike for scientific publications, the EU remains well behind the US in patenting intensity.

Cross-border collaboration in patenting (through co-applications) is very limited compared to co-authorship of scientific output (**Table 8**). This indicates that knowledge production through inventions is more geographically concentrated within domestic borders, particularly in China. Collaboration weight is, however, asymmetric: US and Chinese applicants are more present in EU patents than EU applicants are in their patent portfolios. The strongest connections for the EU are with China (2.37% of EU filings involved at least a Chinese co-applicant) and the US (1.56%). While only 0.04% of Chinese filings and 0.34% of US filings involve at least an EU applicant. It is crucial for the EU to carefully monitor the evolution of its collaborations with China to avoid becoming overly dependent on Chinese partnerships, which could limit its strategic autonomy in the long run.

Figure 30. Share of innovation activities (left), number of innovation activities by year (centre), innovation activities per capita (right) in cloud computing and data technologies



Source: DGTES database.

Table 9. Affinity matrix: innovation in cloud computing and data technologies

Filings with applicants from	Share with at least one co-applicant from: EU	US	CN	UK
EU	100%	1.56%	2.37%	0.11%
US	0.34%	100%	0.47%	0.02%
CN	0.04%	0.04%	100%	0.00%
UK	0.77%	0.58%	0.19%	100%

Source: DGTES database.

4.2.3. Startups and scaleups insights

Three metrics have been defined for the analysis of startups and scaleup trends (**Table 9**). Together they capture the level of investment activity, the amount of capital funded, and its origin and destination.

The first indicator (**number of venture capital deals by year**) computes the number of venture capital and private equity deals closed by EU-based firms by year *vis à vis* firms in other geographical areas. It is a measure of investment activity and is useful to understand how active different global player are in startup and scaleup financing independently of the size of the deals. Analysing the deals over time provide information on the dynamism of the venture ecosystem

The second indicator (**venture capital funding amount by year**) highlights the amount of venture capital and private equity raised by EU-based firms *vis à vis* firms in other geographical areas. It complements the number of deals by capturing the scale of capital mobilised, identifying which global players attract the highest amount of private funding over time. A growing number of deals doesn't necessarily translate into larger funding volumes, particularly as firms move towards the scale-up phase.

While the first two indicators highlight the situation of each global player as standalone, the third one (**venture capital investment flows**) accounts for the funding through venture capital that flows across geographical areas. It helps identify the extent to which firms reply on domestic or foreign investors. Large cross-border investment flows can provide domestic firms with access to capital to grow and scale their businesses, but might signal exposure to sudden changes in investment plans or policies in foreign countries.

All proposed indicators are computed by investment stages, therefore it is possible to grasp a view both on startups (early investment stages) and scaleups (late investment stages). They are computed using Crunchbase data, a commercial database that records information on private and public companies, investors, and funding rounds.

Table 10. Startup and scaleup metrics

Metric	Description
Number of venture capital deals by year	Total number of venture capital and private equity deals closed by EU-based firms by year *vis à vis* firms in other geographical areas. The metric is broken down by investment stage (startup and scaleup) and by digital technological domain.
Venture capital funding amount by year	Total amount of venture capital and private equity (in EUR) raised by EU-based firms by year *vis à vis* firms in other geographical areas. The metric is broken down by investor's geographical area of residence, investment stage, and by digital technological domain. When more than one investor participated in an investment round, each individual investment is estimated as 1 / n, where n is the number of investors in the round. For comparison, investment stages are 'startup' (angel, seed, and early-VC rounds) and 'scaleup' (late-VC and private equity rounds).
Venture capital investment flows	Bilateral venture capital and private equity flows between the EU and foreign countries. The metric is broken down by investment stage (startup and scaleup) and by technological domain and is composed by two sub-indicators: i) Inward VC and PE measured as the proportion of EU's total VC and PE funding sourced from another country; and ii) outward VC and PE measured as the proportion of the foreign country's total VC and PE funding that originates from the EU. If a firm operates in several technological domains, the amount of funding secured by that firm is allocated proportionally across all relevant domains. When a financing round involves multiple investors, the round's total value is divided equally among the participating investors before being attributed to their respective countries. Hence, this indicator is an estimation of the country-pair financing in each technological domain.

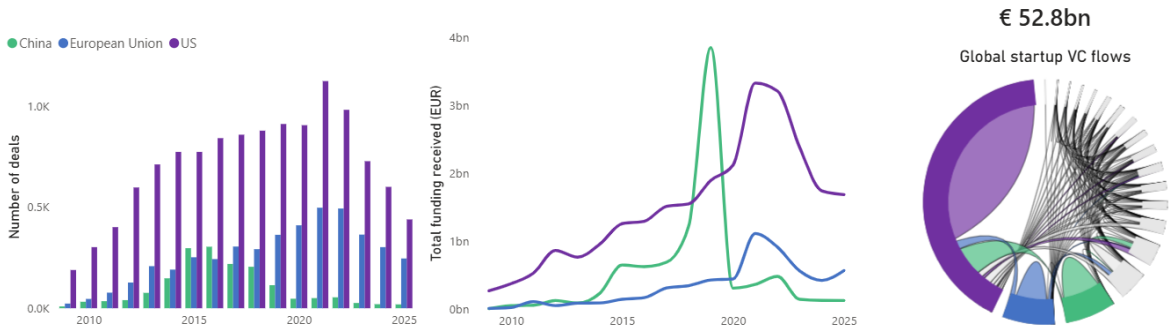
Source: JRC

The **findings** in the Cloud and Computing and Data Technologies domain show that **between 2009 and 2025, EU firms raised over EUR 23 billion in venture funding, mostly from EU investors and foreign investors in the US and UK.**

Although the EU venture market is much smaller than the US market, EU startups receive around two thirds of their funding from domestic investors (**Figure 30** and **Figure 30**, right plots). This domestic share falls sharply as firms scale, with around only one third of EU scaleup funding originating within the EU, indicating a potential dependence on foreign capital at later stages. As firms move towards the scaleup stage, the combination of larger financing needs and limited domestic funding increases the reliance on foreign investors. The US acts as the main foreign venture capital and private equity hub for the EU, and the relationship is highly asymmetric. US investors provide around 18% of the funding received by EU startups, compared with only 2% of US startup funding originating from EU investors. The imbalance appears larger for scaleups: US investors supplied 43% of funding to EU firms, while EU investors provide only 2% of funding received by US scaleups. The UK represents the second largest foreign source and destination of capital in cloud computing and data technologies. UK investors provide 8% of EU startups funding and 19% of EU scaleup funding, while EU investors account for 11% and 9% of funding received by UK startups and scaleups, respectively.

These dependencies coexist with a higher dynamism in the EU venture market (**Figure 29** and **Figure 30**, left and centre plots). EU startup activity is catching up in number of deals but not in funding, while EU scaleups registered fewer deals than the US and face a much wider funding gap. Since the mid-2010s, the number of deals involving EU firms has increased, particularly at the startup stage, though the gap with the US market both in terms of number and amount of deals remains large. In 2025, US startups raised around three times as much capital as EU startups, while US scaleups raised more than twelve times as much as their EU counterparts.

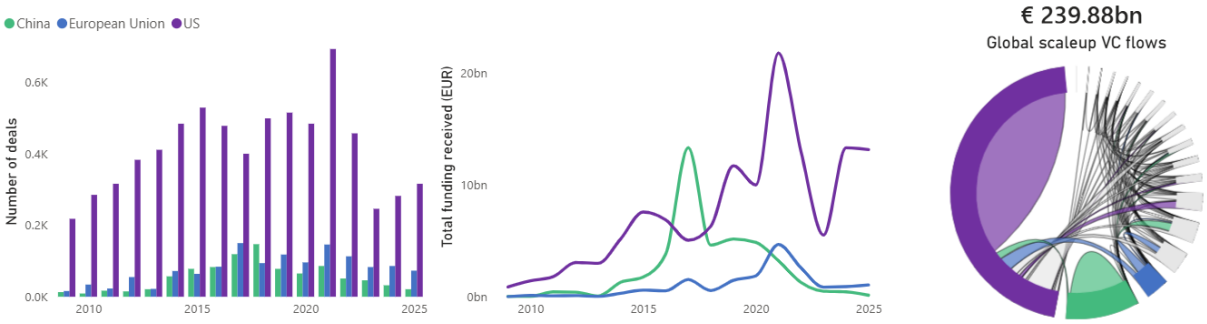
Figure 31. Startups - Number of venture capital deals by year (left), venture capital funding amount by year (centre), venture capital investment flows (right) in cloud computing and data technologies



Source: DGTES database.

Note: Semi-circular arcs represent investment remaining within the same macro-area, while other arcs show the total flows between two selected areas, coloured by the macro-area attracting the larger share of that investment. Source: DGTES database.

Figure 32. Scaleups - Number of venture capital deals by year (left), venture capital funding amount by year (centre), venture capital investment flows (right) in cloud computing and data technologies



Source: DGTES database.

Note: Semi-circular arcs represent investment remaining within the same macro-area, while other arcs show the total flows between two selected areas, coloured by the macro-area attracting the larger share of that investment. Source: DGTES database.

4.3. Conclusions and further development

This chapter shows how the JRC DGTES approach can help assess EU's position and foreign dependencies across the digital ecosystem. Rather than relying on a single measure of technological strength, the framework follows the technological development path that goes from research and

innovation to firm creation and scaleup, combining information on scientific publications, patent filings, and venture capital funding.

The approach provides two complementary perspectives. First, it measures the relative position of the EU and main global players across the technological path. Second, it maps cross-border linkages and their asymmetries, identifying where EU activities involve foreign researchers, innovators, or investors, and whether these relationships are balanced towards both directions. Looking jointly at relative strength and international linkages helps distinguish areas where foreign connections accompany a strong domestic ecosystem from those where they may signal greater external reliance.

From the application of the DGTES approach to measure digital sovereignty on cloud and data technologies domain, it emerges how the EU remains scientifically strong, but its lead is under pressure. **Research** collaboration is an asset, yet sustained competitiveness will require preserving a strong domestic knowledge base and avoiding over-reliance on external partners for critical expertise.

The clearest sovereignty vulnerability that emerges in the value chain is related to **innovation**. The EU's relatively strong research base is not translating into comparable proprietary technological assets, increasing the risk of dependence on foreign-owned innovation and reducing strategic autonomy in key digital technologies. The asymmetry with China is particularly important to monitor.

Concerning startups and scaleups, the results point to **scaleup finance** as a potential source for external dependence. EU firms can emerge domestically, but as capital needs grow they become much more reliant on foreign investors, especially from the US. This can weaken the EU's ability to retain control over the growth, ownership, and strategic direction of critical digital firms.

While the proposed approach offers novel insights across technological domains, its interpretation is **shaped by the coverage and characteristics of the underlying data**. Several extensions could further enrich the analysis.

First, innovation indicators rely on patent data, that are subject to publication lags of around 18 months from the filing date. Figures for the last two years should therefore be interpreted with caution (Pasimeni and Georgakaki, 2020). Aggregating patent activities over longer periods can mitigate this issue, but it remains relevant for annual figures. Second, patents filings provide a comparable measure of inventive activity. But do not capture differences in their technological and economic significance. Citation data, granted patents and international patent families could complement the indicator with information on patent quality and relevance, while accounting for differences in patenting strategies across countries (Dechezleprêtre et al., 2017).

Third, the research-activity data are drawn from a curated collection of roughly 150 digital-focused journals. This improves the relevance of the retrieved publications and keeps the computational feasibility of the analysis as including all journals covered in Scopus could encounter some limitations both from the technical side and on accuracy of results (as non-specifically digital journals might retrieve less pertinent publications).

Fourth, startup and scaleups indicators rely on Crunchbase data, which could be complemented with other data sources such as Dealroom or Pitchbook to increase geographical coverage and provide a robustness check (Berger, M. et al., 2026).

Fifth, the identification of research, innovation and business activities within each technological domain relies on a curated set of keywords. This provides a consistent classification across indicators,

while results depend on the information available in the underlying text fields and on regularly updating these keywords to reflect technological developments.

Finally, activities associated to multiple technologies are assigned equal fractionality across domains. This approach avoids double counting of the activities when aggregating across the digital ecosystem, although it produces lower domain-level totals than approaches based on non-fractional counts.

These extensions would provide avenues to further strengthen the framework while preserving its consistent application across technological domains and geographical areas.

Section C

Digital Products and Markets



5. Corporate Control in Digital Production Networks: Power and Interconnectedness Position

5.1. Approach, methodology and data limitations

While traditional analyses of international trade often focus on import and export flows—a highly relevant topic, analysed in **Chapter 7** of this report—this chapter aims to complement this view by studying the **power and influence that Multinational Enterprises (MNEs)[46] create in the production of digital services and products, as a crucial aspect of digital sovereignty**. To do so, it analyzes the extent to which domestic production is controlled by foreign corporations and provides insights into the ownership structures, power dynamics, and interconnectivity levels that underpin digital economy networks.

This study uses the bilateral gross-output matrix of the OECD Analytical AMNE database (2026) that contains detailed data on the activities of foreign affiliates in OECD countries (inward and outward activity of multinationals). It covers 80 economies plus the "Rest of the World", 41 industries and the period 2000–2023. The database combines multinational enterprise statistics with other sources within the Inter-Country Input-Output (ICIO) framework, estimating missing information and reconciling data to ensure international consistency (OECD, 2026).

Through the Analytical AMNE data, we can examine the **control and geographical organisation of production as a specific dimension of digital sovereignty**. The analysis distinguishes between where digital production takes place and where the corporation undertaking this production comes from, providing a perspective that complements trade, domestic production, input-output and foreign direct investment statistics (Cadestin et al., 2018). The bilateral matrix identifies production by **host country** and ultimate **controlling country**. Host country refers to the country where the production activity is taking place, while controlling country refers to the parent country of the Multinational Enterprise that implements such production. Accordingly, domestic observations represent domestically controlled production, including both multinational and other domestic enterprises. Cross-border observations identify foreign-affiliate production controlled from another country (OECD, 2026). In this study, these relationships form a directed, weighted network linking "controlling" countries to "host" countries, allowing the assessment of inward and outward productive control, geographical concentration and network position.

Some limitations should be considered when interpreting results based on these data. The Analytical AMNE database is not based solely on directly observed bilateral data, as the OECD combines reported AMNE information with other sources, including the OECD Inter-Country Input-Output database, to produce a complete and internationally consistent dataset (Cadestin et al., 2018). This makes the data useful for comparative analysis, but also means that bilateral relationships partly reflect estimation, harmonisation and reconciliation procedures rather than direct observations of individual firms or investment events. In addition, gross output measures productive activity rather than value added, or income retained by the parent economy, and

[46] A multinational enterprise (MNE) is an enterprise that controls or owns business activities in more than one country, typically through a parent enterprise and its foreign affiliates. In this chapter, the concept is used in line with the OECD Analytical AMNE framework, which attributes production to the country of the ultimate controlling parent enterprise.

changes in monetary values may reflect prices and exchange rates as well as production volumes (OECD, 2024). Ownership-based indicators capture the corporate execution of production in a given country, but provide only a partial measure of actual control and strategic autonomy. They do not directly identify control over data, intellectual property, critical technologies, digital infrastructure, or public-sector digital capabilities, such as data governance, regulatory capacity and the development of public digital services. Sectoral aggregation also limits the identification of specific digital activities, while country-level aggregates may conceal differences in firm concentration, technological criticality and infrastructure resilience. Moreover, foreign ownership and geographical concentration do not automatically imply dependency or vulnerability, since their strategic implications depend on factors such as substitutability, market concentration, contractual arrangements, minority investments and reliance on foreign suppliers. Our results should therefore be interpreted as indicators of the **influence and production dimension of digital sovereignty**, rather than as a comprehensive assessment of digital sovereignty or production autonomy as a whole. A broader evaluation requires complementary evidence on critical inputs, technological capabilities, market concentration, intellectual property, data and cloud infrastructure, public-sector capacity, and the substitutability of essential technologies.

Despite these limitations, the 2026 Analytical AMNE database provides a unique opportunity to analyse the control of global production networks in the digital economy. For the purpose of this study, we focus on 2023 data [47] for three key sectors: computer, electronic and optical products (C26), telecommunications (J61), and IT and other information services (J62T63), because these are the industry aggregates most directly associated with the production of core digital goods, connectivity services, and digital/IT services.

5.1.1. Power and Interconnectedness Indicators

The bilateral ownership matrix of the OECD Analytical AMNE database provides a basis for deriving a range of indicators of the relative importance and interconnectedness of production controlled by enterprises with ownership in specific countries. By linking each ultimate controlling country to the countries where production takes place, the matrix enables an assessment of the scale, geographical reach and network position of these production relationships. This study considers seven indicators, presented in **Table 10**, to capture complementary aspects of countries' power and interconnectedness in digital production networks.

The seven indicators are derived from the bilateral gross-output matrix, X_{ij}, where i denotes the economy of the ultimate controlling parent and j the host economy in which production takes place. Each observation measures gross output produced in economy j under the control of enterprises ultimately owned from economy i. Diagonal observations ($i=j$) represent domestically controlled production, including production by both domestic MNEs and other domestic enterprises, while off-diagonal observations ($i \neq j$) identify production by foreign affiliates of MNEs and define the directed international network, with links running from parent to host economies ($i \rightarrow j$) and weights corresponding to bilateral gross output. Based on this distinction, $\boldsymbol{OUT_i}$ denotes total production controlled by parent enterprises from a given economy, including both domestic production (by MNEs and other domestic enterprises) and production abroad (by foreign affiliates of MNEs).

[47] The latest year available in the 2026 release of the Analytical AMNE database.

Conversely, IN_i denotes production hosted within an economy but controlled by foreign MNEs, excluding domestically controlled production. Finally, X_{ii} represents the production taking place within a country under the control of its own enterprises, including both domestic MNEs and other domestic enterprises.

Table 11. Definition of Power and Interconnectedness Indicators

Indicator	Formula	Description	Classification
Total production volume	$\mathrm{OUT_i} = \sum_{j=1}^{N} \mathrm{X_{ij}}$	Total production both inward (domestically) and outward (outside the parent country) of MNEs from the parent country. *Absolute indicator (size-dependent).*	**X-Axis: Corporate Production Power** (Directly proportional)
International influence	$\mathrm{INT_i} = \mathrm{OUT_i} - \mathrm{X_{ii}}$	Part of the Total MNEs production volume directed toward foreign countries. Higher values indicate greater weight in international production networks. *Absolute indicator (size-dependent).*	**X-Axis: Corporate Production Power** (Directly proportional)
Global influence share	$\mathrm{GIS_i} = \frac{\mathrm{OUT_i} - \mathrm{IN_i}}{\mathrm{OUT_i} + \mathrm{IN_i}}$	Relative balance between outgoing and incoming MNEs influence in a country. High values indicate high international influence of a country's MNEs, with little external incoming influence from foreign MNEs. **Low values** indicate low international influence, together with domestic production mostly dominated by foreign MNEs. *Relative indicator (size-independent).*	**X-Axis: Corporate Production Power** (Directly proportional)
Network Centrality (Eigenvalue)[48]	$\mathrm{EC_i} = \mathrm{v_i}$	Measures the **structural importance** of a country within the international network. Higher values identify structurally important actors within the global digital ecosystem. *Relative indicator (size-independent).*	**X-Axis: Corporate Production Power** (Directly proportional)
Production Autonomy	$\mathrm{PA_i} = \frac{\mathrm{X_{ii}}}{\mathrm{OUT_i}}$	Share of a country's total parent-controlled production that takes place domestically. Higher values indicate a stronger domestic orientation of production controlled by enterprises from	**Y-Axis: Corporate Production Interconnectedness** (Inversely proportional)

[48] EC: Eigenvector Centrality

Indicator	Formula	Description	Classification
		that country. *Relative indicator (size-independent).*	
Network Influence	$NI_i = \sum_{j=1}^{N} L_{ij}$	Measures the total direct and indirect influence propagated through the international network (based on the Leontiev's matrix L). Higher values indicate stronger systemic influence. *Relative indicator (size-independent).*	**Y-Axis: Corporate Production Interconnectedness** (Directly proportional)
Network Resilience	$NR_i = 1 - \widetilde{SV}_i = \sum_{j=1}^{N} L_{ji} - L_{ii}$	Measures a proxy for resilience to external shocks (using the Leontiev's matrix L). The raw measure Systemic Vulnerability (SV) captures the cumulative network influence received from other countries. It is reverse-normalized to construct the Network Resilience indicator, so that higher scores indicate lower structural exposure and potentially greater resilience to external shocks. *Relative indicator (size-independent).*	**Y-Axis: Corporate Production Interconnectedness** (Directly proportional)

Source: JRC

The indicators considered in Table 1 have been **grouped into two dimensions: "Corporate Production Power" and "Corporate Production Interconnectedness"**. This step is particularly important from the perspective of digital sovereignty, as it is based on the hypothesis that high sovereignty power does not mean isolation (Di Marco et al. 2025). On the contrary, the capacity of a country to exercise its independence in the digital domain is often associated with its capacity to shape, participate in, and exercise leverage over foreign production ecosystems in global production networks (Coe and Yeung, 2019; Mayer and Lu, 2025). Particularly, decoupling these two dimensions from the broader concept of digital sovereignty **allows us to study the paradigm of becoming *"open but not powerless"* and unveil that different, complementary strategies can be defined to achieve digital sovereignty.**

In this context, **corporate production power means the capacity to command and exert influence over the production of digital services and products** both within the territory of a country (internal sovereignty) and in other countries abroad (external influence; Pohle and Thiel, 2020). While power can translate into leverage and influence to shape the digital landscape of other nations, while imposing its own standards and regulations, it is important to clarify that the present measurement limits to the relative influence of multinationals over the global production network.

The power dimension is represented by the X-axis and is measured through four indicators that are directly proportional to a country's corporate production power level (see **Table 10**), as follows. The *Total Production Volume* is relevant to a country's corporate production power as it represents the overall scale of its digital production capabilities, enabling it to exert influence over the global

economy. *International Influence* measures a country's ability to extend its economic reach beyond its borders. A country's *Global Influence Share* indicates the extent to which it can project its own influence globally, while resisting external influence from other countries. Finally, *Network Centrality* reflects a country's ability to occupy a structurally important position in global digital production networks, potentially allowing it to shape the flow of goods, services, and ideas.

The **Corporate Production Interconnectedness dimension, on the other hand, measures a nation's integration into complex global networks** both by looking at network characteristics (e.g., network density and complexity; Cariani et al., 2024) and the autonomy (or dependency) levels of a country production (Arjona et al., 2023). It can be seen as a proxy for a country's openness to the rest of the world, as it captures the extent to which its digital economy is integrated into global production networks, reflecting its degree of exposure to and engagement with international corporate production.

This dimension is represented by the Y-axis and driven by indicators that reflect a country's systemic influence, resilience, and domestic orientation. *Production Autonomy* reflects a country's reliance on domestic production, with lower scores indicating greater interconnectedness with the global economy. *Network Influence* measures the extent to which a country is influenced by and connected to other countries in the global digital economy. Finally, *Network Resilience* indicates a country's ability to withstand external disruptions and maintain its position within global digital production networks, with higher scores suggesting greater interconnectedness and adaptability.

Interconnectedness should not therefore be understood simply as the opposite of sovereignty. Network-based approaches to international political economy emphasise that interconnectedness can itself generate asymmetric forms of structural power when particular actors occupy central or difficult-to-substitute positions within international networks (Farrell & Newman, 2019). From this perspective, the relevant question is not only how internationally connected an economy is, but also the position it occupies within these connections and the extent to which relationships generate leverage or exposure.

By plotting these two dimensions against each other, a two-dimensional analytical framework is constructed, allowing for the identification of **four distinct quadrants** (see **Figure 32**). Each quadrant represents a unique combination of power and interconnectedness levels, providing insights into a country's position within the global digital economy. The quadrants are defined by the intersection of the X-axis and Y-axis, with countries falling into one of four categories as follows:

- **Global Influencers** (High Power, High Interconnectedness): Central, highly integrated nodes that shape international networks while remaining highly interconnected.
- **Independent Powers** (High Power, Low Interconnectedness): Countries that project significant external influence while maintaining high production autonomy and self-reliance.
- **Connected Followers** (Low Power, High Interconnectedness): Highly integrated countries whose domestic production is largely dominated by foreign MNEs.
- **Limited Players** (Low Power, Low Interconnectedness): Countries characterized by high domestic orientation but very limited integration or influence within global MNE networks.

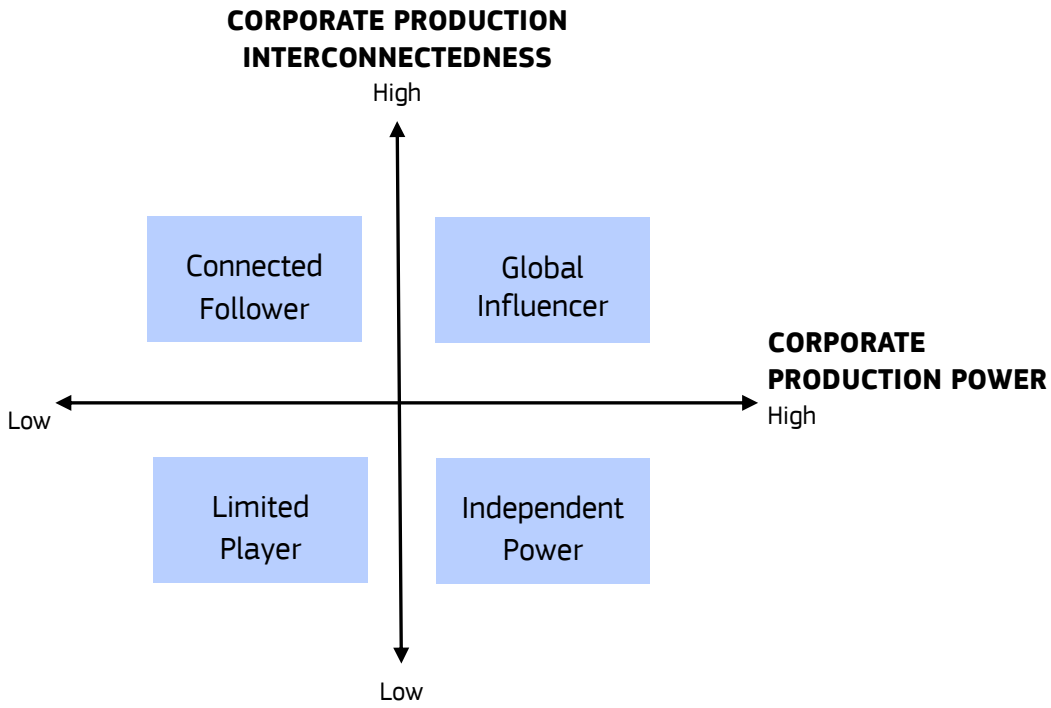
The thresholds distinguishing the allocation of countries to one of the four quadrants are defined by the average country score on each axis. For the X-axis, for example, a country positioned to the

right of the threshold has a composite index score above the country average in 2023; same for a country located in one of the two upper quadrants based on the Y-axis.

Power and Interconnectedness scores are standardized composite indices transformed onto a 0–100 display scale. The quadrant boundary corresponds to a composite score of zero and is displayed at 50. Scores are relative to the sector-year reference distribution and are not directly comparable as absolute levels across sectors or years.

In addition, to better map counties' positioning, the study uses a bubble-plot in which the size of each country's bubble is proportional to its Total Production Volume indicator, reflecting its overall MNE production footprint. This visualization allows obtaining an additional layer of analysis, as countries with larger bubbles have greater production, while smaller bubbles indicate lower production.

Figure 33. Power-interconnectedness quadrants definition



Source: JRC

It is worth noting that the indicators have been normalized to a relative scale of 0-100, facilitating comparisons across countries within each sector. However, normalisation does not eliminate the influence of a country's economic size, as the indicators capture different characteristics of digital production networks. The results should therefore be interpreted as relative indicator scores rather than measures that are uniformly independent of country size.The following sections present the results of the analysis for each of the three sectors selected: (i) IT and other information services; (ii) telecommunications; and (iii) computer, electronic and optical products. For each sector, the analysis provides insights at both the global and EU levels, with a focus on the countries that occupy central positions in international control networks. Particularly, the in-depth analyses across the seven indicators are performed for the top countries in terms of Total Production Volume. Finally, the EU27 average shown in the results of this chapter is calculated as a weighted average, taking into account the relative "Total Production Volume " of each EU Member State, to provide a

more accurate representation of the EU's position. The resulting analytical dataset that includes the complete set of indicators of power and interconnectedness is available through the JRC Open Data Catalogue (Isaraj et al., 2026).

5.2. Insights

5.2.1. Context overview: EU position, partner structure and historical trends

The EU's position in international digital production networks differs considerably across sectors. In 2023, its inward production footprint exceeded its outward footprint in both IT and information services and telecommunications, with outward-to-inward ratios of 0.32 and 0.48, respectively. In contrast, computer, electronic and optical products displayed a more balanced relationship, with EU-controlled production outside the Union slightly exceeding foreign-controlled production within it (1.14, see **Table 11**).

Table 12. EU outward and inward ownership-based production footprints, 2023

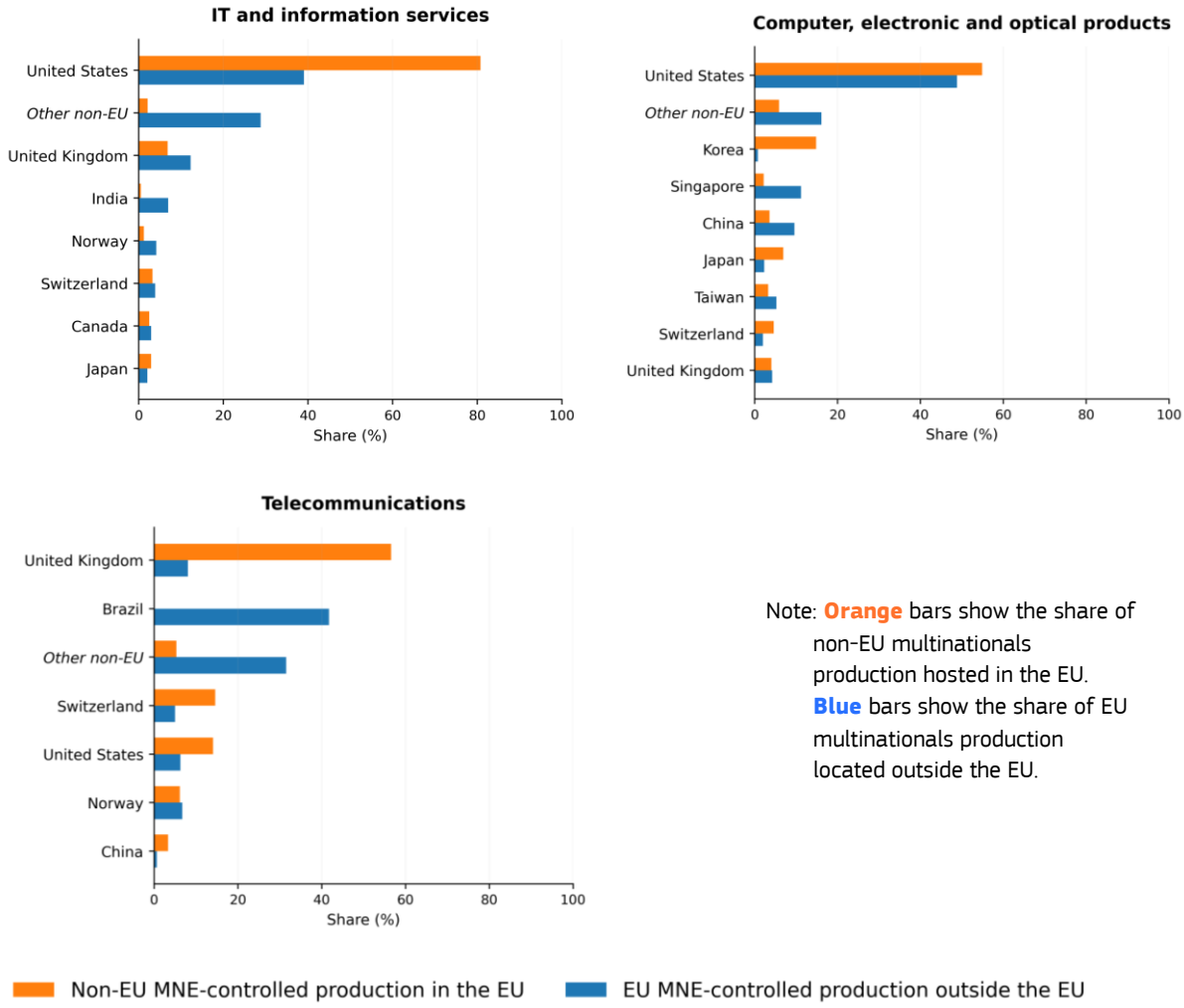
Sector	Production by EU multinationals outside the EU	Production by non-EU multinationals inside the EU	Outward / inward
IT and information services	117,194	360,601	0.32
Telecommunications	32,628	68,117	0.48
Computer, electronic and optical products	136,652	119,862	1.14

Source: JRC

Notes: Production values are expressed in millions of current US dollars; outward-to-inward ratios are dimensionless.

These differences illustrate the sector-specific scale and direction of cross-border productive control. However, aggregate inward and outward footprints provide only a partial picture, as they do not reveal the geographical concentration or structure of the underlying production relationships. When looking at the geographical distribution of the EU's inward and outward production footprints, the data reveal substantial differences across sectors and between the two directions of productive control, as shown in **Figure 33**.

Figure 34. Geographical composition of EU inward and outward multinational production, 2023



Source: JRC

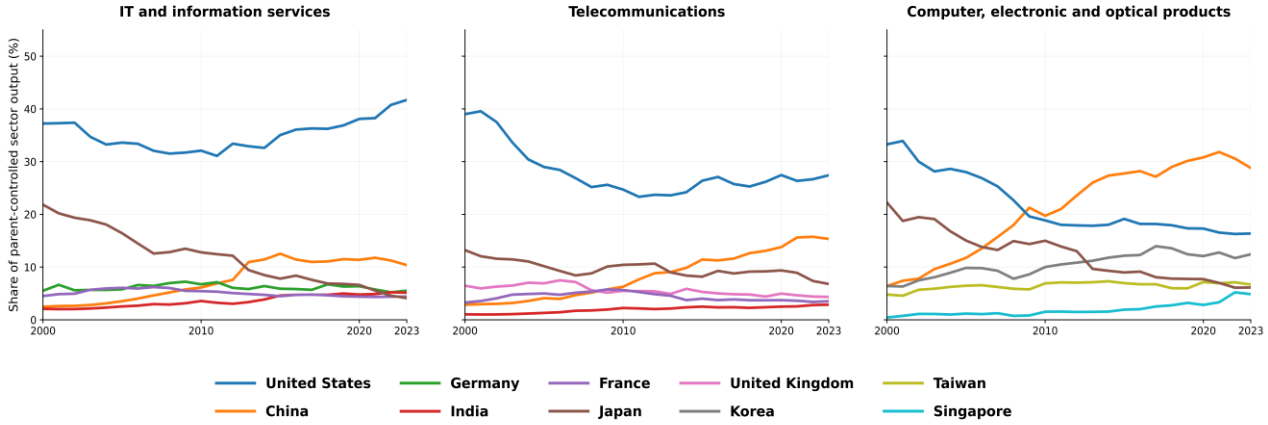
In IT and information services, the inward footprint was strongly concentrated among US parent companies, which accounted for 80.8% of non-EU-controlled production within the European Union. The outward footprint was more geographically distributed, although the United States remained its largest destination (39.0%).

In telecommunications, the United Kingdom accounted for the largest share of the EU's inward footprint (56.5%), while Brazil is the principal destination of EU-controlled production abroad (41.8%). **In computer, electronic and optical products**, the United States was the leading partner in both directions, accounting for 54.9% of the inward footprint and 48.8% of the outward footprint.

These patterns establish geographical relationships to be examined more systematically in the network analysis. In particular, a large outward footprint may coexist with strong concentration in a small number of hosts, while an aggregate inward–outward balance may conceal different partner structures. This is why footprint size alone cannot substitute for network-position and concentration-related indicators.

Finally, complementing the 2023 EU analysis, **Figure 34** traces the evolution of global production shares for the six leading parent economies in each digital sector between 2000 and 2023. By including both domestic-owned and foreign-hosted production, it captures changes in their relative production scale over time.

Figure 35. Evolution of parent-controlled sector output by major economies, 2000–2023



Source: JRC

Notes: Shares use total parent-attributed sectoral gross output across all host economies in the bilateral matrix as the denominator. The selected economies are the six leading economies by total production footprint in each digital sector, and colours identify the same economies consistently across panels.

The trajectories reveal that changes in production scale are sector-specific. In IT and information services, the United States retains the largest share among the displayed economies, with a decline during the 2000s followed by renewed growth after the early 2010s. China gains relative weight, while Japan's share falls substantially. In telecommunications, the US share declines considerably before stabilizing, alongside an increase in China's share. Computer, electronic and optical products display a more pronounced change in relative positions: China overtakes the United States among the displayed economies around 2009–2010; Korea gains share, while Japan declines.

These trends provide historical context for the subsequent analysis. The sector-specific radar charts compare the seven indicators for the six leading economies and the EU27 weighted average in 2023, extending the assessment beyond production scale to examine international influence, production autonomy and structural network position.

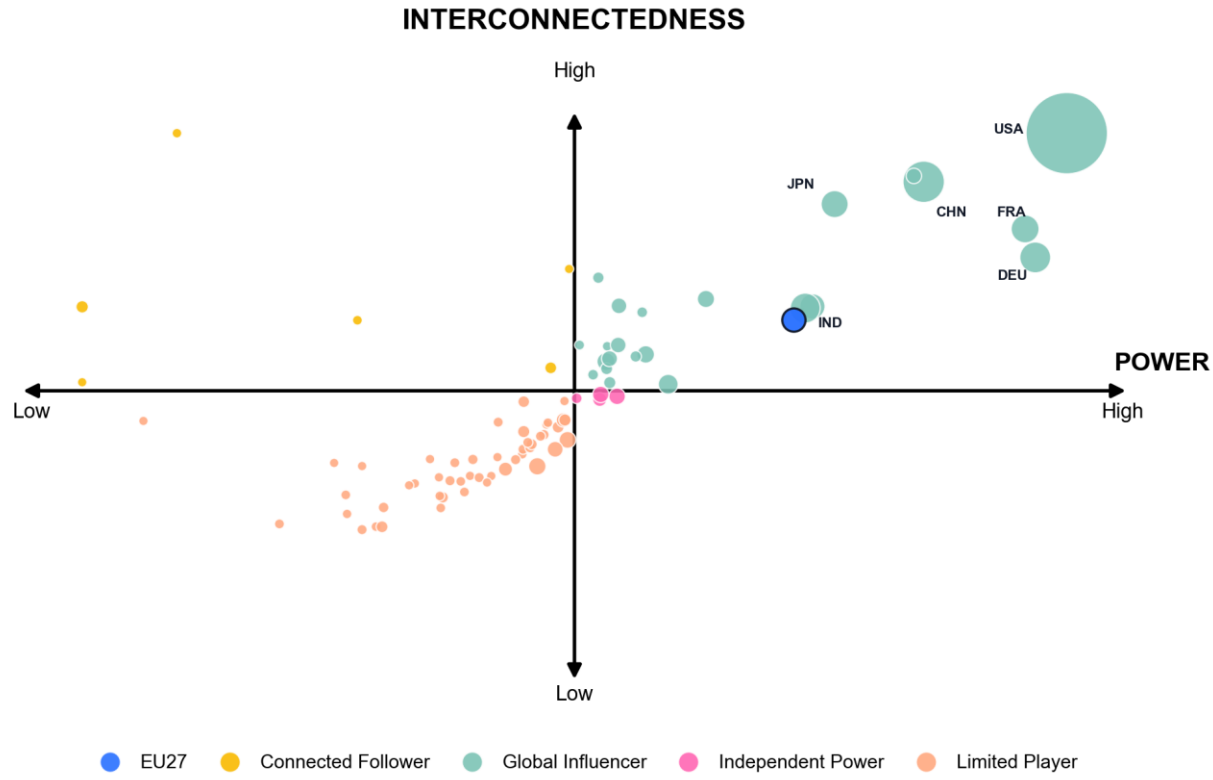
5.2.2. IT and Information Services: power and interconnectedness

Global landscape

The empirical results for the IT and Information Services sector in 2023 reveal that multinationals control is concentrated among few countries, with a large number of countries with relatively low power and interconnectedness levels.

Figure 35 illustrates this trend. In the **Global Influencer quadrant**, leading powers such as the United States (100, 100), China (91, 85), Germany (76, 97), France (81, 96), the United Kingdom (66, 74), Japan (86, 76), India (66, 73), and the EU27 weighted average (EU27: 64, 72) combine high structural centrality with dominant outward production footprints. In contrast, economies in the **Connected Follower** quadrant—most notably Mexico (100, 10), Norway (54, 48), and EU members like Ireland (66, 0)—exhibit deep integration into international production networks that are owned and directed by foreign multinationals. Meanwhile, the **Independent Power** category captures nations like Brazil (49, 54) and Spain (49, 53), which project notable outward corporate power while maintaining high production autonomy. Finally, a **significant majority of nations cluster in the Limited Players** quadrant, spanning several European economies such as Portugal (27, 31) and Hungary (23, 28), as well as non-European actors like Australia (40, 49), Turkey (44, 49), Argentina (43, 48), South Africa (37, 40), and Indonesia (39, 45), all characterized by limited outward multinational reach and weaker ties to global production chains.

Figure 36. Countries power and interconnectedness levels in the IT and Information Services sector, 2023



Source: JRC

Table 13. Leading economies and EU27 benchmark by production volume in the IT and Information Services sector, 2023

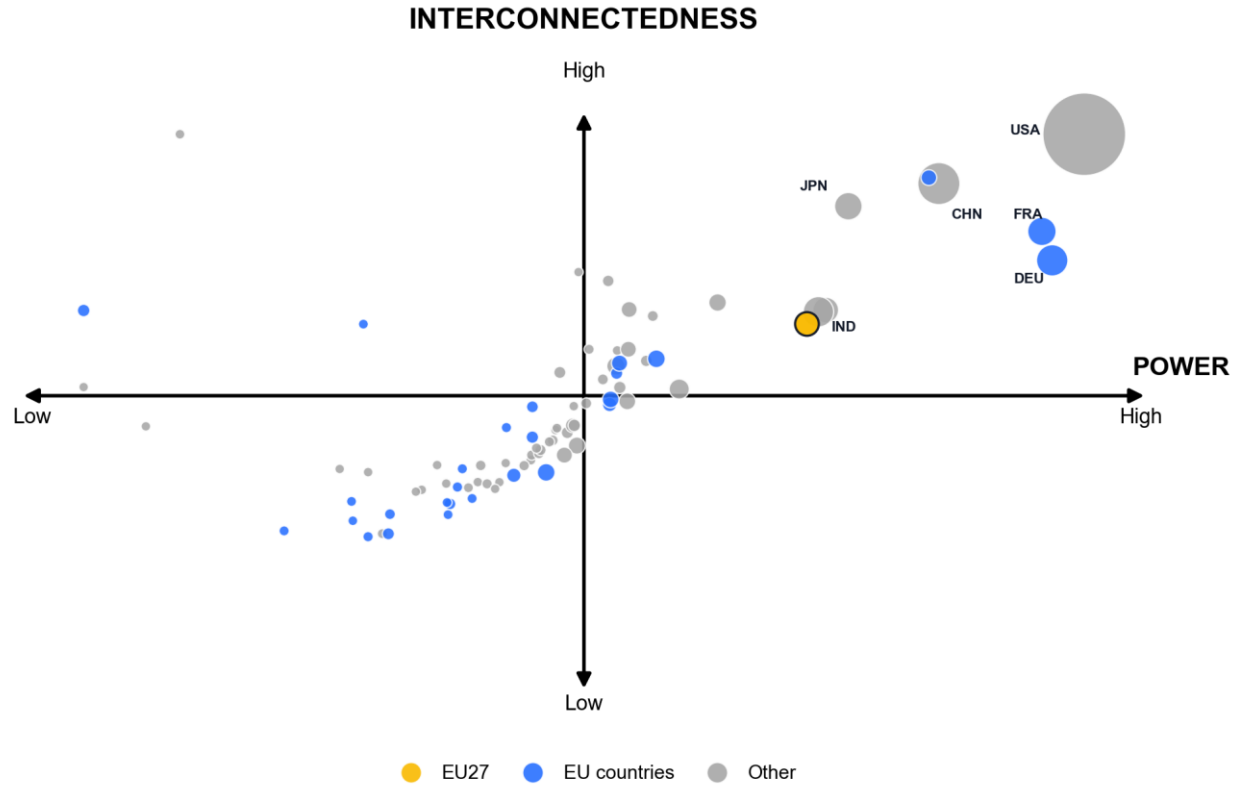
Country	Code	Corporate	Corporate	Group	Total
United States	USA	100	100	Global influencer	100
China	CHN	91	85	Global influencer	25
Germany	DEU	76	97	Global influencer	13
India	IND	66	73	Global influencer	12

France	FRA	81	96	Global influencer	11
Japan	JPN	86	76	Global influencer	10
United	GBR	66	74	Global influencer	8
EU27	**EU27**	**64**	**72**	**Global influencer**	**7**

Source: JRC

Power and interconnectedness levels in EU27

Figure 37. EU countries power and interconnectedness levels in the IT and Information Services sector, 2023



Source: JRC

When looking at the EU (**Figure 36**), **Member States show structural variation across the four quadrants, despite the consolidated weighted average (EU27) positions as a Global Influencer** (64, 72; 7), reflecting the collective weight of the block. At the national level, **Germany** (76, 97; 13) and **France** (81, 96; 11) lead as core Global Influencers, accompanied by), the **Netherlands** (57, 57), **Sweden** (56, 54), and **Finland** (54, 53). These countries maintain high network integration alongside outward multinational reach.

Spain (49, 53) and **Belgium** (48, 53) place as Independent Powers, maintaining power scores above 50 while recording lower interconnectedness. Conversely, **Ireland** (66, 0) and **Malta** (64, 28) sit in the Connected Follower quadrant, where elevated interconnectedness is coupled with minimal outward power, reflecting reliance on foreign multinational activity. In this context, Ireland

illustrates why a single EU average is insufficient: its IT output has a very different parent-economy mix from Germany, France, Italy or Poland. This does not mean that the presence of foreign multinationals is necessarily harmful; it identifies where the geographical location of production and the nationality of corporate control diverge. Policy interpretation also requires employment, tax, intellectual-property, market-structure and infrastructure evidence.

Table 14. Ownership structure of IT services production in selected EU host economies, 2023

Host (IT services)	Non-EU parent share	US parent share	Domestic parent
Ireland	93.7%	92.3%	4.7%
Germany	20.3%	14.7%	69.3%
France	12.9%	7.4%	74.3%
Italy	19.9%	15.7%	68.1%
Poland	21.6%	9.8%	65.3%
Netherlands	35.0%	29.2%	54.2%
Spain	20.5%	12.6%	60.7%

Source: JRC

A majority of EU members classify as Limited Players. This group spans major Southern and Central economies such as Italy (35, 46), Poland (35, 43), Austria (42, 45), Denmark (48, 45), Czechia (29, 37), Portugal (27, 31), and Romania (24, 30), all registering below the median threshold across both dimensions. This result may be attributed, in part, to the structural characteristics of the EU's business ecosystem, which is characterized by a high proportion of small and medium-sized enterprises (SMEs) that tend to operate primarily at the national level, limiting their international influence and interconnectedness.

Table 15. Power, Interconnectedness, and Total Production Volume in EU countries in the IT and Information Services sector, 2023

Country	Code	Corporate	Corporate	Group	Total
Germany	DEU	76	97	Global influencer	13
France	FRA	81	96	Global influencer	11
Netherlands	NLD	57	57	Global influencer	3
Italy	ITA	35	46	Limited player	3
Spain	ESP	49	53	Independent Power	3
Sweden	SWE	56	54	Global influencer	3
Luxembourg	LUX	92	84	Global influencer[49]	2

[49] Luxembourg's high power and interconnectedness values may be somewhat anomalous, and may be explained by the presence of numerous multinational company headquarters in the country, which are often established for tax optimization purposes.

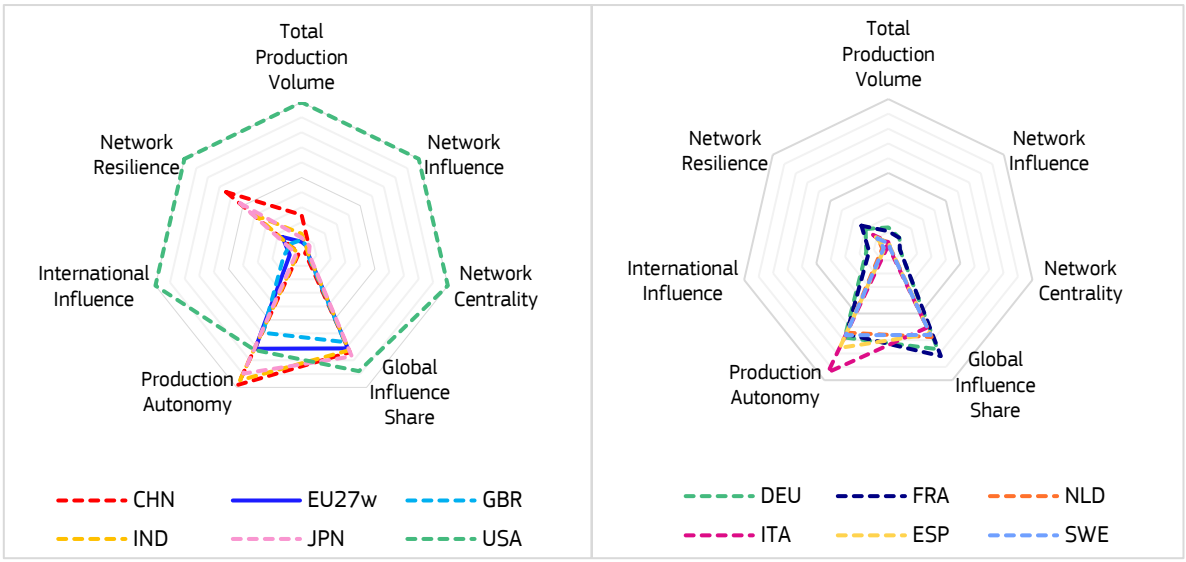
Poland	POL	35	43	Limited player	2
Belgium	BEL	48	53	Independent Power	2
Ireland	IRL	66	0	Connected Follower	1
Austria	AUT	42	45	Limited player	1
Finland	FIN	54	53	Global influencer	1
Romania	ROU	24	30	Limited player	1
Denmark	DNK	48	45	Limited player	1
Czechia	CZE	29	37	Limited player	1
Portugal	PRT	27	31	Limited player	≈0
Slovak Republic	SVK	33	37	Limited player	≈0
Hungary	HUN	23	28	Limited player	≈0
Estonia	EST	44	42	Limited player	≈0
Cyprus	CYP	36	38	Limited player	≈0
Bulgaria	BGR	24	20	Limited player	≈0
Greece	GRC	30	39	Limited player	≈0
Lithuania	LTU	30	27	Limited player	≈0
Croatia	HRV	27	36	Limited player	≈0
Malta	MLT	64	28	Connected Follower	≈0
Slovenia	SVN	30	36	Limited player	≈0
Latvia	LVA	26	27	Limited player	≈0

Source: JRC

Country profiles

When looking across the seven indicators in the IT and Information Services sector for the countries with the highest Total Production Volume values (see **Figure 37**), **the country profiles reveal a structural pattern of US global domination**. The United States registers the maximum value in 5 out of 7 indicators — Total Production Volume, Network Influence, Network Centrality, International Influence, and Network Resilience — and moderate to high values in the other two — 88% of Influence Share and 77% of Production Autonomy — indicating both extensive domestic capacity and outward systemic reach. These results could point to the fact that US-headquartered tech multinationals dominate both international production footprint and structural network centrality.

Figure 38. Country profiles of key non-EU (left) and EU (right) countries in the IT and Information Services sector, 2023



Source: JRC

The **major Asian economies display high domestic production autonomy paired with differentiated network positions**. China accounts for 25% of Total Production Volume and achieves a Network Resilience score of 65%, supported by a Production Autonomy of 98% and an International Influence Share of 74%. However, its Network Centrality (2%), Network Influence (6%), and relative International Influence (2%) remain modest compared to the US baseline. Japan presents a comparable orientation, recording 10% in Total Production Volume, 90% in Production Autonomy, and 77% in International Influence Share, with Network Resilience at 52% and Network Centrality at 5%. India exhibits 12% in Total Production Volume and 95% in Production Autonomy, with a 73% International Influence Share and 40% Network Resilience, while registering 5% in Network Centrality and 4% in Network Influence. This could indicate that **China, India, and Japan's IT ecosystems rely on large domestic markets or distinct national champions, while their multinational networks are more regionalized, specialized, or constrained, rather than acting as controllers of global IT value chains**.

In contrast to the domestic orientation of China, India, and Japan, the **European actors exhibit lower Production Autonomy and greater outward orientation, reflecting that European countries host a representative volume of foreign (primarily US) multinational activity—reducing their domestic autonomy—while simultaneously projecting their own highly specialized corporate networks outward across a diverse, multi-country footprint.** The United Kingdom records a Production Autonomy of 59% and an International Influence of 12%, the highest relative outward level after the US, alongside 8% in Total Production Volume and 66% in International Influence Share. Its Network Centrality and Network Influence reach 4% and 5%, respectively, with Network Resilience at 9%. The EU27 weighted average posts 7% in Total Production Volume, 71% in Production Autonomy, and 71% in International Influence Share, with International Influence at 8%, Network Resilience at 16%, Network Centrality at 4%, and Network Influence at 5%.

Within the EU, Germany and France are the most influential EU countries with Global Influence Share scores of 77% and 82%, respectively, indicating that they have a significant impact

on the global market. However, their Production Autonomy scores are moderate, with 68% and 65%, respectively, suggesting that a sizeable share of production controlled by German and French enterprises is located abroad, reflecting a relatively internationalised production footprint.

Other EU countries, such as the Netherlands, Italy, Spain, and Sweden, have lower Total Production Volume and Network Influence scores, but still have significant Global Influence Share scores. Particularly, **Italy has a high Production Autonomy score of 94%,** suggesting that production controlled by Italian enterprises may be predominantly located domestically, but its International Influence for the studied domain score is low, at 1%. This pattern is consistent with Italy's comparatively lower degree of productive internationalisation among the largest EU economies, particularly in services (ISTAT, 2026).

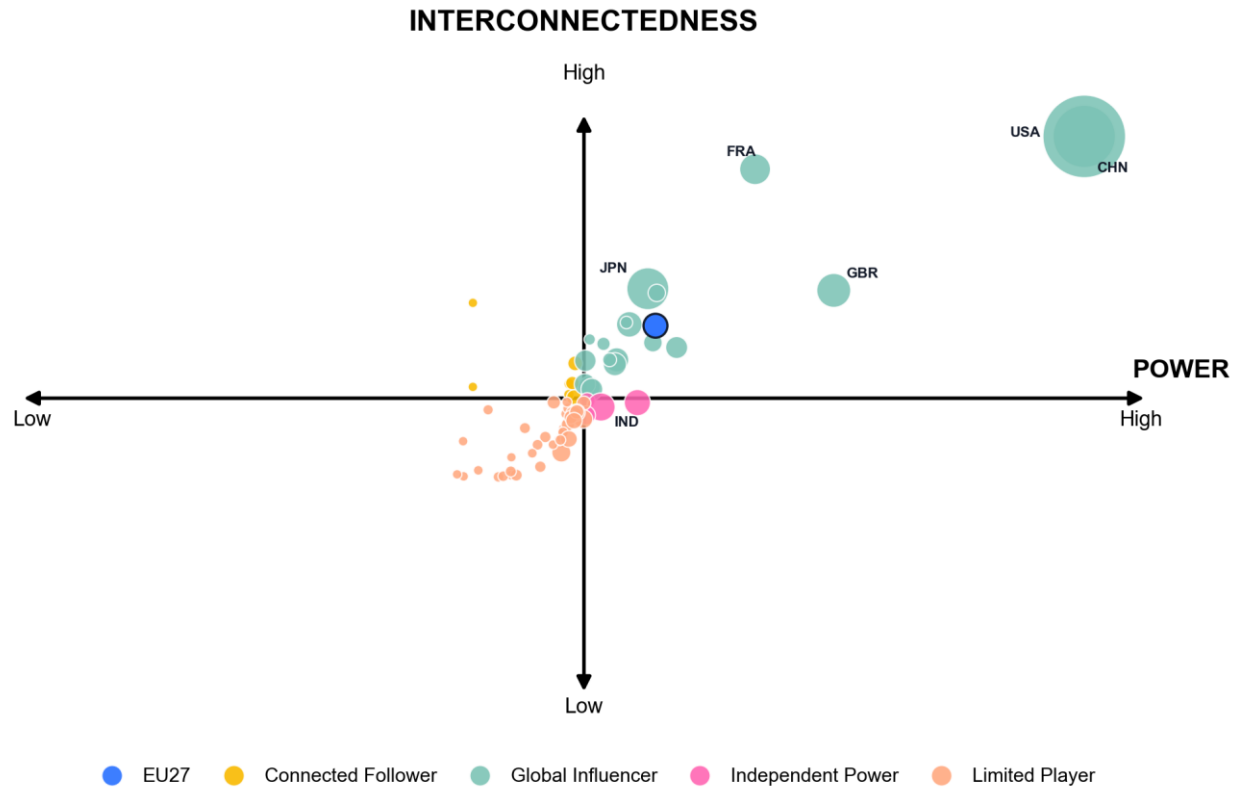
Generally, the Network Resilience scores of EU countries vary, with Germany and France having moderate scores, at 20% and 23%, respectively. The Netherlands, Italy, Spain, and Sweden have lower Network Resilience scores, with 8%, 13%, 11%, and 9%, respectively, indicating that they may be more vulnerable to external shocks and disruptions to their production networks.

5.2.3. Telecommunications: power and interconnectedness

Global landscape

The empirical results for the Telecommunications sector in 2023 reveal a highly interconnected economy, with only a few players occupying moderate to high power positions. In the Global Influencer quadrant, **leading powers such as the United States (100, 100) and China (100, 100) combine high structural centrality with dominant outward production footprints.** These two countries serve as the global benchmarks, with Total Production Volume values (MNEs production footprint) of 100% and 56%, respectively.

Figure 39. Countries power and interconnectedness levels in the Telecommunications sector, 2023



Source: JRC

Other countries, such as **Japan (71, 56), the United Kingdom (71, 75), France (94, 67), Canada (64, 55), and Korea (57, 53), are also positioned as Global Influencers, with high Interconnectedness Levels and moderate to high Power Levels.** These countries have significant connections to the global telecommunications network and exert considerable influence, but to a lesser extent than the United States and China.

In contrast, economies in the **Independent Power category, such as India (48, 52) and Germany (49, 55)**, exhibit moderate Interconnectedness Levels and Power Levels. India has an Interconnectedness Level of 48% and a Power Level of 52%, while Germany has an Interconnectedness Level of 49% and a Power Level of 55%. These countries have significant domestic telecommunications sectors and project their own corporate networks outward, but have limited connections to the global network compared to the Global Influencers.

A significant **majority of nations cluster in the Limited Player quadrant**, spanning large European economies such as Italy (47, 50) and Poland (35, 43), as well as non-European actors like Brazil (40, 48) and Australia (52, 51). These countries have low Interconnectedness Levels and Power Levels, indicating limited connections to the global telecommunications network and limited influence.

The size of the bubbles in the quadrants, which represents the Total Production Volume of each country, provides insights into the volume of MNEs production in the telecommunications sector. **The United States has the largest bubble, indicating the largest MNEs production footprint**. In second place, China follows with a Total Production Volume of 56%, indicating a significant but smaller MNEs production footprint. The other Global Influencers, including Japan, the

United Kingdom, France, Canada, and Korea, have smaller bubbles, with Total Production Volume ranging from 25% to 16%. The Isolated Autarkies, such as Italy and Poland, have the smallest bubbles, indicating limited MNEs production footprints.

Table 16. Leading economies and EU27 benchmark by production volume in the Telecommunications sector, 2023

Country	Code	Interconnectedne	Power	Group	Total
United States	USA	100	100	Global influencer	100
China	CHN	100	100	Global influencer	56
Japan	JPN	71	56	Global influencer	25
United Kingdom	GBR	71	75	Global influencer	16
France	FRA	94	67	Global influencer	13
India	IND	48	52	Independent Power	10
Germany	DEU	49	55	Independent Power	9
EU27 weighted	EU27	64	57	Global influencer	7

Source: JRC

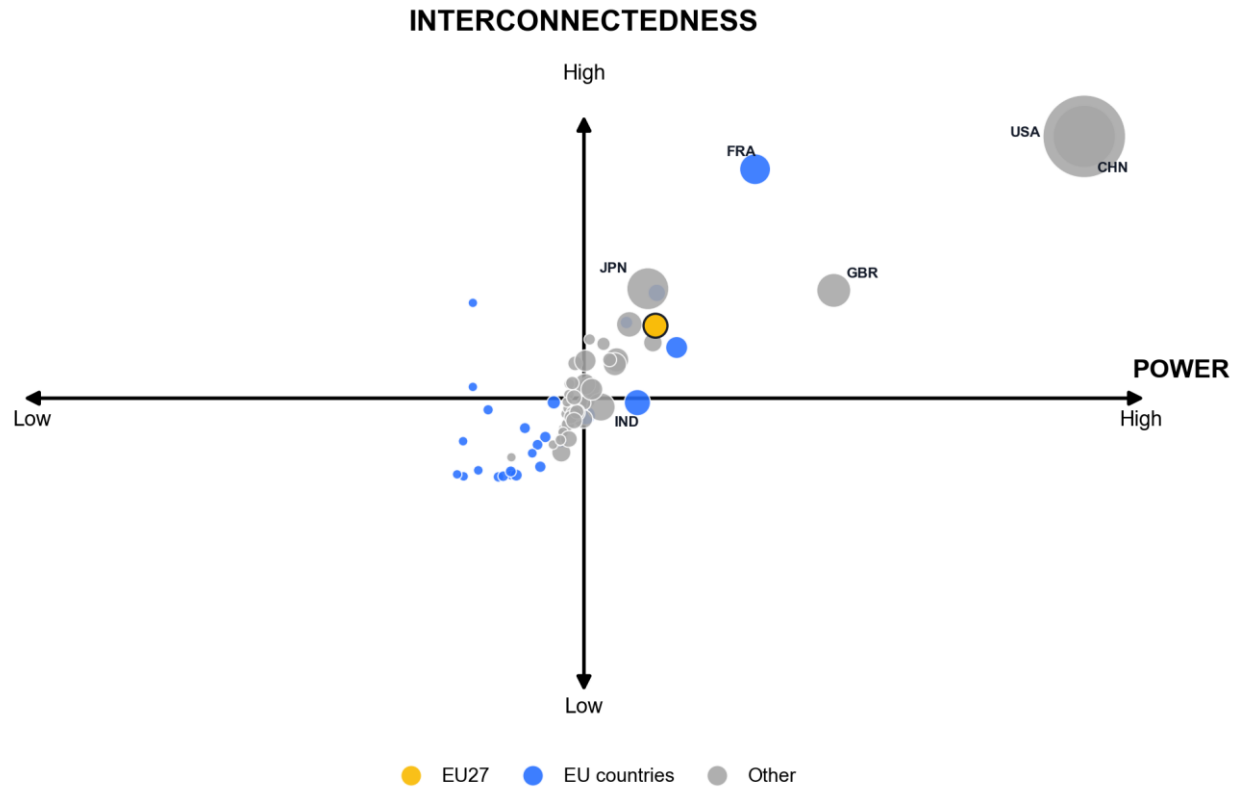
Power and interconnectedness levels in EU27

Figure 39 highlights a distinctive pattern among EU27 Member States: most cluster in the lower-left quadrant, combining relatively low power with relatively low interconnectedness. France is the clearest exception, displaying high interconnectedness and a stronger power position than most other EU countries in this sector. This distribution reveals substantial heterogeneity within the Union.

The EU27 weighted average lies in the upper-right quadrant, contrasting with the position of many individual Member States. This contrast suggests that the EU single market may play a role in enhancing the collective influence and interconnectedness of its members, as individual Member States often have more limited influence and connections on their own. However, it remains considerably closer to the centre than the United States and China. The weighted average therefore presents a different picture from the country-level distribution, highlighting the importance of examining both when assessing the EU's position.

From a digital sovereignty perspective, this pattern suggests that the Union's collective position coexists with limited power across many Member States. Low interconnectedness should be interpreted cautiously, since it may reflect limited international integration rather than greater autonomy.

Figure 40. EU countries power and interconnectedness levels in the Telecommunications sector, 2023



Source: JRC

Table 17. Power, Interconnectedness, and Total Production Volume in EU countries in the Telecommunications sector, 2023

Country	Code	Interconnectednes	Power	Group	Total
France	FRA	94	67	Global influencer	13
Germany	DEU	49	55	Independent Power	9
Spain	ESP	60	59	Global influencer	6
Italy	ITA	47	50	Independent Power	4
Sweden	SWE	70	57	Global influencer	3
Belgium	BEL	42	48	Limited player	1
Netherlands	NLD	49	47	Limited player	1
Luxembourg	LUX	64	54	Global influencer	1
Poland	POL	35	43	Limited player	1
Denmark	DNK	37	46	Limited player	1
Czechia	CZE	43	46	Limited player	1
Greece	GRC	44	44	Limited player	1
Romania	ROU	36	43	Limited player	≈0
Finland	FIN	41	45	Limited player	≈0

Portugal	PRT	35	42	Limited player	≈0
Ireland	IRL	35	41	Limited player	≈0
Austria	AUT	48	40	Limited player	≈0
Hungary	HUN	36	43	Limited player	≈0
Slovenia	SVN	39	45	Limited player	≈0
Cyprus	CYP	42	47	Limited player	≈0
Slovak	SVK	36	39	Limited player	≈0
Latvia	LVA	35	43	Limited player	≈0
Bulgaria	BGR	35	38	Limited player	≈0
Croatia	HRV	42	38	Limited player	≈0
Estonia	EST	52	39	Connected Follower	≈0
Lithuania	LTU	35	37	Limited player	≈0
Malta	MLT	68	39	Connected Follower	≈0

Source: JRC

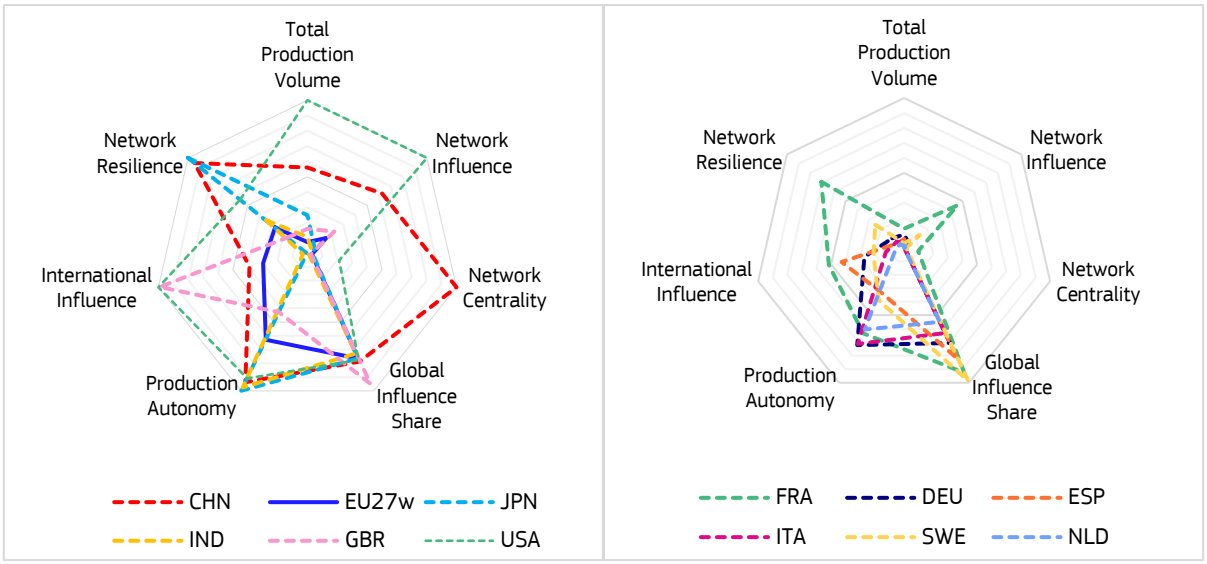
Country profiles

When looking across the seven indicators (**Figure 40**) the analysis **reveals different structural profiles, with the US and China as the main dominant players but with leading positions in different indicators.** The US registers the maximum value in Total Production Volume, Network Influence, and International Influence, and moderate to high values in Production Autonomy (94%) and Global Influence Share (79%). However, **the maximum value of the Network Centrality indicator is displayed by China (100%), with the US following in second place with a notably lower score (21%)**. This structural position is consistent with the broader international significance of large Chinese ICT firms. For example, Huawei and ZTE feature among major global corporate R&D investors, reflecting the scale of China's corporate capabilities in ICT-related industries (EU Industrial R&D Investment Scoreboard, 2023).

China and Japan display very high values of Network Resilience (94% and 100% respectively) indicating a combination of a diverse and complex network of relationships that could allow them country to adapt and respond to changing global economic conditions.

Regarding Total Production Volume and Network Influence, Japan, India, the UK and the EU27 weighted average, have relatively low values. However, all of them except still have significant Global Influence Share, indicating (values between 73% and 97%) indicating that they exert higher international influence, with regard to the external incoming influence from foreign MNEs.

Figure 41. Country profiles of top non-EU (left) and EU (right) countries in the Telecommunications sector (2023)



Source: JRC

Regarding the country profiles of main EU players, the telecommunications landscape is characterized by a diverse range of countries with varying levels of influence. **France stands out as the most influential EU country,** with a significant Total Production Volume and Network Influence. This can be attributed to its strong domestic telecommunications sector and its ability to project its influence globally.

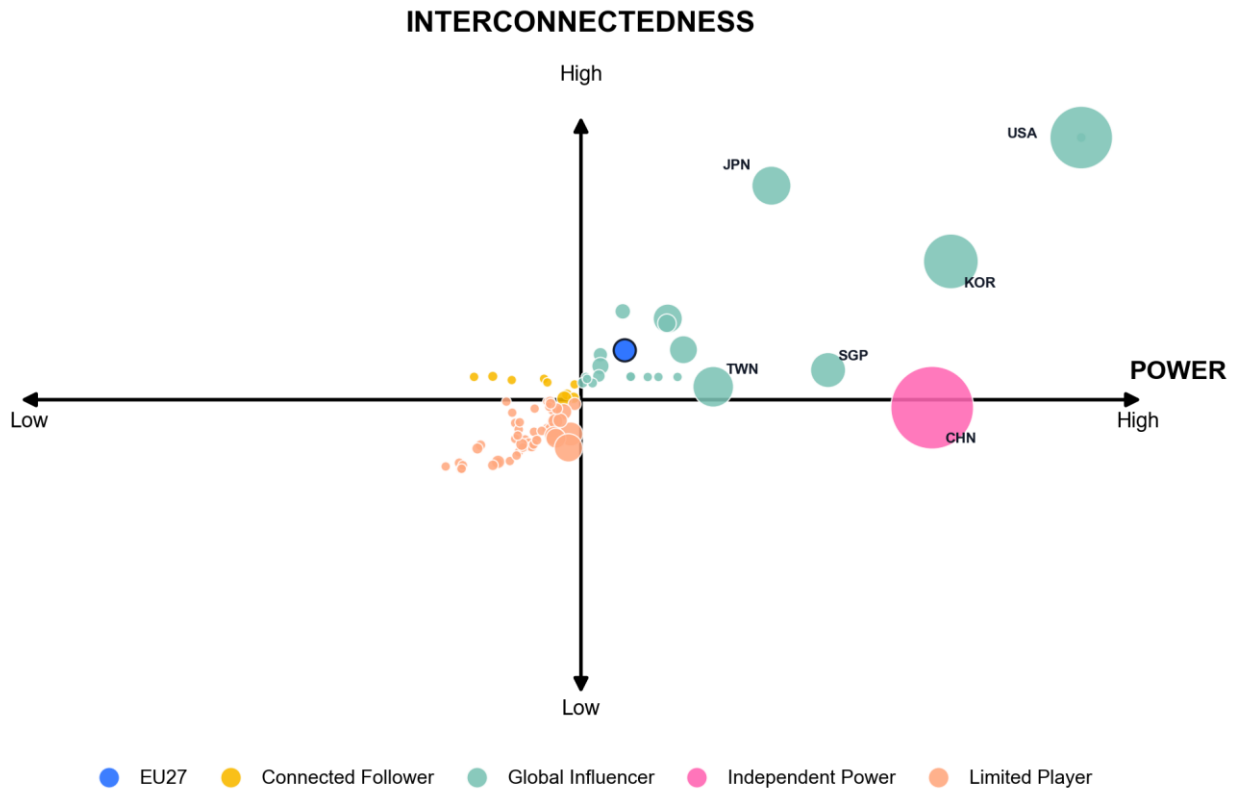
The EU countries' relatively low Production Autonomy scores suggest that a **comparatively large share of production controlled by their telecommunications enterprises is located abroad**. This points to a more internationally distributed production footprint. It may partly reflect the internationalisation of major European telecommunications groups, which can operate substantial activities outside their home economies. For example, Deutsche Telekom generated 77% of its net revenue outside Germany in 2023 (Deutsche Telekom, 2024). Computer Electronic and Optical Products: power and interconnectedness trends

5.2.4. Computer and Electronics: power and interconnectedness

Global landscape

The empirical results for the Computer and Electronics sector reveal a **different landscape of global influence and interconnectedness than in the previous two sectors**. The biggest difference relies in the fact that the largest value in Total Production Volume displayed by China, does not correspond to the largest values in power and interconnectedness, displayed by the US.

Figure 42. Countries power and interconnectedness levels in the Computer Electronic and Optical Products sector, 2023



Source: JRC

In the Global Influencer quadrant, countries such as the **United States, Korea, and Japan combine high interconnectedness with dominant power positions**. The United States has an Interconnectedness Level of 100% and a Power Level of 100%, indicating its significant influence over the global network. Korea and Japan also have high Interconnectedness Levels, at 76% and 91%, respectively, and moderate to high Power Levels, at 87% and 69%, respectively

Other countries, such as **China, Taiwan, and Singapore, are positioned as Independent Powers**, with moderate Interconnectedness Levels and high Power Levels. China has an Interconnectedness Level of 49% and a Power Level of 85%, indicating its significant influence over the global network, but also its relatively low level of interconnectedness. Taiwan and Singapore have Interconnectedness Levels of 52% and 56%, respectively, and Power Levels of 63% and 75%, respectively.

Table 18. Leading economies and EU27 benchmark by production volume in the Computer Electronic and Optical Products sector, 2023

Country	Code	Interconnectedne	Power level	Group	Total
China	CHN	49	85	Independent Power	100
United States	USA	100	100	Global influencer	57
Korea	KOR	76	87	Global influencer	43

Taiwan	TWN	52	63	Global influencer	23
Japan	JPN	91	69	Global influencer	21
EU27 weighted	**EU27**	**59**	**54**	**Global influencer**	**6**

Source: JRC

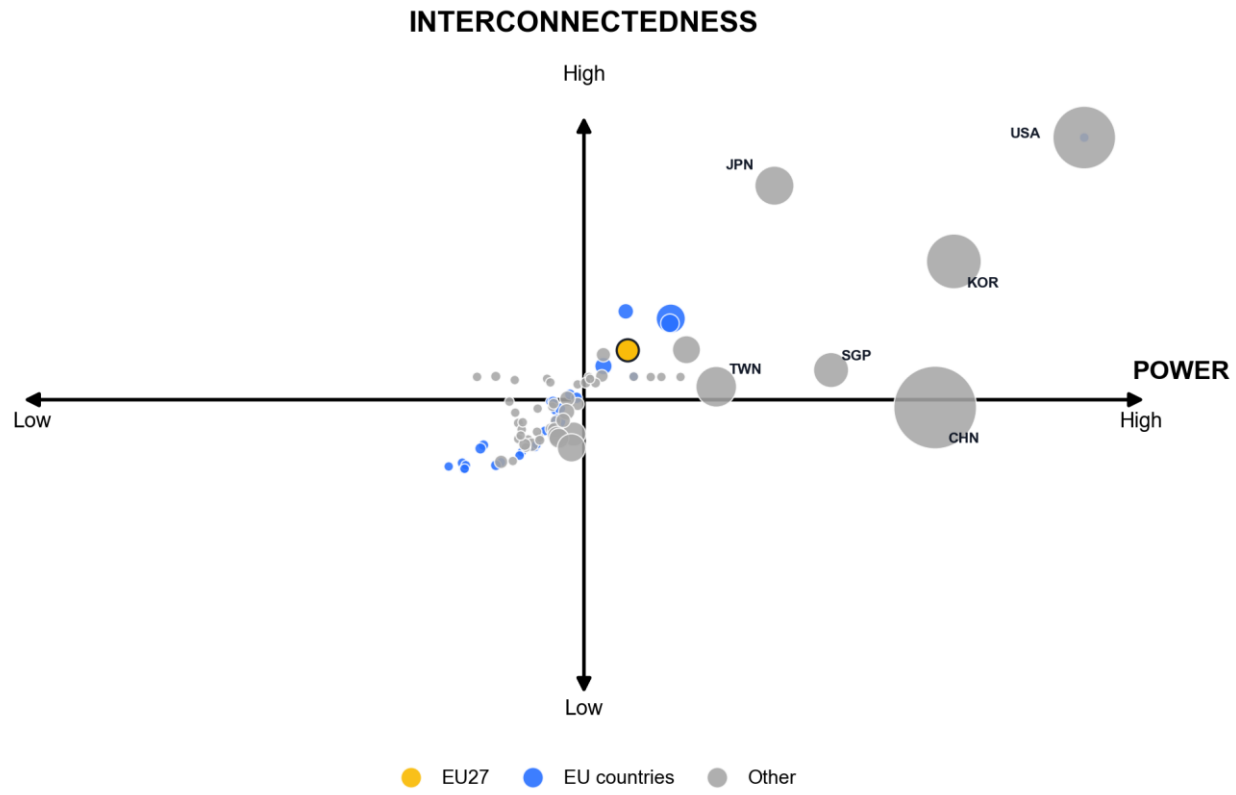
The EU27 weighted average has an Interconnectedness Level of 59% and a Power Level of 54%, positioning it as a Global Influencer. However, the **EU Member States show significant variation in their Interconnectedness Levels and Power Levels**. Germany, for example, has an Interconnectedness Level of 65% and a Power Level of 59%, indicating its significant influence over the global network. France has an Interconnectedness Level of 56% and a Power Level of 52%, while the United Kingdom has an Interconnectedness Level of 50% and a Power Level of 48%.

The size of the bubbles in the quadrants, which represents the Total Production Volume of each country, provides additional insights into the global landscape. China has the largest bubble, indicating the country owning the biggest MNEs production volume, but its Interconnectedness Level is relatively low, indicating its limited connections to the global network. The US on the other hand has a smaller bubble, with a Total Production Volume of 57%. Other countries, such as Korea and Japan, have smaller bubbles, but still have significant Total Production Volume scores, at 43% and 21%, respectively.

Power and interconnectedness levels in EU27

Figure 42 shows that most EU27 countries cluster in the lower-left quadrant, combining relatively low power with relatively low interconnectedness. A small number of Member States occupy the upper-right quadrant, revealing an uneven distribution of both dimensions within the Union. The EU27 weighted average also lies in the upper-right quadrant but remains close to the centre and well below the power levels of the leading non-EU economies. This pattern highlights the contrast between the Union's average position and the more limited power of most individual Member States.

Figure 43. EU countries power and interconnectedness levels in Computer Electronic and Optical Products sector (2023)



Source: JRC

Table 19. Power, Interconnectedness, and Total Production Volume in EU countries in the Computer Electronic and Optical Products sector, 2023

Country	Code	Interconnectednes	Power	Group	Total
Germany	DEU	65	59	Global influencer	11
Netherlands	NLD	65	59	Global influencer	4
France	FRA	56	52	Global influencer	3
Finland	FIN	67	54	Global influencer	2
Italy	ITA	46	47	Limited player	2
Austria	AUT	48	47	Limited player	1
Denmark	DNK	50	49	Connected Follower	1
Sweden	SWE	48	48	Limited player	1
Ireland	IRL	41	40	Limited player	1
Belgium	BEL	51	49	Connected Follower	≈0
Poland	POL	37	41	Limited player	≈0
Spain	ESP	41	45	Limited player	≈0

Czechia	CZE	41	40	Limited player	≈0
Malta	MLT	50	47	Limited player	≈0
Hungary	HUN	38	38	Limited player	≈0
Luxembourg	LUX	54	55	Global influencer	≈0
Lithuania	LTU	44	46	Limited player	≈0
Slovak	SVK	37	38	Limited player	≈0
Slovenia	SVN	39	44	Limited player	≈0
Greece	GRC	41	45	Limited player	≈0
Romania	ROU	37	38	Limited player	≈0
Latvia	LVA	50	47	Limited player	≈0
Portugal	PRT	37	38	Limited player	≈0
Cyprus[50]	CYP	100	100	Global influencer	≈0
Bulgaria	BGR	38	42	Limited player	≈0
Croatia	HRV	40	44	Limited player	≈0
Estonia	EST	37	36	Limited player	≈0

Source: own elaboration

Country profiles

When looking at detailed indicators (**Figure 43**), the Computer, Electronic, and Optical Products sector is characterized by a mix of countries with varying levels of influence and autonomy. **China is the dominant player**, with a Total Production Volume of 100%, indicating its significant impact on the global market. However, its Network Influence is relatively low, at 14%, suggesting that **it may not have as strong a presence in the global network as other countries**. China's high Production Autonomy score of 94% indicates that the great majority of production controlled by Chinese parent enterprises is located domestically., but its low Network Resilience score of 10% implies that it may be vulnerable to external shocks and disruptions to its production networks.

The **United States** is another major player, with a high Network Influence of 100% and a significant Total Production Volume of 57%. Its high International Influence score of 100% suggests that it has a strong presence in foreign markets, but its relatively low Production Autonomy score of 47% indicates a **highly internationalised production footprint, with a substantial share of US parent-controlled production located outside the United States**.

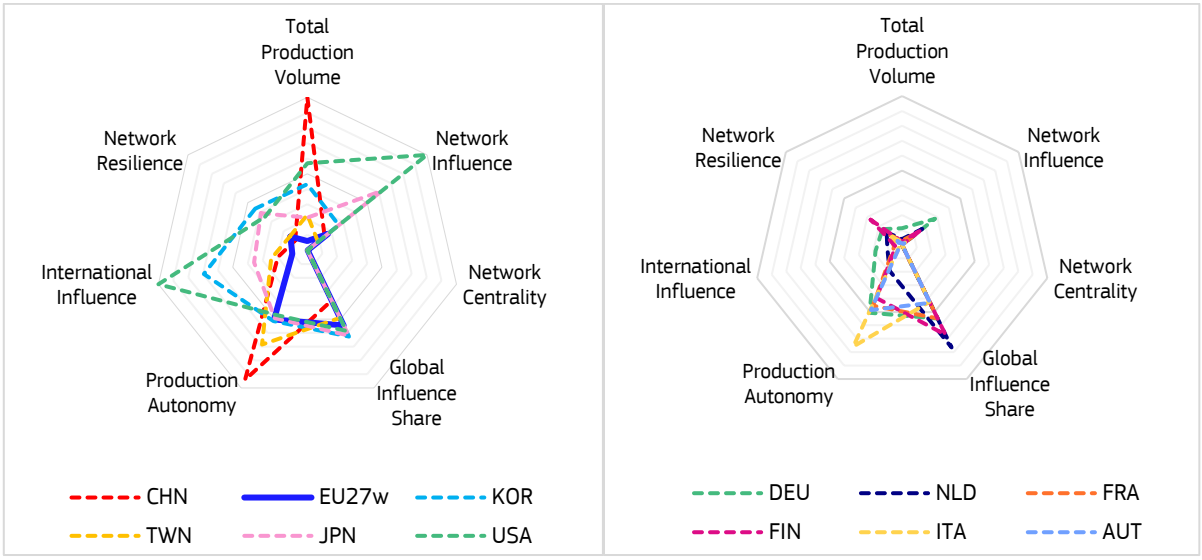
Other countries, such as Korea and Taiwan, have significant Total Production Volume and Network Influence scores, indicating their importance in the global supply chain. Korea's high Global Influence Share of 63% and International Influence score of 70% suggest that it has a strong

[50] Cyprus's high rankings may be influenced by a combination of factors, including the small denominator effect or statistical anomalies. As such, these results should be viewed with caution and considered in the context of broader trends and patterns in the electronics sector.

presence in foreign markets, while Taiwan's high Production Autonomy score of 68% indicates its domestic orientation of parent-controlled production. Japan is also a significant player, with a high Network Influence of 62% and a moderate Total Production Volume of 21%.

The EU27 weighted average has a relatively low Total Production Volume and Network Influence, but a significant Global Influence Share of 55%, suggesting that it has a dispersed influence across its Member States. The low Network Resilience scores of many countries in this sector, including the EU27 weighted average, imply that they may be vulnerable to external shocks and disruptions to their production networks.

Figure 44. Country profiles of top non-EU (left) and EU (right) countries in Computer Electronic and Optical Products sector (2023)



Source: JRC

When looking at main EU players in the Computer, Electronic, and Optical Products sector, **Germany appears as the most influential EU country**, with a Total Production Volume of 11% and a Network Influence of 28%, indicating its significant presence in the global network. **However, its Production Autonomy score of 51% suggests that** roughly half of German parent-controlled production is located domestically and the remainder abroad.

Other EU countries, such as **the Netherlands and France**, have lower Total Production Volume and Network Influence scores, but still have **significant Global Influence Share scores**, indicating their importance in the global supply chain. The Netherlands has a high Global Influence Share of 76%, despite its relatively low Total Production Volume of 4%, suggesting that it has a strong presence in foreign markets. France has a moderate Global Influence Share of 55%, but its low International Influence score of 6% suggests that it may not have as strong a presence in foreign markets as other EU countries.

Finland is a notable player, with a high Global Influence Share of 67% and a moderate Network Influence of 17%, despite its relatively low Total Production Volume of 2%. Its high Network Resilience score of 27% suggests that it may be better equipped to withstand external shocks and disruptions to its production networks.

Italy and Austria have relatively low Total Production Volume and Network Influence scores, but still have significant Production Autonomy scores, indicating their **strong domestic orientation of parent-controlled production**. However, their low International Influence scores suggest that they may not have as strong a presence in foreign markets as other EU countries.

5.3. Conclusions and key takeaways

The present analysis provides a nuanced understanding of the complex relationships between countries in the global digital economy based on an analysis of multinationals production networks. It complements the analysis of trade data in Chapter 7 of this report. By considering both power and interconnectedness dimensions, it helps to **identify countries that exert significant control over the global digital economy, as well as those where their domestic production is heavily dependent on foreign multinationals.**

Accordingly, it enables a more comprehensive analysis of the international control structures in the production of digital services and goods, **moving beyond a simplistic classification of countries as either dominant or dependent**, shedding light on the complex relationships between countries and the implications for digital sovereignty and international dependencies.

Key takeaways

The analysis shows that **power and interconnectedness frequently coexist in multinational production networks**, although their relationship differs across digital sectors, reinforcing the **"open but not powerless" approach, as digital sovereignty cannot be pursued in isolation.** Leading countries generally combine substantial productive capacity and international influence with strong network integration. This pattern supports a conception of digital sovereignty in which countries exercise influence through international connections while retaining domestic capabilities. If power and interconnectedness reinforce one another over time, this could generate a *Matthew effect*, whereby already powerful economies use their network positions to accumulate further influence, widening the gap with less powerful economies. However, the results establish an association between the two dimensions rather than demonstrating such a cumulative, self-reinforcing mechanism.

Despite these regularities, **results also show a large heterogeneity in countries' positioning**, as in the computer, electronic and optical production, where China has the largest parent-controlled production footprint but is classified as an Independent Power, combining high power with comparatively low interconnectedness. The United States, despite its smaller production footprint, achieves higher composite scores in both dimensions. **Production scale therefore does not translate automatically into equivalent international reach or network influence.**

Another finding revolves around **the role of scaling domestic champions for global deployment. This is represented in the fact that high Production Autonomy can coexist with substantial outward projection**. As defined in this study, this indicator measures the proportion of an economy's parent-controlled production located domestically. A country with a large domestic production base can consequently retain high Production Autonomy while controlling considerable production abroad. The United States illustrates this combination in telecommunications, where high domestic orientation accompanies leading International Influence and Network Influence scores.

Conversely, **lower Production Autonomy does not necessarily imply limited power,** highlighting the importance of **distinguishing foreign market presence from domestic vulnerability in digital sovereignty**. In IT and information services, Germany and France combine comparatively lower domestic orientation with strong power positions and substantial outward corporate activity. Lower Production Autonomy here indicates that a larger proportion of their parent-controlled production takes place abroad. Foreign-controlled production hosted domestically represents a separate dimension, which must be assessed through the inward ownership footprint. These two characteristics can coexist but should not be treated as equivalent measures of dependence.

Power and influence also need to be distinguished from network resilience, where the latter can be targeted independently of scale production. In telecommunications, the United States leads in production volume and influence, whereas Japan and China record the highest Network Resilience scores. In electronics, China combines the largest production footprint with a Network Resilience score of only 10 on the normalised scale. These differences show that productive scale, outward influence and the network characteristics captured by the resilience indicator represent distinct capabilities. The latter should be interpreted as a structural proxy rather than direct evidence of how an economy would withstand a particular disruption.

Similarly, network centrality and influence do not produce the same country ranking, suggesting that policymakers should **track network centrality to identify where foreign entities occupy dominant intermediary positions in corporate networks, even if those entities hold smaller total production volumes**. In telecommunications, China achieves the maximum normalised Network Centrality score of 100, compared with 21 for the United States, despite US leadership in other influence indicators. Centrality captures an economy's position within the ownership network, while influence indicators capture other aspects of productive control and network propagation. The results demonstrate this distinction, but do not establish whether it arises from differences in corporate concentration, economic diversification or other underlying factors.

Insights on EU27

The EU27's weighted average position in the upper-right quadrant across all sectors highlights the potential benefits of integration and cooperation among Member States. While many individual EU countries may be characterized as Limited Players, their collective strength and interconnectedness can lead to a more influential and resilient European presence in the global digital economy. This result underscores the value of the EU's single market, which can help to amplify the impact of individual Member States and promote a more cohesive and competitive European presence on the global stage.

Another key finding is the **substantial structural variation across Member States**. The production-weighted EU27 average falls within the Global Influencer quadrant in all three sectors, while most Member States occupy the low-power, low-interconnectedness quadrant labelled "Isolated Autarkies". Leadership is concentrated among a limited number of countries and varies by sector: Germany and France stand out in IT services, France in telecommunications, and Germany and the Netherlands in electronics. **The EU27 average therefore summarises an uneven distribution of capabilities;** it should not be interpreted as evidence that all Member States share the same position or act as a unified production network in these areas, nor does it necessarily reflect their relative strengths or weaknesses in other sectors or areas of the economy. Likewise, the "Isolated Autarky" classification indicates a relative position within this framework, rather than literal economic isolation or technological self-sufficiency.

The EU's external production relationships further underline the need for sector-specific interpretation. **In 2023, EU-controlled production outside the Union amounted to 0.32 times non-EU-controlled production inside it in IT services and 0.48 times in telecommunications, compared with 1.14 times in electronics.** Partner concentration adds another dimension: US parents account for 80.8% of the EU's non-EU-controlled IT services production, whereas UK parents account for 56.5% in telecommunications. These patterns identify asymmetries in corporate control, whose strategic implications depend on the activities involved, available alternatives and the concentration of critical capabilities.

6. Asymmetric dependence in products underpinning digital sovereignty

6.1. Introduction

Ensuring secure access to the technologies, components and materials underpinning the digital economy has become an increasingly important dimension of the EU's competitiveness, economic security and technological sovereignty. This reflects a series of disruptions over recent years that have exposed vulnerabilities in highly integrated and geographically concentrated technology value chains.

Semiconductors provide a particularly prominent example. Starting in 2020, the global semiconductor shortage disrupted production across a wide range of European industries and highlighted the EU's dependence on a limited number of suppliers and production locations. The Commission's 2022 assessment underpinning the European Chips Act pointed to structural vulnerabilities across the semiconductor value chain and to the potential exposure of European industry to third-country export restrictions and other disruptions. This experience contributed to the adoption of the European Chips Act in 2023, aimed at strengthening the EU semiconductor ecosystem, increasing the resilience of the supply chain, and reducing external dependencies.

Since then, geopolitical tensions and the growing use of trade and technology restrictions have further brought the security of technology supply chains to the fore. In 2023, China introduced export controls on Gallium and Germanium, two critical raw materials used in semiconductor and other advanced technology applications. At the same time, restrictions on access to advanced semiconductors and semiconductor manufacturing technologies have become an increasingly important feature of international technology competition. These developments illustrate that vulnerabilities can emerge at different points of digital value chains, from access to critical materials and specialised manufacturing equipment to advanced components and final technologies.

These developments have also taken place against a broader reorientation of EU economic policy. The European Economic Security Strategy, adopted in June 2023, identified supply-chain resilience, technology transfer, and the weaponisation of economic dependencies among the main categories of risk to the EU's economic security. Advanced semiconductor technologies were subsequently identified, in October 2023, as one of four critical technology areas requiring further collective risk assessment. The Competitiveness Compass, presented in January 2025, further placed the reduction of excessive dependencies at the centre of the EU's competitiveness agenda, alongside efforts to close the innovation gap and decarbonise the economy. Most recently, the European Tech Sovereignty Package, presented in June 2026, has brought these objectives more explicitly into the digital sphere, with a focus on strengthening European technological and industrial capacity in strategic areas, including semiconductors, AI and cloud, and on securing the supply of critical digital technologies.

Taken together, these initiatives point to a common policy objective: strengthening the EU's capacity to develop and access strategic technologies while reducing vulnerabilities arising from excessive or asymmetric external dependencies.

This does not imply pursuing self-sufficiency. Digital value chains are hyperconnected and inherently global. Therefore, access to international markets, technologies, and inputs remains essential for EU competitiveness. **The policy challenge is to distinguish economic**

interdependencies that support an open and competitive European economy from dependencies that may give rise to vulnerabilities. This requires looking not only at whether the EU relies on external supply, but also at where this reliance is concentrated and at the balance of dependence between the EU and individual trading partners. A high level of external exposure may be particularly relevant where a specific third country accounts for a significant share of EU supply while the EU represents only a limited market for that country's exports. Conversely, the dependence may run in the opposite direction where the EU has a stronger domestic supply position and represents an important source of supply for a third country that accounts for only a limited share of EU exports.

Against this background, the analysis develops a product-level approach to examine the EU's trade position in products underpinning digital sovereignty.[51] It proceeds in two steps. First, it identifies the products relevant for digital sovereignty that can be captured through international trade statistics. Second, it combines information on EU production and international trade to assess external exposure and bilateral trade relationships. This makes it possible to identify asymmetric dependencies in both directions: products for which the EU is asymmetrically dependent on a third-country partner, pointing to a potential EU vulnerability, and products for which a third country is asymmetrically dependent on EU supply, pointing to a position of relative EU strength.

6.2. Products relevant to digital sovereignty

Translating these policy considerations into a product-level trade analysis requires first defining the set of products that underpin digital sovereignty capabilities. There is currently no internationally agreed product classification specifically designed to capture digital sovereignty. Existing classifications, including ICT, high-technology and dual-use products, cover important parts of the digital economy, but do not provide a sufficiently comprehensive basis for examining dependencies across the technologies, components and inputs supporting digital value chains. **This section therefore develops a dedicated taxonomy to identify international traded products classified according to their role in underpinning digital sovereignty**, rather than the industrial sector in which they are produced. The identification followed a multi-stage process (**Figure 44**). Starting from the full HS2017 nomenclature - the international classification used to categorize products for import and export [52] - the screening considered products relevant for computing, data storage and cloud infrastructure, telecommunications, semiconductor production, cybersecurity hardware, sensors and industrial automation, materials and energy infrastructure.[53] The analysis is conducted at the 6 digits (HS6) level, the most detailed product classification that is internationally harmonised across countries, allowing individual product categories to be consistently identified and compared across trading countries. A structured Large Language Model

---

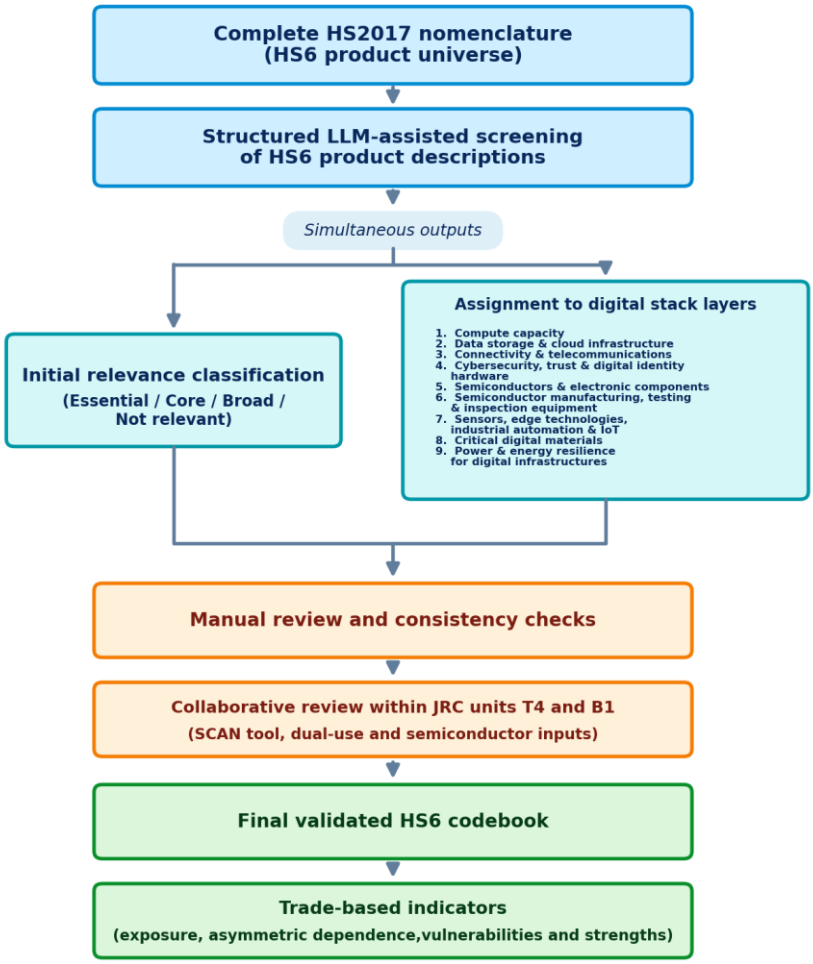
[51] The objective is not to identify all products potentially associated with digital activities, but rather to construct a transparent, reproducible and policy-oriented codebook suitable for measuring import dependencies, supplier concentration, strategic vulnerabilities and indispensability.

[52] This level of aggregation allows for the identification of specific product types and enables the combination of data on global trade, including flows between third countries and product heterogeneity.

[53] **The taxonomy is intended to capture the trade dimension of digital sovereignty** and is therefore limited to physical products recorded in merchandise trade statistics. Other important dimensions – including software, digital services, data flows, intellectual property and cloud services – fall outside the scope of this analysis.

prompt (ChatGPT) [54] assessed each description against predefined criteria, flagged relevant products and proposed a classification. This initial screening was subsequently subject to manual review and expert validation, including through the assessment of dual-use products and additional semiconductor-related as identified in the SCAN methodology (see Bonnet et al. 2025).

Figure 45. Workflow for the identification and validation of the HS6 codebook. Source: own elaboration



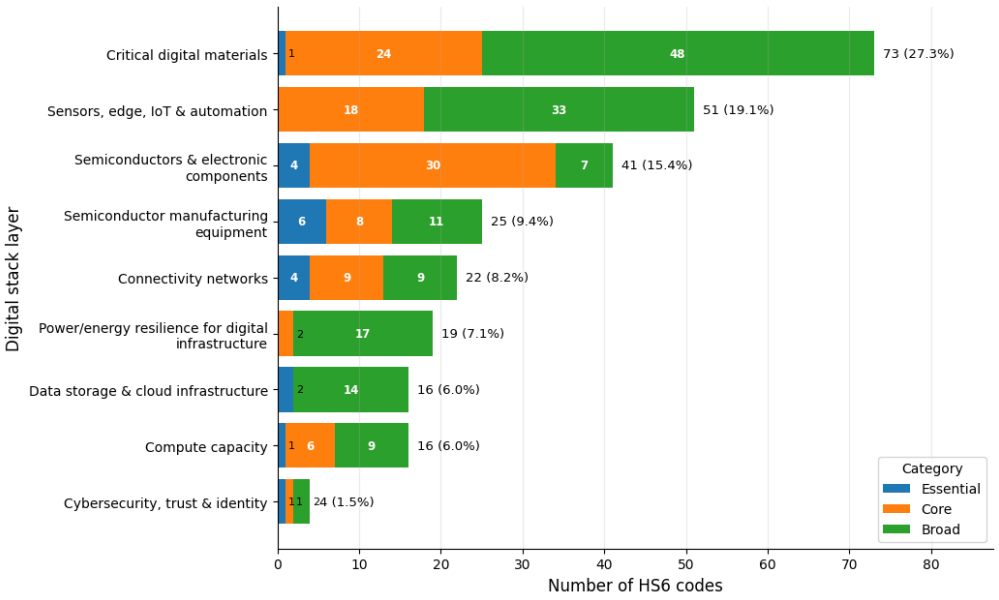
Source: JRC

The resulting sample contains **267 HS6 products**, grouped into **nine digital stack layers**: critical digital materials, sensors-edge-IoT & automation, semiconductor & electronic components, semiconductor manufacturing equipment, connectivity networks, power/energy resilience for digital infrastructure, data storage & cloud infrastructure, compute capacity, and cybersecurity-trust & identity. The full product classification is available through the JRC Open Data Catalogue (Elmallakh et al., 2026).

[54] Model used: GPT-5.4. Accessed through GPT@EC - the European Commission's corporate general purpose generative AI solution

The largest technology layer is critical digital materials, with 73 products, followed by sensors, edge, IoT and automation (51) and semiconductors and electronic components (41) (**Figure 45**). The resulting composition reflects the fact that digital sovereignty depends not only on final digital goods, but also on the components, enabling technologies and selected critical inputs required to produce and operate them.

Figure 46. Cross-classification of HS6 codes by digital stack layer and analytical relevance category.

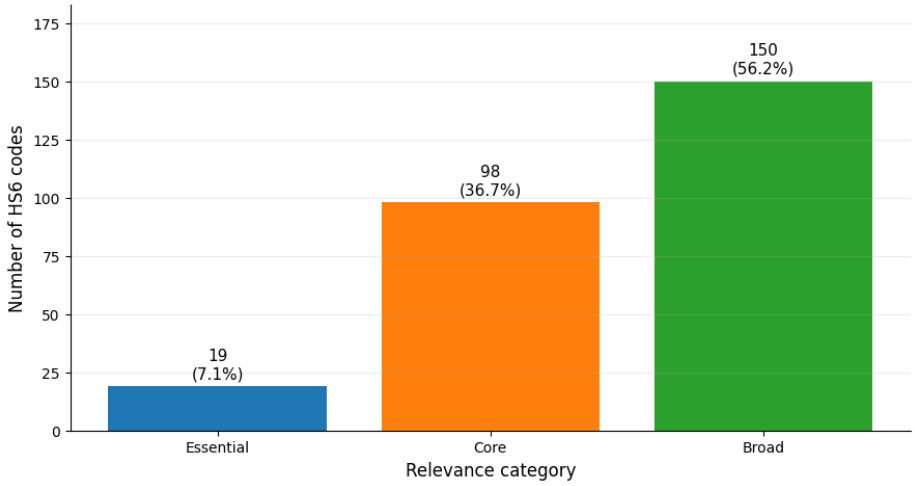


Source: JRC

Notes: Labels at the end of each bar report the total number of HS6 codes in the digital stack layer and its percentage share of the final codebook.

To reflect differences in the strength of the link with digital capabilities, products are classified into three relevance groups. The *essential* group covers 19 digital products (7.1%), including integrated circuits, semiconductor manufacturing equipment, computing hardware, storage devices and strategic networking infrastructure. The *core* group extends the perimeter to 98 important enabling technologies and components (36.7%), while the *broad* group captures the wider digital ecosystem and selected upstream 150 inputs (56.2%) whose relevance for digital technologies is important but less specific at HS6 level (**Figure 46**).

Figure 47. Distribution of HS6 codes by analytical relevance category



Source: JRC

6.3. EU strengths and vulnerabilities: exposure and asymmetric bilateral dependence

Imports and exports provide a first indication of the EU position in products underpinning digital sovereignty, but trade flows alone do not provide the full picture of potential dependences. Large imports may reflect limited EU production or may coexist with substantial domestic supply; similarly, a large bilateral trade flow does not reveal whether dependence is predominantly one-sided or runs in both directions.

Assessing potential vulnerabilities and strengths therefore requires looking beyond the scale and direction of trade. **The analysis considers both the extent to which the EU relies on external rather than domestic supply, and how this reliance is distributed across individual trading partners.** Reliance on foreign supply in fact does not necessarily translate into a trade vulnerability. A potential vulnerability may arise where the EU relies significantly on a foreign supplier, while that supplier is comparatively less reliant on the EU market. Conversely, where a third country relies significantly on EU supply while representing only a limited share of EU exports, the relationship may point to a position of relative EU strength.

Building on the conceptual and methodological approach introduced in Bonnet et al. (2026), these relationships are assessed through two complementary dimensions. The first is the EU exposure, which captures the importance of external supply relative to EU production. The second is the bilateral balance of dependence, which assesses how important relationships are for each side. Combining the two makes it possible to distinguish broad external reliance from asymmetric bilateral dependence and to identify potential EU vulnerabilities and positions of relative strength.

From dependence to asymmetric dependence

High reliance on a foreign supplier does not necessarily imply vulnerability. If the EU is also an important market for that supplier's exports, dependence runs in both directions, and the relationship is more reciprocal. A potential EU vulnerability arises where the EU relies significantly on a specific supplier while that supplier relies only to a limited extent on the EU market. The same logic applies in reverse: where a third country relies significantly on EU supply while representing only a limited share of EU exports, the relationship points to a position of relative EU strength.

6.3.1. Data inputs

The analysis combines detailed trade and production data for all products identified above to construct a product-level dataset covering the EU's trade relationships with third countries and its domestic production capacity.[55]

Trade data refer to 2024 and are sourced from the BACI database.[56,57] Flow is particularly concentrated in core and broad products, which account for the largest import and export values across the categories. Essential products are associated with comparatively smaller export and import values. (**Figure 47**).

EU trade balance in these products varies markedly across trading partners (**Figure 48**). In 2024, the EU deficit was heavily concentrated in East and Southeast Asia, most notably with China. By contrast, the EU recorded surpluses with a broad range of other partners.

Trade data are then combined with information on EU domestic production from Eurostat Prodcom58 to assess the relative importance of external and domestic sources of supply, providing the basis for the exposure indicator used in the subsequent analysis.[59]

---

55 Very low import values have been removed, specifically those lower than € 10,000. The trimming involves around 46% of total number of exporter-product pairs when looking at EU imports and 24% of total number of importer-product pairs when looking at EU exports. However, these observations account for only 0.0038% of total EU import value and 0.0077% of total EU export value, respectively.

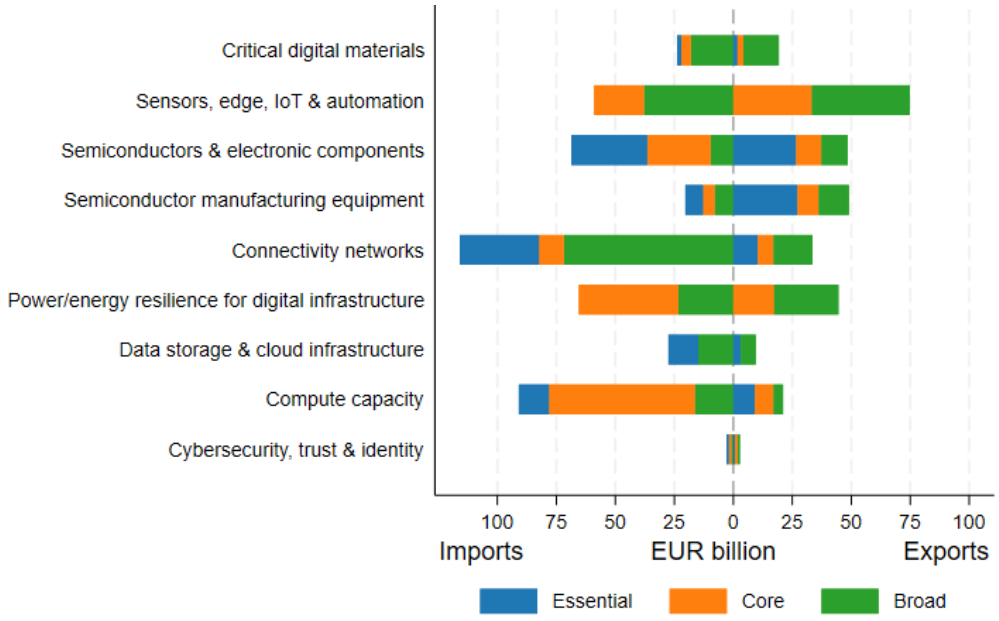
56 BACI is a publicly available database that provides data on bilateral trade flows for 200 countries, including EU and extra-EU bilateral flows, at the product level (5000 products). Products correspond to the "Harmonized System" nomenclature (6 digit code). BACI relies on data from the United Nations Statistical Division (Comtrade dataset). The extraction has been done for all chapters and took place in July 2026. Trade values are expressed in thousand US dollars and converted to euros

57 China, HK, and MO have been aggregated into one single country group (excluding the intra-region trade).

58 Prodcom is based on a European survey of manufacturing production.

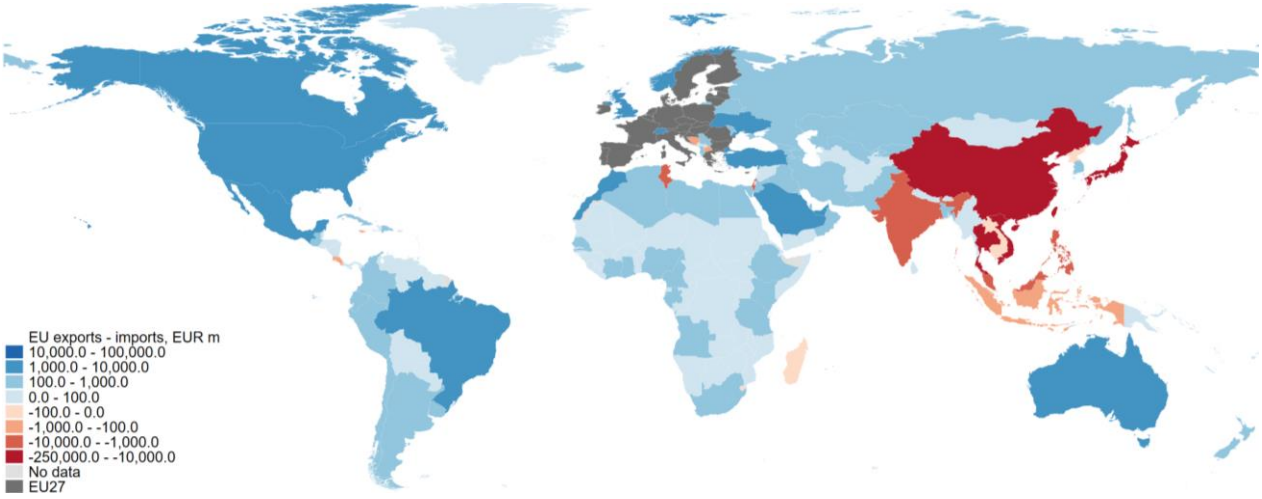
59 Integrating BACI and Prodcom requires addressing differences between their product classifications. Prodcom is broadly linked to the EU Combined Nomenclature (CN), but the correspondence is not always one-to-one. Trade data are generally available at a finer level of product detail, resulting in one-to-many and, in some cases, many-to-many relationships between Prodcom and CN codes. Since the CN is itself based on the international HS classification, these discrepancies also affect the conversion of production data to the HS6 level used in the analysis. To address this issue, the analysis applies the allocation procedure developed by Grasso et al. (forthcoming) as proposed in Bonnet et al (2026). Where a Prodcom category corresponds to several more detailed

Figure 48. EU27 extra-EU imports and exports of products relevant for digital sovereignty, by value-chain position and relevance category, 2024



Source: JRC analysis based on BACI data.

Figure 49. EU27 trade balance with third countries for products underpinning digital sovereignty, 2024



Source: JRC analysis based on BACI data.
Notes: Values are summed across all digital HS6 products by partner. China includes Hong Kong and Macao.

CN8 products, production is allocated across the corresponding CN8 codes according to their shares in total EU exports. The resulting production estimates are then aggregated, together with the trade data, to the HS6 level. This procedure makes it possible to exploit the additional information contained in Prodcom while maintaining a common and relatively detailed product classification throughout the analysis.

6.3.2. Analytical approach

The analysis approach **proceeds in two steps**. First, exposure is assessed at product level to determine the extent to which the EU relies on supply from outside the Union (i.e., how much the EU is *dependent* on foreign supply). Second, the analysis moves to individual country to assess whether dependence on a product is concentrated in specific trading partners and whether the importance of the bilateral relationship is asymmetric.

This sequence distinguishes **three related but different concepts: relevance for digital sovereignty, external exposure and asymmetric bilateral dependence.** A product may be relevant for digital sovereignty without the EU being highly exposed to external supply; similarly, high external exposure does not necessarily imply asymmetric dependence on a specific trading partner. The bilateral dimension therefore adds information on who depends more on whom within individual trade relationships.

Exposure

As clarified, the first step assesses the extent to which EU supply of each product relevant for digital sovereignty relies on imports from third countries. External exposure is defined as the share of extra-EU imports in total (gross) EU supply:[60],

$$Exposure_p = \frac{M_{extraEU27,p}}{M_{extraEU27,p} + Y_{EU27,p}},$$

where $M_{extraEU27,k,t}$ denotes EU imports from third countries and $Y_{EU27,kt}$ the domestic EU production of product *p*. The index ranges from 0 to 1 and measures the contribution of foreign supply relative to the combined availability of imported and domestical production. Higher values indicate greater reliance on external supply relative to domestic production, and hence a more limited domestic production base relative to the scale of imports.[61]

Following Bonnet et al. (2026), a 40% threshold is used to distinguish products according to their degree of exposure. Products with an exposure above 0.4 are classified as high-exposure products. For these products, extra-EU imports are large relative to the combination of imports and EU production, pointing to a comparatively limited domestic production base relative to external

---

60 Total gross EU supply is defined as the sum of domestic production and extra-EU imports. It differs from apparent consumption, which additionally subtracts exports. Gross supply is used here because the purpose of the indicator is to assess the relative contribution of external and domestic sources to the availability of a product in the EU, rather than to estimate domestic consumption.

61 Production data are unavailable for around 11% of product-year observations. For these observations, exposure is imputed using the relationship between the production-based exposure indicator and a trade-based proxy calculated from extra-EU imports and EU exports. The proxy is defined as the share of extra-EU imports in the sum of extra-EU imports, extra-EU exports and intra-EU exports. Using observations for which production data are available, the production-based exposure indicator is regressed on this trade-based measure, including year fixed effects. The estimated relationship is then used to impute exposure for observations with missing production data. Total intra-EU exports are used to measure intra-EU traade, in line with Eurostat practice, given their more complete coverage compared with intra-EU imports (see Bonnet et al, 2025)

supply. These products constitute the starting point for the subsequent analysis of potential EU vulnerabilities. Conversely, products with an exposure below 0.4 are classified as low-exposure products. In these cases, EU production is comparatively more important relative to extra-EU imports, indicating a stronger domestic supply position. These products are analysed separately to assess whether this stronger production base is accompanied by bilateral trade relationships that point to a position of relative EU strength.

The second step of the analysis therefore moves to assess for each product whether the EU trade relationship with a specific third-country partner is characterised by asymmetric dependence.

Bilateral trade relationships

Two perspectives are considered: from the import side, the analysis assesses the importance of individual third-country suppliers for EU imports and, reciprocally, the importance of the EU market for those suppliers. From the export side, it assesses the importance of the EU as a supplier to individual third countries and, reciprocally, the importance of those countries as destination markets for EU exports.

The EU exposure position determines how these two perspectives are used. For high exposure products, the analysis looks for potential vulnerabilities. It therefore considers the EU as an importer and assesses whether a substantial share of EU imports comes from a specific third-country suppliers, while the EU represents only a limited share of that supplier exports.

For low exposure products, where EU production plays a comparatively stronger role, the analysis looks instead for potential areas of EU strength. It therefore considers the EU as an exporter and assesses whether a third country relies significantly on EU supply while accounting for only a limited share of EU exports. In this way, the two perspectives capture asymmetric dependence in opposite directions: EU dependence on a third-country supplier and third-country dependence on EU supply.

<u>High-exposure products: the EU as importer</u>

For products with exposure above 40%, the analysis identifies the foreign countries on which the EU relies as suppliers. The first indicator, import share, measures the share of total EU imports of product *p* originating from each third country*:*

$$ImportShare_{EU\leftarrow c,p} = \frac{Import_{EU\leftarrow c,p}}{TotalImport_{EU,p}},$$

where $Import_{EU\leftarrow c,p}$ denotes EU imports of product *p* from country *c*. The indicator therefore captures the relative importance of individual suppliers within the EU's external sourcing of the product. This, however, provides only one side of the bilateral relationship. An important supplier for the EU may itself depend strongly on access to the EU market. To capture this reciprocal dimension, the second indicator, market dependency, measures the share of the supplier country's total exports of product *p* directed to the EU:

$$MarketDependency_{c\rightarrow EU,p} = \frac{Export_{c\rightarrow EU,p}}{TotalExport_{c,p}}.$$

A high value indicates that the EU represents an important destination market for the exporting country.

Taken together, the two indicators capture the relative importance of the bilateral relationship for each side: the importance of the third country as a supplier to the EU and the importance of the EU as a market for that country. EU vulnerabilities arise when the former is high and the latter is low.

Low-exposure products: the EU as exporter

For products with exposure below 40%, the analysis shifts to the export side and focuses on the EU importance as a supplier to third countries. The first indicator, EU share of partner imports, measures the share of country *c* total imports of product *p* originating from the EU:

$$ImportShare_{c\leftarrow EU,p} = \frac{Import_{c\leftarrow EU,p}}{TotalImport_{c,p}},$$

The indicator captures the relative importance of the EU as a source of supply for the third country. A high value indicates that the partner sources a substantial share of its imports of the product from the EU. The reciprocal side of the relationship considers the importance of the third country as a destination for EU exports. The second indicator, partner share of EU exports, measures the share of total extra-EU exports of product *p* directed to country *c*:

$$MarketDependency_{EU\rightarrow c,p} = \frac{Export_{EU\rightarrow c,p}}{TotalExport_{EU,p}}.$$

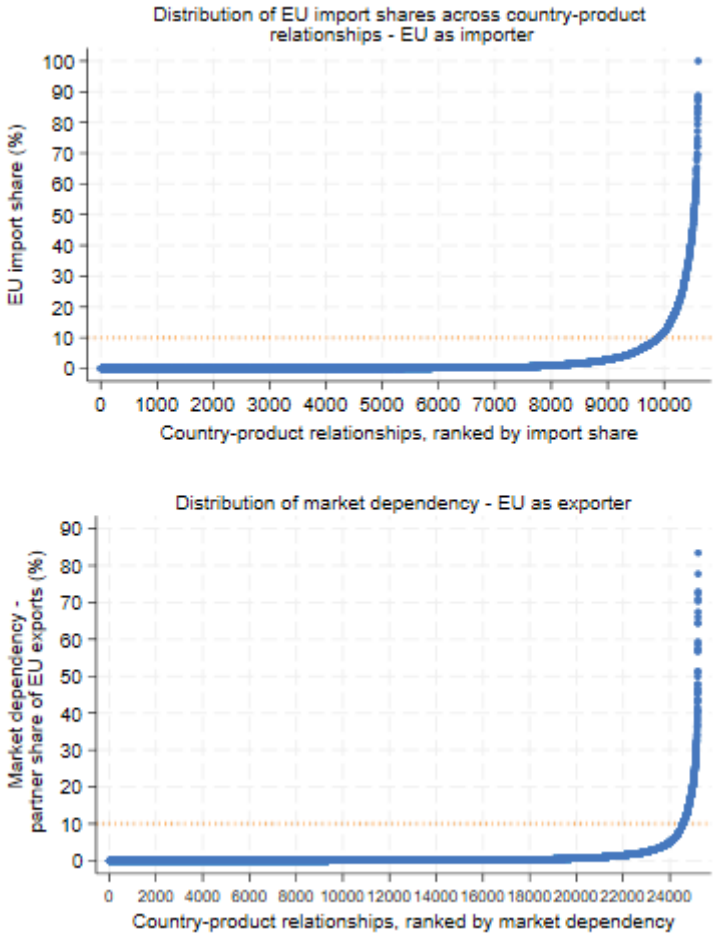
A high value indicates that the partner represents an important destination market for EU exports.

Taken together, the two indicators capture the importance of the EU as a supplier to the third country, and the importance of that country as a market for the EU. A position of relative EU strength arises when the former is high and the latter is low.

Asymmetric bilateral relationships

To identify the bilateral relationships of greatest relevance, the analysis distinguishes between high and low values of the bilateral indicators using a 10% threshold. The threshold is defined from the EU perspective, based on the empirical distribution of individual partners' shares in EU imports and exports. As shown in **Figure 49**, most country-product trade relationships lie below 10% when considering the share accounted for by individual partners in EU imports or exports. A value above 10% therefore identifies cases in which a single third country represents a comparatively important supplier or destination market for the EU.

Figure 50. Distribution of bilateral trade dependence indicators from the EU perspective



Source: JRC analysis based on BACI data

The same threshold is then applied to the reciprocal side of the relationship to assess whether the EU is similarly important for the third country. This provides a common benchmark for distinguishing asymmetric bilateral relationships. The 10% threshold should therefore be interpreted as an empirical screening criterion, rather than as a structural definition of dependency.

To sum up, combining the bilateral indicators with the initial exposure measure allows two types of asymmetric relationships to be identified. **For high-exposure products, a potential EU vulnerability** ("EU asymmetric dependence on the partner") is identified **where a third country accounts for more than 10% of EU imports, while the EU absorbs less than 10% of that country's exports** of the product. **For low-exposure products**, the reverse configuration is considered: a **potential EU strength** ("Partner asymmetric dependence on the EU") is identified **where the EU supplies more than 10% of a third country's imports, while that country accounts for less than 10% of EU extra-EU exports** of the product. Table 19 summarises the resulting screening approach.

Table 20. Approach for identifying potential EU vulnerabilities and strengths in trade positions

Exposure	Perspective	Import share	Market dependency	Identification
> 0.40	EU as importer	EU Import share > 10%	EU share of partner exports < 10%	EU asymmetric dependence on the partner (**potential vulnerability**)
< 0.40	EU as exporter	EU share of partner imports > 10%	Partner share of EU exports < 10%	Partner asymmetric dependence on the EU (**potential strength**)

Methodological framework

For high-exposure products (>40%), a potential EU vulnerability is identified when a partner supplies more than 10% of EU imports while the EU accounts for less than 10% of that partner's exports; for low-exposure products (<40%), a relative EU strength is identified when the EU supplies more than 10% of the partner's imports while that partner accounts for less than 10% of EU exports

Source: JRC

6.4. Results on trade dependencies and bilateral relationships

On the import side, the screening identifies **31 products,** accounting for **EUR 18.6 billion** in selected EU imports**, for which in 2024 the EU is potentially vulnerable to at least one third-country supplier**. The fact that only a subset of the products is identified by bilateral screening highlights the distinction between strategic relevance for digital sovereignty, external exposure, and asymmetric bilateral dependence. A product may be relevant for digital sovereignty without the EU being highly exposed to external supply or asymmetrically dependent on a specific trading partner. In particular, even high external exposure does not necessarily imply asymmetric dependence on an individual supplier.

On the export side, the screening identifies **125 products,** accounting for **EUR 72.8 billion** in selected EU exports, **associated with potential EU strengths.** For these products, at least one third country depends relatively strongly on EU supply, while that country represents a comparatively less important destination for EU exports. The substantially larger number of products identified on the export side suggests that potential EU strengths extend across a broader product base than potential EU vulnerabilities.

The section follows with a description of the geographical and product composition of these relationships, with particular attention to whether countries on which the EU depends also display dependencies on EU supply in other products.

6.4.1. Geography of potential EU vulnerabilities and strengths

Across the products identified in Section 2 as relevant for underpinning digital sovereignty, the geography of asymmetric dependence differs sharply between potential EU vulnerabilities and strengths (**Figure 50**).

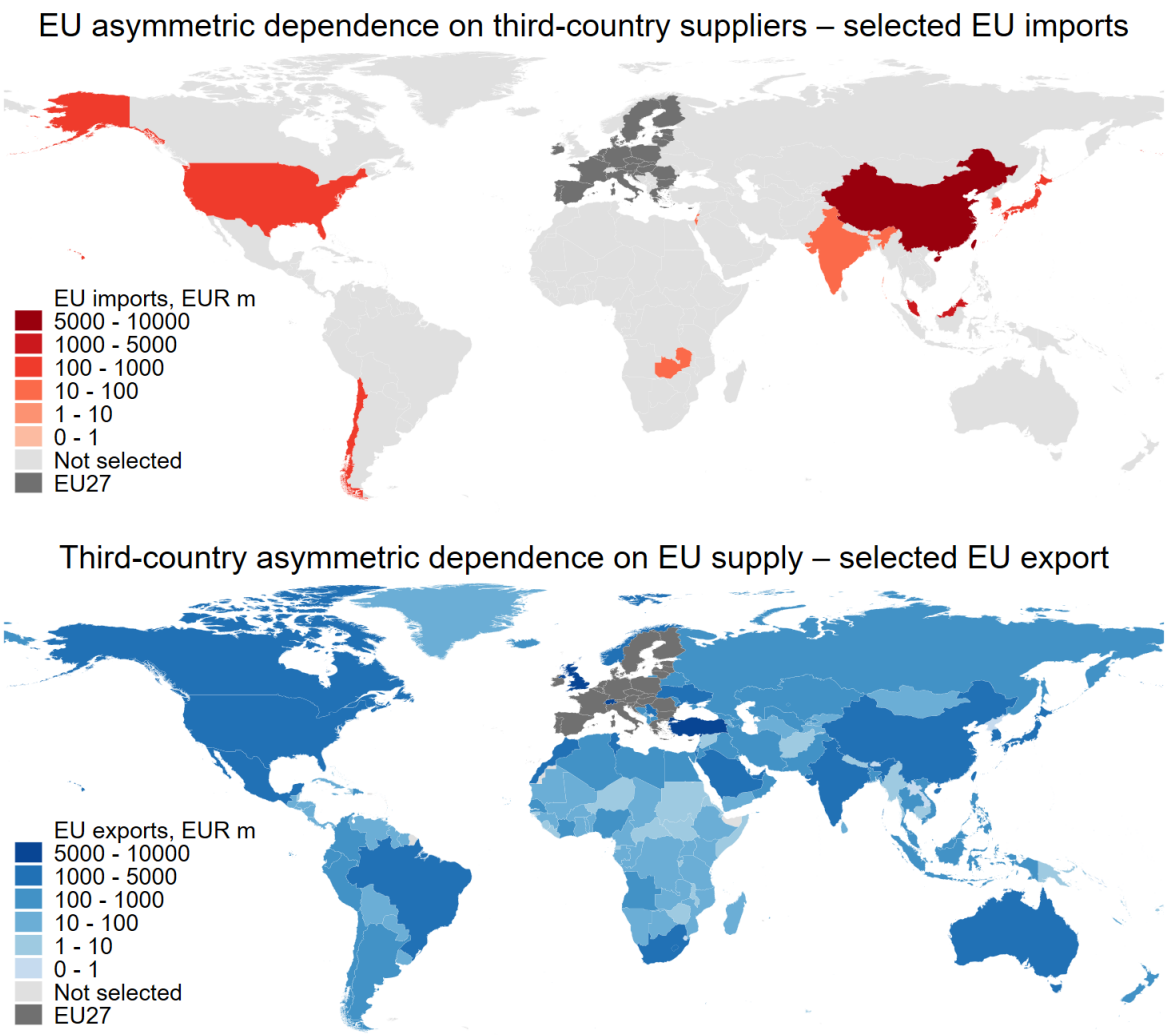
Potential EU vulnerabilities are confined to only **11 partners** and are strongly concentrated in East and Southeast Asia. **Taiwan**, **China** (including Hong Kong and Macao) and **Malaysia** together account for EUR 16.6 billion, or around 90% of the total imports associated with the identified asymmetric relationships. Notably, Taiwan accounts for the largest value, at EUR 6.8 billion, followed by China at EUR 5 billion, and Malaysia at EUR 4.8 billion. Values associated with the remaining partners are considerably smaller (e.g. Japan follows with EUR 0.5 billion). Potential vulnerabilities are also identified outside Asia, including Japan, Korea, Singapore, and the United States, but the associated trade values are considerably smaller. The concentration is therefore not only in the number of partners, but especially in the economic value associated with a small group of Asian suppliers.

Potential EU strengths have a much broader geographical reach, thus reflection the diversified EU industrial capabilities. Third-country asymmetric dependence on EU supply is in fact identified across **188 trading partners** and extending across all major world regions. Among the countries for which potential EU vulnerabilities are also identified, the largest export values associated with potential EU strengths are found for **India**, **Japan** and **Korea**, followed by the **United States.** Potential EU strengths also extend well beyond this group, confirming a much wider geographical distribution than on the vulnerability side.

Geographically concentrated vulnerabilities, widespread strengths

Potential EU vulnerabilities are concentrated in a narrow set of 31 products and 11 partners (EUR 18.6 billion), predominantly in Asia and especially Taiwan, China and Malaysia. Potential EU strengths are substantially broader, spanning 125 products and 188 partners (EUR 72.8 billion), with sizeable relationships including India, Japan, Korea and the United States.

Figure 51. Geographical distribution of asymmetric trade dependency in product underpinning digital



Source: JRC analysis based on BACI data.

Notes: Trade values are summed over selected products by partner. China includes Hong Kong and Macao.

6.4.2. EU vulnerabilities and strengths across selected partners

The concentration of potential vulnerabilities in a relatively small number of partners raises a further question: **do the same countries also depend on EU supply for other products relevant for digital sovereignty?** To address this question, the analysis focuses on the 11 partners with at least one asymmetric dependence on the EU and examines their export-side relationships to identify potential EU strength (**Table 20**). The results show that asymmetric dependencies run in both directions for all 11 partners.

For Taiwan, EU asymmetric dependence accounts for EUR 6.8 billion in selected imports, compared with EUR 1.4 billion in EU exports associated with Taiwan's asymmetric dependence on EU supply. A similar imbalance is observed for China, with EUR 5.0 billion in selected imports compared with EUR

1.5 billion in selected exports. For most of the other partners, however, the pattern is reversed. India stands out particularly strongly, with only EUR 36 million associated with potential EU vulnerabilities compared with EUR 3.8 billion in exports associated with potential EU strengths. A similar pattern emerges for Japan (EUR 0.5 billion versus EUR 3.5 billion), Korea (EUR 0.4 billion versus EUR 3.3 billion) and the United States (EUR 0.3 billion versus EUR 2.4 billion). Singapore and Israel also show substantially larger trade values on the EU-strength side. These differences indicate that the bilateral picture can vary considerably across partners, even though asymmetric dependencies are identified in both directions.

The number of products involved adds a different dimension to this picture. For most selected partners, asymmetric dependence on EU supply extends across substantially more products than EU asymmetric dependence on the partner. The contrast is particularly pronounced for India (1 versus 86 products), Israel (2 versus 103), Chile (1 versus 88), Korea (2 versus 71), Japan (8 versus 63), and Taiwan (5 versus 65). China is distinctive in displaying a comparatively broader set of potential EU vulnerabilities: 17 products, compared with 38 products associated with potential EU strengths.

Trade values and product counts thus show that the economic magnitude of asymmetric dependence is not necessarily related to the number of products involved. The comparison between Taiwan and China is particularly illustrative. EU asymmetric dependence on Taiwan is concentrated in only five products, yet these account for EUR 6.8 billion in selected imports. Dependence on China extends across 17 products, but is associated with a lower aggregate import value of EUR 5.0 billion. At the other extreme, countries such as India and Israel show very limited EU vulnerabilities but a broad range of products for which they are asymmetrically dependent on EU supply.

These two directions should not be interpreted as offsetting one another. They concern different products and potentially different parts of digital value chains. The results instead show that the direction, breadth and economic magnitude of asymmetric dependence are product- and partner-specific.

Table 21. Asymmetric dependence, by partner country, 2024

Country	EU imports: No. of HS6 products	EU imports: Value (EUR million)	EU exports: No. of HS6 products	EU exports: Value (EUR million)
TWN	5	6,803.5	65	1,447.5
CHN+	17	5,023.6	38	1,505.4
MYS	6	4,793.3	48	648.6
JPN	8	461.4	63	3,497.4
KOR	2	428.9	71	3,342.6
SGP	3	386.2	65	1,854.0
USA	4	333.5	13	2,391.9
CHL	1	186.2	88	641.3
ISR	2	55.5	103	1,509.7

ZMB	1	54.5	43	53.5
IND	1	36.1	86	3,793.1
Other countries	**0**	**0.0**	**125**	**52,078.5**
Total	**31**	**18,562.7**	**125**	**72,763.4**

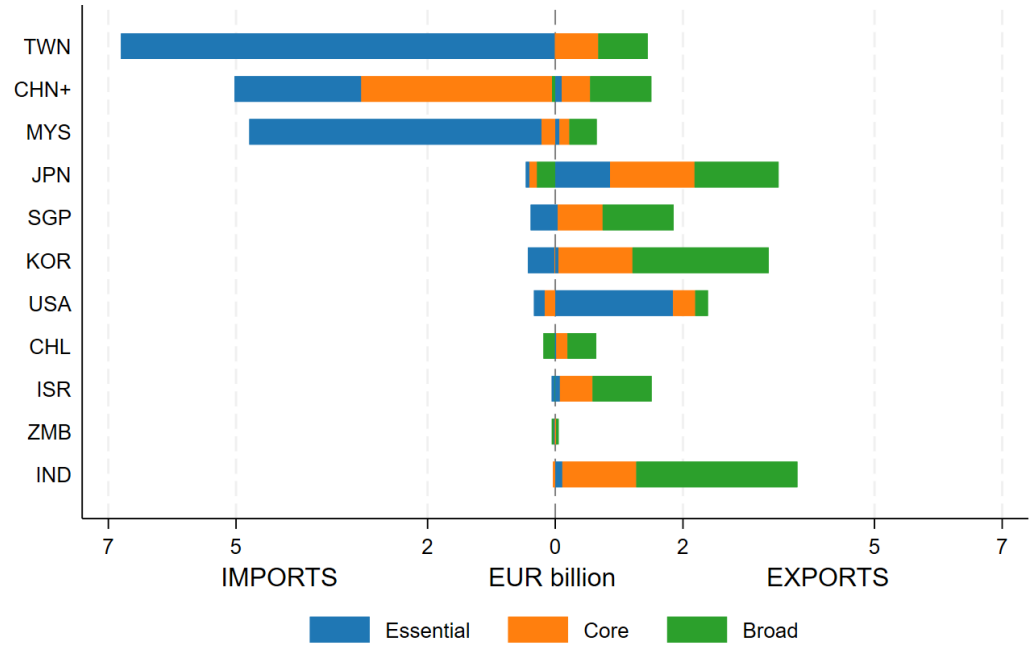
Source: JRC analysis based on BACI data.

Notes: 1) Trade values are expressed in EUR million. 2) EU imports refer to selected country-product pairs with EU asymmetric dependence on the partner (Exposure > 0.4, Import share > 0.1 and Market dependency < 0.1). EU exports refer to selected country-product pairs with partner asymmetric dependence on the EU (Exposure < 0.4, Import share > 0.1 and Market dependency < 0.1. 3) Asymmetric dependencies are reported only for partners for which at least one potential EU vulnerability is identified. 4) Product counts refer to distinct HS6 codes for each partner; the same product may therefore be selected for more than one partner. China (CHN+) includes Hong Kong and Macao. 5) Other countries comprise 173 partners for EU exports and 0 for EU imports; in total, 14 partners are selected for EU imports and 187 for EU exports.

The product composition of these relationships differs across partners and between the two directions (**Figure 51** and **Figure 52**). Potential **EU vulnerabilities** are concentrated in a relatively small number of high-value ***essential*** and ***core*** products. For **Taiwan and Malaysia**, the identified vulnerabilities are strongly concentrated in ***essential*** products, including processors and controllers, other integrated circuits, telecom equipment parts, data-processing units and memory chips. **China** shows a more diversified composition, with both ***essential*** and ***core*** products accounting for most of the import values. In particular, *core* products represent a considerably larger share than for Taiwan and Malaysia, pointing to vulnerabilities extending beyond products most directly underpinning digital technologies to a broader set of enabling products

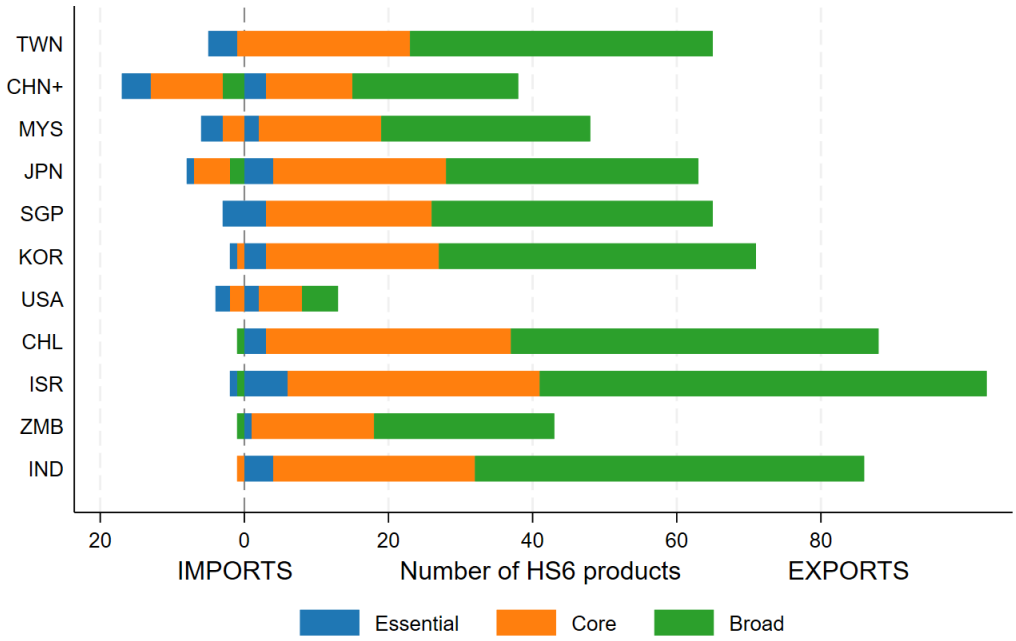
Potential **EU strengths** are considerably more diversified across product categories, with **core** and **broad** products accounting for much of the wider product base across almost all countries, and thus reflecting the more diversified EU industrial capabilities. The **United States** stands out as an exception, with **essential** products accounting for a particularly large share of the trade value associated with potential EU strengths, despite the relatively small number of products involved.

Figure 52. EU27 trade value with selected partners



Source: JRC analysis based on BACI data.
Note: Imports refer to country-product relationships identified as potential EU vulnerabilities. Exports refer to bilateral counter-dependencies for the same set of trading partners.

Figure 53. Number of EU27 traded products with selected partners



Source: JRC analysis based on BACI data.

Notes: Imports refer to country-product relationships identified as potential EU vulnerabilities. Exports refer to bilateral counter-dependencies for the same set of trading partners.

6.4.3. Evolution of asymmetric dependencies over time for selected partners

Comparing the results between 2017 to 2024 shows that potential EU vulnerabilities became substantially larger in economic value while remaining concentrated in a similar number of products. The number of distinct products declined slightly from 35 to 31, while the **associated value of selected EU imports increased by 60%**, from EUR 11.6 billion to EUR 18.6 billion (Table 21). Potential EU vulnerabilities therefore became more concentrated in value, with substantially larger trade flows associated with a slightly smaller product base. This increase was accompanied by a marked **shift in the geographical composition of potential EU vulnerabilities**. China remained a major source of asymmetric dependence, although selected imports declined from EUR 5.8 billion in 2017 to EUR 5.0 billion in 2024. By contrast, selected **imports from Taiwan more than tripled**, from EUR 2.0 billion to EUR 6.8 billion, while those from **Malaysia increased** from EUR 94 million to EUR 4.8 billion. Together, Taiwan and Malaysia accounted for around 62% of selected import value in 2024, compared with around 18% in 2017. Potential EU vulnerabilities therefore not only increased substantially in value but also became more geographically concentrated, shifting towards a small number of Asian suppliers such as Taiwan and Malaysia consistently with the increasing importance of Asian semiconductor production and the reorganisation of global electronics value chains. Over time, Taiwan has in fact consolidated its leading position in semiconductor manufacturing, while Malaysia has strengthened its role in semiconductor assembly, testing and packaging.

Finally, **potential EU strengths show a more stable evolution**. The number of distinct products for which third-country partners are asymmetrically dependent on EU supply declined slightly, from 130 in 2017 to 125 in 2024, while the associated value of selected EU exports increased by 8%, from EUR 67.6 billion to EUR 72.8 billion. There were nevertheless some shifts across individual partners. Selected exports to the United States almost doubled, from EUR 1.2 billion to EUR 2.4 billion, while those to Taiwan increased from EUR 1.0 billion to EUR 1.4 billion and India emerged as one of the largest identified relationships in 2024, with EUR 3.8 billion in selected EU exports. This increased could be explained by the expansion of the digital sector and the associated demand for specialised equipment and industrial inputs. In the United States, investments supported by the US Chips and Science Act[62] have increased demand for semiconductor manufacturing equipment, an area in which European suppliers hold important positions. Similarly, Taiwan's continued expansion of semiconductor production has supported demand for specialised machinery, materials and industrial equipment

Table 22. Asymmetric dependence by partner country, 2017

Country	EU imports: No. of HS6 products	EU imports: Value (EUR million)	EU exports: No. of HS6 products	EU exports: Value (EUR million)
CHN+	18	5,756.9	40	1,633.9
TWN	3	2,003.6	64	986.0

62 US Chips Act

PHL	1	1,007.2	47	227.4
KOR	4	997.5	71	3,264.6
USA	9	696.7	21	1,204.4
VNM	1	540.8	47	285.6
JPN	8	392.6	61	2,402.6
MYS	3	93.7	63	956.6
SGP	2	73.0	66	1,657.6
ISR	2	13.7	110	1,688.3
Other countries	**0**	**0.0**	**130**	**53,294.6**
Total	**35**	**11,575.7**	**130**	**67,601.6**

Source: JRC analysis based on BACI data

Notes: 1) Trade values are expressed in current EUR million. 2) EU imports refer to selected country-product pairs with EU asymmetric dependence on the partner (Exposure > 0.4, Import share > 0.1 and Market dependency < 0.1). EU exports refer to selected country-product pairs with partner asymmetric dependence on the EU (Exposure < 0.4, Import share > 0.1 and Market dependency < 0.1. 3) Asymmetric dependencies are reported only for partners for which at least one potential EU vulnerability is identified. 4) Product counts refer to distinct HS6 codes for each partner; the same product may therefore be selected for more than one partner. China (CHN+) includes Hong Kong and Macao. 5) Other countries comprise 173 partners for EU exports and 0 for EU imports; in total, 14 partners are selected for EU imports and 187 for EU exports.

Concentrated high-value vulnerabilities and diversified product strengths

Asymmetric dependence runs in both directions, but with markedly different patterns. Potential EU vulnerabilities dominate in value for Taiwan (EUR 6.8 vs 1.4 billion), China (EUR 5.0 vs 1.5 billion) and Malaysia (EUR 4.8 vs 0.6 billion), while the reverse holds for most other selected partners, notably India, Japan, Korea and the United States.

EU vulnerabilities tend to involve fewer but high-value products, concentrated in essential products for Taiwan and Malaysia and extending also to core products for China. Potential EU strengths span a much broader product base, predominantly across core and broad products, highlighting that EU strengths in digital value chains extend beyond directly digital products to the broader industrial and technological base supporting their production and use. The United States stands out from this broader pattern, with relatively few but high-value essential products.

The two directions do not offset each other: they concern different products and differ substantially in breadth, economic magnitude and product composition.

Between 2017 and 2024, these patterns evolved differently. The economic value associated with potential EU vulnerabilities increased by 60%, from EUR 11.6 billion to EUR 18.6 billion, without becoming broader in terms of products. Potential EU strengths evolved more gradually, with the value of selected EU exports increasing by 8%, from EUR 67.6 billion to EUR 72.8 billion, despite more substantial increases in some bilateral relationships, notably with the United States and Taiwan.

6.5. Deep dives

A closer look at the individual products behind these relationships reveals well-known dependencies in digital value chains. However, some products that might be expected to emerge do not enter the final selection[63]. This may occur because the bilateral relationship is more reciprocal than required by the screening, but also because dependencies identified for very specific products may not be fully captured at HS6 level. This latter point is particularly relevant for *broad* and *core* products. The screening is conducted at HS6 level, and some HS6 categories encompass products with different technological characteristics and applications. A vulnerability or supply strength concentrated in a specific product may therefore be diluted when assessed together with other products within the same HS6 category.

In this section, the analysis adds a further dimension by considering potential substitutability of the identified asymmetric dependences. An asymmetric dependence may be more significant when alternative suppliers are limited, while an identified EU strength may be reinforced where the EU also holds a strong position in global supply. To capture this dimension, the figures below complement the bilateral indicators with the relevant supplier's share of global exports for each product. Link thickness reflects this share: thicker links indicate a larger global export share and, potentially, lower substitutability. For potential EU vulnerabilities, thicker links therefore identify products for which the foreign supplier may be more difficult to replace. In the opposite direction, they identify potential EU strengths for which the EU accounts for a significant share of global exports and may therefore be more difficult for the partner to replace as a supplier.

Taiwan: concentrated semiconductor-related vulnerabilities

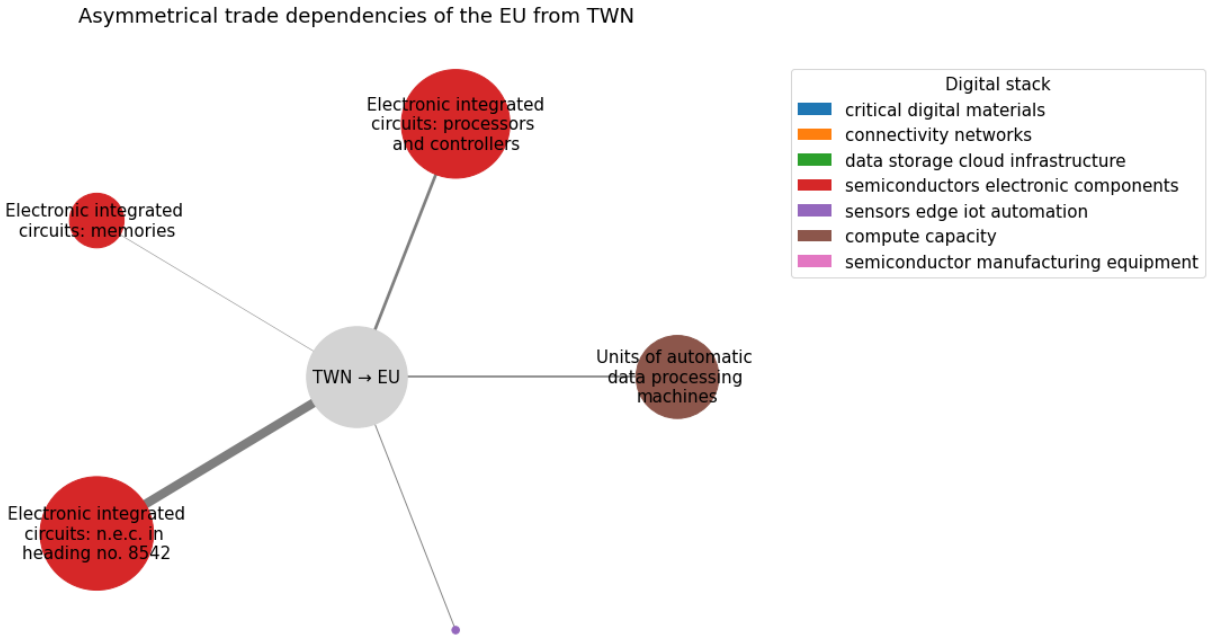
Taiwan represents the clearest example of a concentrated, high-value vulnerability. Only five HS6 products are selected, but together they account for EUR 6.8 billion in EU imports (**Figure 53**). The **vulnerability** is strongly concentrated in **semiconductor and computing products**, including electronic integrated circuits (EUR 2.5 billion), processors and controllers (EUR 2.3 billion), data-processing machines (EUR 1.4 billion), and integrated-circuit memories (EUR 0.6 billion). This pattern is consistent with Taiwan's central position in the semiconductor value chain and with previous evidence on the structure of the EU semiconductor supply chain (Bonnet et al, 2025). Taiwan has in fact been identified as a major source of EU imports of integrated circuits and, in particular, processors and memory products. What stands out in the present analysis is therefore not simply the presence of semiconductors, which is largely expected, but the degree of concentration of the identified vulnerability: a very large share of the EUR 6.8 billion in vulnerable imports is concentrated in only a handful of products. The global export dimension reinforces this finding. For several of the semiconductor products identified, including electronic integrated circuits, processors and controllers, and integrated-circuit memories, **Taiwan accounts for a large share of global exports**. EU asymmetric dependence on Taiwan in these products is therefore accompanied by relatively limited scope for sourcing from alternative suppliers. This is particularly relevant for electronic integrated circuits and processors and controllers, which combine a large bilateral import value with a strong Taiwanese position in global exports. EU asymmetric

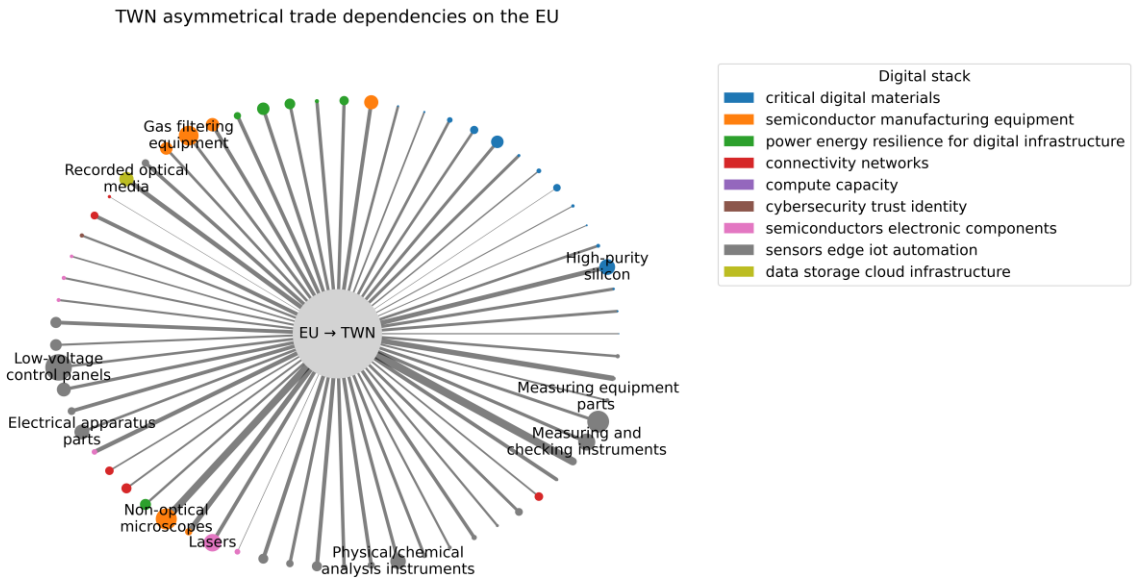
[63] See the sub-section on China below

dependence on Taiwan in these products is therefore accompanied by potentially more limited alternative sourcing options.

The bilateral relationship looks quite different in the opposite direction. Taiwan is asymmetrically **dependent on EU supply across 65 products in the critical materials, semiconductor equipment, sensors edge**, which are associated with around EUR 1.4 billion in EU exports. These EU strengths are widely distributed across the digital supply chain and include products such as gas filtering equipment, recorded optical media, low-voltage control panels, electrical apparatus parts, non-optical microscopes, lasers, physical and chemical analysis instruments, measuring equipment parts, measuring and checking instruments, and high-purity silicon. For some of them, Taiwan dependence on the EU supply is reinforced by the EU strong position in global export thus suggesting more limited alternative sources of supply for Taiwan and reinforcing the potential EU strength identified for these products. This is the case for example of high purity silicon, non-optical microscopes, and lasers.

Figure 54. EU asymmetric dependence on Taiwan and vice versa (Taiwan asymmetric dependence on the EU)





Note: Link thickness is proportional to the exporter share of the product-partner in total trade.

Source: JRC analysis based on BACI data.

Notes: The graphs identify high-exposure products (>0.4) for which the EU shows strong import dependency (import share >0.1) and limited market dependency (<0.1). For the selected exporters, EU import values are aggregated at the HS6 level and products are represented as a node linked to the exporting country. 2) Bubble size reflects import value, colors indicate the product's relevance category, and the link thickness is proportional to the value of exports of that partner-product in global exports.

China: expected vulnerabilities, but also more reciprocal dependencies

China presents a broader and more diversified pattern of potential **EU vulnerability** than Taiwan. In 2024, the EU is asymmetrically dependent on China for 17 products, accounting for EUR 5.0 billion in selected imports (**Figure 54**). The largest selected relationship concerns **materials** (e.g. doped electronic materials), **connectivity networks**, including telecom parts (EUR 2.5 billion), and **semiconductors electronic components, notably other integrated circuits** (EUR 1.3 billion**)** followed by memories and ceramic capacitors. For several of these products, EU dependence is reinforced by China strong position in global exports. This is particularly visible for telecom parts, several materials (such as for which relatively thick links indicate a large Chinese share of global exports. In these cases, China's importance goes beyond its role as a major bilateral supplier to the EU: its position in global exports suggests potentially more limited scope for sourcing from alternative suppliers.

The composition of the selected products is broadly consistent with China position in EU digital-products trade. Telecommunications equipment, electrical machinery and material are among the EU largest import categories from China, while China is also an important supplier across electronics-related value chains. The screening therefore identifies several dependencies that would be expected a priori. **At the same time, some products that might be expected to represent areas of EU dependence do not enter the final selection because the bilateral relationship is more reciprocal than required by the screening**. For Gallium for example, which is an important input into the semiconductor value chain, China occupies a highly

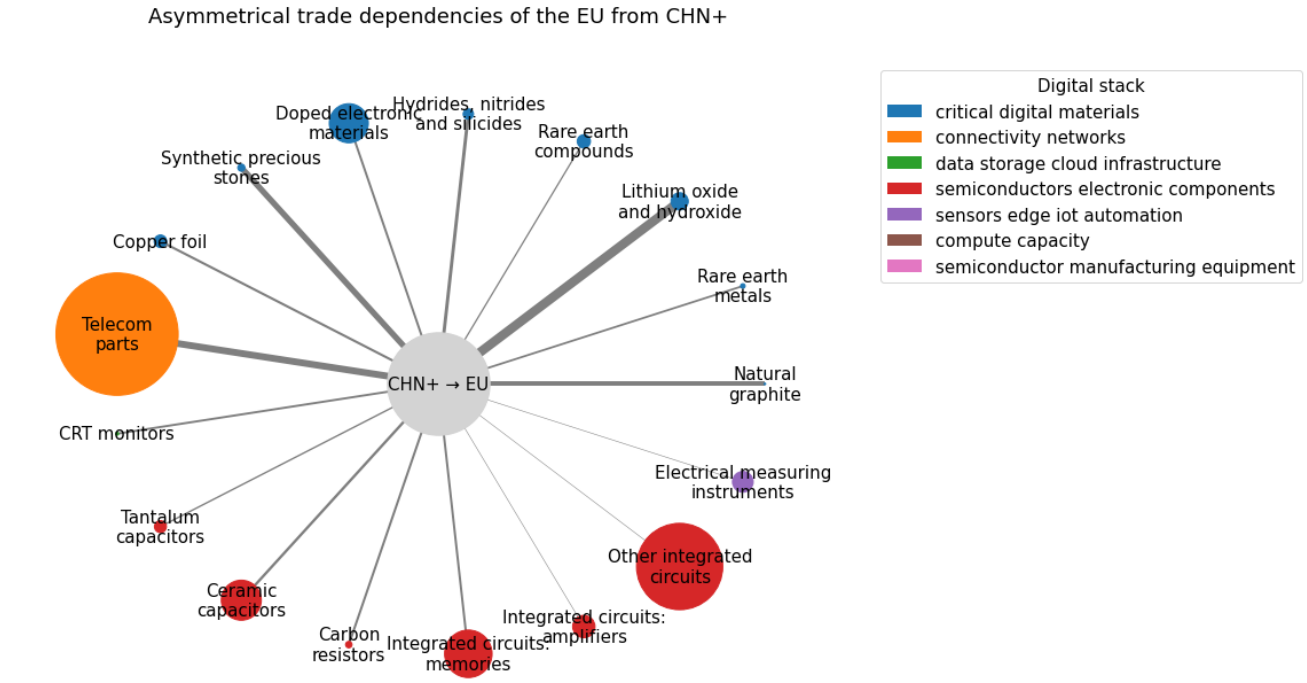
concentrated position in global Gallium production (Bonnet et al. 2025) In the present analysis, however, the relevant Gallium product does not enter the final China vulnerability set because the EU accounts for more than 10% of Chinese exports of the product. The EU is therefore reliant on Chinese supply, but China also relies to a non-negligible extent on the EU market. The absence of gallium from the final selection should consequently not be interpreted as indicating an absence of dependency. Rather, it illustrates the distinction between external dependence and asymmetric bilateral dependence: the first may remain substantial even where the second is not identified by the screening.

The bilateral relationship again looks different when analysed in the opposite direction. The screening identifies 38 products where China is asymmetrically **dependent on the EU**, corresponding to around EUR 1.5 billion in EU exports to China. These potential EU strengths extend across a broader range of products, including **semiconductor equipment (**e.g. semiconductor film and polishing pads, cerium compounds**)**, **connectivity networks (**e.g. radar apparatus, insulated electric conductors**)**, **material** (e.g. aluminium oxide), **power energy** (e.g. industrial fans, air-conditioning equipment, thermal equipment parts,), **cybersecurity trust identity** (e.g. smart cards), sensors edge (liquid and gas meters.), and data storage cloud infrastructure (high-voltage control panels and control-panel parts). Some of these potential EU strengths are further reinforced by the EU's position in global exports, for example semiconductor polishing pads, semiconductor film, industrial fans, cerium compounds, thermal equipment parts, sound equipment parts, control-panel parts, liquid and gas meters, and gases such as argon and nitrogen.

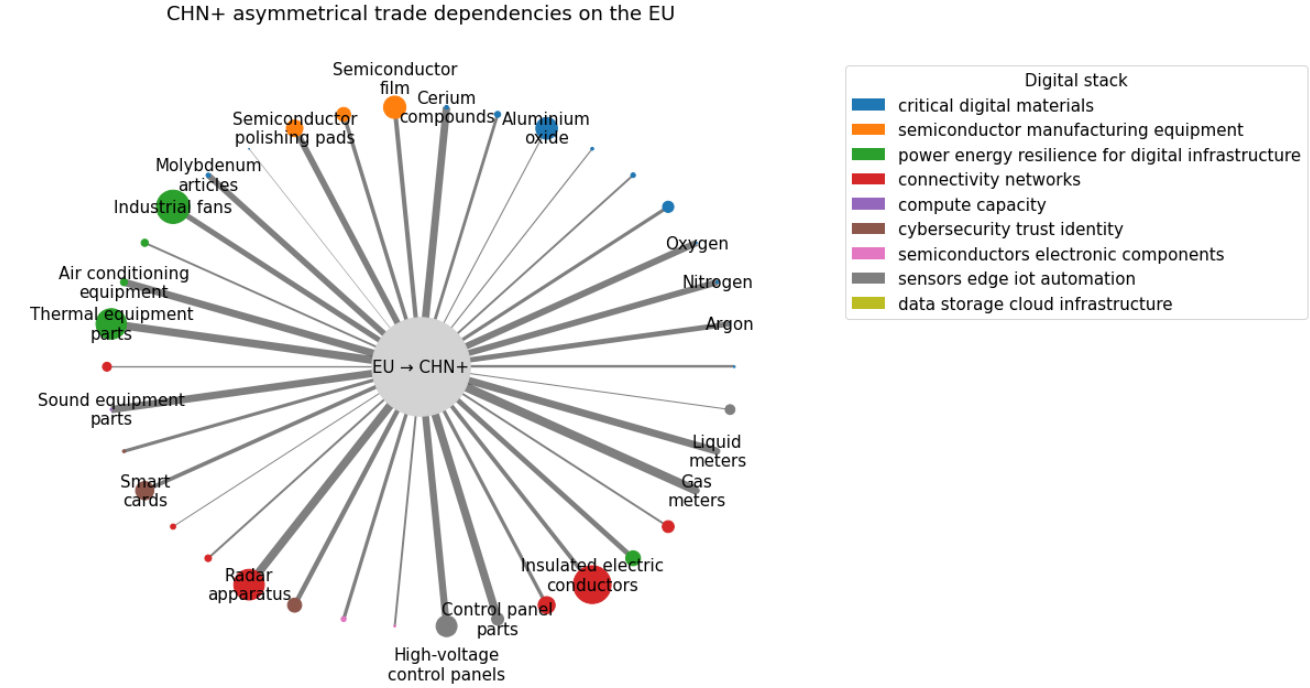
As on the vulnerability side, however, the screening does not capture every product in which the EU might be expected to hold a strong supply position. For example, previous JRC analysis points to significant EU production and a strong export position for high-purity silicon which is a key input into semiconductor wafer production. However, around 45% of EU exports of this product are directed to China. The EU may therefore represent an important supplier for China, but China is simultaneously a major destination market for EU producers. The relationship is consequently characterised by substantial dependence in both directions rather than by the one-sided dependence captured by the counter-dependency screening. A similar consideration applies to semiconductor manufacturing equipment, where Europe occupies a strong position. Recent JRC evidence (Bonnet et al., 2025) also shows the EU as an important exporter of semiconductor manufacturing equipment to China, including lithography. Nevertheless, such equipment does not necessarily appear among the identified counter-dependencies. China itself represents an important destination for EU exports, the bilateral relationship is thus more reciprocal than required by the counter-dependency criterion.

Gallium, high-purity silicon, and semiconductor manufacturing equipment therefore illustrate the two sides of the same mechanism. Gallium represents an expected area of EU dependence on China that does not translate into a selected vulnerability because the EU is also an important market for Chinese exports. High-purity silicon and semiconductor manufacturing equipment represents an expected area of EU supply strength that does not necessarily translate into a selected counter-dependency because China is also an important market for EU exporters.

Figure 55. EU asymmetric dependence on China and vice versa (China asymmetric dependence on the EU)



Note: Link thickness is proportional to the exporter share of the product-partner in total trade.



Note: Link thickness is proportional to the exporter share of the product-partner in total trade.

Source: JRC analysis based on BACI data

Notes: The graphs identify high-exposure products (>0.4) for which the EU shows strong import dependency (import share >0.1) and limited market dependency (<0.1). For the selected exporters, EU import values are aggregated at the HS6 level and products are represented as a node linked to the exporting country. 2) Bubble size reflects import value, colors indicate the product's relevance category and the link thickness is proportional to the value of exports of that partner-product in global exports.

United States: dependencies not fully captured by trade data

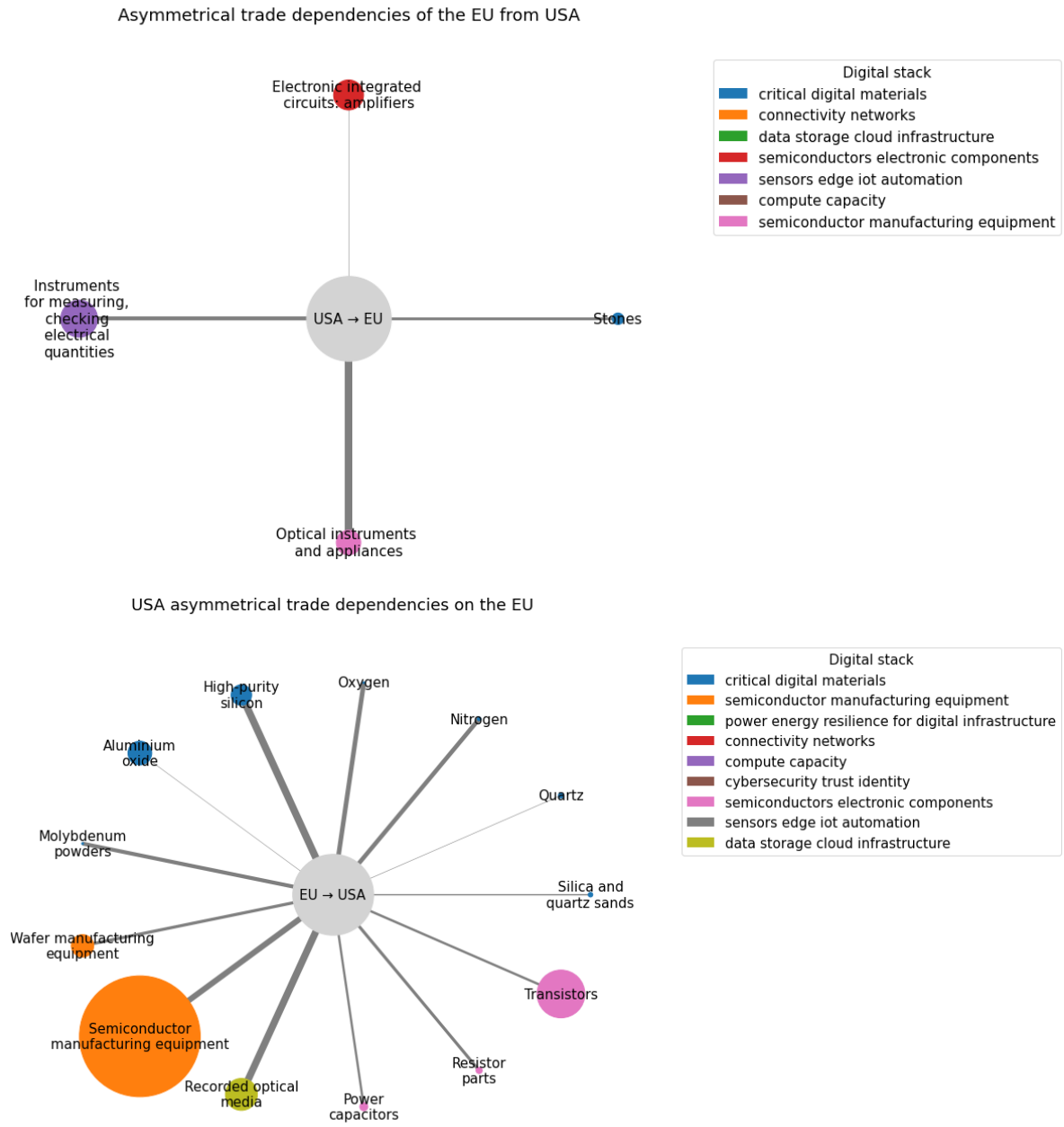
The US is an interesting case. Results show that potential **EU vulnerabilities** are limited to only four products in four digital layers, accounting for around EUR 334 million in EU imports (**Figure 55**). These comprise **electronic integrated-circuit amplifiers**, **instruments for measuring or checking electrical quantities, optical instruments and appliances**, and **stones**. The relatively small number and value of the identified vulnerabilities contrast sharply with Taiwan and China.

These limited vulnerabilities should not, however, be interpreted as indicating that EU digital dependencies on the US are limited. An important part of the US position in digital and semiconductor value chains lies in activities that are not well represented by HS6 trade in goods. This is particularly relevant for cloud provision, data, AI, and semiconductor design and Electronic Design Automation (EDA) tools. Concerning EDA, the European Commission's current semiconductor strategy explicitly identifies semiconductor design as an area in which the EU remains dependent on third countries, while the Chips for Europe Initiative includes access to EDA tools as part of its effort to reinforce European chip-design capacity. Of course, these dependencies are conceptually important for digital sovereignty but cannot be fully captured through a screening based on trade data at HS6 level.

The US case therefore highlights an important boundary of the analysis: the screening identifies asymmetric dependencies embodied in traded goods, but does not provide a comprehensive mapping of dependencies in digital services, software, intellectual property, cloud infrastructure, data or other non-goods dimensions of the digital technology stack.

In the opposite side, potential **EU strengths** are substantially broader. They span a range of products, notably **materials** (e.g. high purity silicon and aluminum), **semiconductors components** and **equipment** (e.g. wafer and transistors). Semiconductor manufacturing equipment stands out in particular in terms of trade value, while several of these products are also associated with relatively thick links, indicating a significant EU share of global exports and potentially lower substitutability of EU supply.

Figure 56. EU asymmetric dependence on the US and viceversa (US asymmetric dependence on the EU)



Source: JRC analysis based on BACI data

Notes: The graphs identify high-exposure products (>0.4) for which the EU shows strong import dependency (import share >0.1) and limited market dependency (<0.1). For the selected exporters, EU import values are aggregated at the HS6 level and products are represented as a node linked to the exporting country. 2) Bubble size reflects import value, colors indicate the product's relevance category and the link thickness is proportional to the value of exports of that partner-product in global exports.

6.6. Conclusions

The chapter develops a framework to identify trade relationships that may be particularly relevant for EU digital sovereignty. The underlying idea is that neither the importance of a product, nor

reliance on imports is sufficient, on its own, to identify a potential vulnerability or strength. The analysis therefore combines three dimensions. It first defines the set of traded products underpinning digital sovereignty; second, it assesses the extent to which EU supply relies on external rather than domestic sources; and, finally, it examines bilateral trade relationships to establish who depends more on whom. For products characterised by high external exposure, the analysis identifies potential EU vulnerabilities where the EU relies significantly on a particular supplier while that supplier is comparatively less reliant on the EU market. For products with a stronger EU production base, the same logic is applied in the opposite direction to identify positions of relative EU strength. The exporter's position in global exports provides an additional indication of potential substitutability. In this way, the framework moves beyond measuring import dependence alone and distinguishes external exposure, bilateral asymmetry and the direction of dependence.

Taken together, these dimensions provide a progressive screening, where each step adds information and narrows the assessment. A product may be relevant for digital sovereignty without the EU being highly exposed to external supply; high exposure may exist without dependence being concentrated in a particular partner; and bilateral asymmetric dependence may be less consequential where alternative suppliers are readily available. Potential vulnerabilities may therefore be reinforced where high external exposure and bilateral asymmetry coincide with a strong global export position of the supplier. The same logic applies in the opposite direction: positions of relative EU strength may be reinforced where a third country relies significantly on EU supply and the EU also accounts for a large share of global exports. The global export dimension remains an additional layer of interpretation rather than a formal criterion of the bilateral screening.

The results identify a relatively concentrated set of potential EU vulnerabilities. Out of the 267 products identified as relevant for digital sovereignty, 31 products are associated with EU asymmetric dependence on at least one third-country supplier in 2024, involving 11 partners and EUR 19 billion in selected imports. The geographical concentration is particularly pronounced: Taiwan, China and Malaysia together account for around 90% of this value. The nature of these dependencies nevertheless differs considerably. Taiwan represents the largest vulnerability and combines a small number of high-value products with a strong concentration in *essential* semiconductor and computing products. China's vulnerabilities are *broader*, spanning 17 products across semiconductor and electronic components, connectivity products and specialised materials and inputs. For several products identified for both countries, their strong position in global exports further reinforces the potential vulnerability by indicating more limited alternative sources of supply.

At the same time, the EU holds positions of relative strength across a considerably broader set of products and partners. The screening identifies 125 products for which at least one third country is asymmetrically dependent on EU supply, involving 188 partners and EUR 73.0 billion in selected EU exports. Their product composition is also more diversified, extending predominantly across *core* and *broad* products and reflecting strengths in a wider industrial and technological base supporting digital production and use. The United States stands out from this general pattern, with relatively few but high-value *essential* products among the identified EU strengths. Dependence can therefore run in both directions within the same bilateral relationship, but across different products. Potential EU vulnerabilities dominate in value for Taiwan, China and Malaysia, while the opposite pattern is observed for most other selected partners, including India, Japan, Korea and the United States. These positions of strength should not, however, be interpreted as offsetting EU vulnerabilities: the two directions differ in product composition, breadth, economic magnitude and potential substitutability. The results also highlight that the EU strengths in digital value chains

extend beyond directly digital products to the broader industrial and technological capabilities supporting their production and use. This contrasts with the greater concentration of potential vulnerabilities in fewer, high-value essential and core products. The distinction is important for digital sovereignty: EU strengths do not necessarily mirror its vulnerabilities product by product, but may instead lie in different technologies, equipment, components and specialised inputs within the wider digital ecosystem.

The comparison between 2017 and 2024 points to different dynamics on the two sides of asymmetric dependence. The economic value associated with potential EU vulnerabilities increased by 60%, from EUR 12 billion to EUR 19 billion, while the number of products declined slightly from 35 to 31. This increase was accompanied by a marked geographical reconfiguration, with Taiwan and Malaysia gaining importance relative to 2017. Potential EU strengths evolved more gradually: selected EU exports increased by 8%, from EUR 67.6 billion to EUR 72.8 billion, while the number of products remained broadly stable, declining from 130 to 125. Aggregate stability nevertheless masks more substantial changes in individual bilateral relationships, including increased values associated with potential EU strengths towards the United States and Taiwan. The evolution therefore combines a sharp increase and greater concentration in the economic value of potential vulnerabilities with a broader and more stable base of potential EU strengths.

The country's cases further illustrate that trade dependence and asymmetric dependence are not equivalent. In the case of China, some expected dependencies do not enter the final selection precisely because the bilateral relationship is more reciprocal. Gallium, for example, does not qualify as a potential EU vulnerability because the EU is also an important market for Chinese exports, while high-purity silicon and semiconductor manufacturing equipment do not qualify as potential EU strengths because China is also an important destination for EU exports. A strong position in global exports can therefore reinforce an identified asymmetric dependence, but does not by itself make a bilateral relationship asymmetric.

The final selection should, all in all, not be read as a comprehensive mapping of all technological dependencies relevant to digital sovereignty. Rather, it identifies the subset of product-country relationships in which trade in products relevant for digital sovereignty displays the particular combination of external exposure and bilateral asymmetry captured by the screening. Products that do not enter the final selection may still be associated with important dependencies, for example where dependence is more reciprocal than required by the screening or where it arises at a level of technological specificity that cannot be captured at HS6 level. They may also fall outside trade in goods altogether.

This last limitation is particularly important for digital sovereignty. The analysis captures trade in goods and therefore only one dimension of digital sovereignty. Dependencies in software, services, intellectual property, cloud infrastructure, data and AI, semiconductor design and other non-product dimensions of the digital technology stack fall, largely, outside its scope. The US illustrates this limitation particularly clearly: the relatively small number of product-level dependencies identified by the screening should not be interpreted as evidence of limited EU digital dependence on the US, since important US positions in areas such as cloud services, data and AI, semiconductor design and EDA tools are not captured by trade data.

Future work could therefore extend the framework by complementing trade in goods with evidence on services and technological capabilities. This would allow the trade-based screening developed here to form part of a broader framework for monitoring EU digital sovereignty and distinguishing normal interdependence within global value chains from concentrated and asymmetric dependencies that may warrant closer attention.

Section D
People



7. Digital sovereignty skills: Emerging perspectives

7.1. Approach, methodology and limitations

7.1.1. Introduction

The general importance of digital skills is strongly recognised by the current Commission (e.g. via the overarching Union of Skills strategy[64], the AI Continent Action Plan[65], the Digital Decade Policy Programme[66], and the Digital Education Action Plan[67]).

Regarding digital sovereignty more specifically, individual skills are also key requisite (Bellini et al., 2025). Although "digital sovereignty skills" has been used to denote general autonomy and confidence in digital environments (e.g., Hartmann & Shajek, 2023; Berkel et al., 2025), digital sovereignty competence goes beyond the ability to use digital technologies effectively and critically. It concerns individuals' capacity to understand and act upon the dependencies, power relations, technological choices and geopolitical conditions that shape their digital environments, to decide how their data is collected, used and shared, and ultimately benefit from their own data and digital identities. It therefore encompasses not only effective participation in digital environments, but also the agency to make informed choices about technologies, data and infrastructures, including the capacity to identify dependencies, exercise rights, retain meaningful alternatives and contribute to shaping digital systems (Di Marco et al., ibid., Fratini et al., 2026; Jansen et al., 2023).

The overall objective of this chapter is to identify indicators of digital sovereignty skills. Identifying and describing digital sovereignty skills and, ultimately, addressing these skills needs, aligns to the objectives of the forthcoming Education Package, which includes digital sovereignty as a theme[68]. The preliminary work in this chapter also aligns to the Commission's June 2026 Technological Sovereignty Package[69]. This Package embeds several policies/strategies including the EU Open Source Strategy, which includes a skills component[70].

64 https://commission.europa.eu/topics/competitiveness/union-skills_en

65 https://digital-strategy.ec.europa.eu/en/library/ai-continent-action-plan

66 https://digital-strategy.ec.europa.eu/en/policies/digital-decade-policy-programme

67 https://education.ec.europa.eu/focus-topics/digital-education/actions

68 A Call for Evidence to support the development of the Package was launched by the Commission in September 2026. One of the three areas for which evidence is sought is Digital Education Infrastructure, which covers *human agency, inclusiveness, and digital sovereignty*. https://education.ec.europa.eu/whats-new/news/commission-launches-call-for-evidence-on-new-education-package

69 https://digital-strategy.ec.europa.eu/en/policies/eu-tech-sovereignty

70 https://digital-strategy.ec.europa.eu/en/policies/open-source-strategy.. The Technical Sovereignty package also includes the proposal for a Cloud and AI Development Act (https://digital-strategy.ec.europa.eu/en/library/proposal-cloud-and-ai-development-act-cada), the proposal for a Chips Act 2.0 (https://digital-strategy.ec.europa.eu/en/library/proposal-chips-act-20), and the Strategic Roadmap for Digitalisation and AI in Energy (https://energy.ec.europa.eu/topics/eus-energy-system/digitalisation-energy-system_en#strategic-roadmap-for-digitalisation-and-ai-in-energy), which are along more infrastructural lines.

7.1.2. Approach

Digital sovereignty skills is a recent and emerging topic, as of yet "largely absent from citizens' competency profiles" (Di Marco et al., 2025, p. 7), and in need of development in education and training contexts (Pawellek et al., 2026).

While the Di Marco et al. (ibid.) model operates primarily at system or EU level, the present analysis seeks to describe knowledge, skills and attitudes that individuals would require in order to enable the forms of agency described by that model.

In this preliminary work, digital sovereignty competence is not conceptualised as one homogeneous competence possessed in different degrees by different people. It is seen instead as a role-differentiated and complementary capacity, where different actors exercise different forms of agency, and contribute toward, digital sovereignty. Inspired by the definition in Di Marco et al.'s (2025) model – "the EU capacity to exercise its independence in the digital domain while remaining open and connected to global networks. It focuses on the ability to decide, invest, and innovate according to European values of democracy, openness, and the rule of law. Rather than implying isolation or protectionism, digital sovereignty refers to strengthening EU skills, infrastructures, and governance to ensure that digital transformation supports competitiveness, resilience, and trust" (Di Marco et al., ibid., p. 2) – we propose a preliminary working definition to guide the identification of specific competences and indicators:

> **Digital sovereignty competence** refers to the capacities of individuals to exercise and enable agency and independence, while remaining open and connected, in the digital domain.
>
> These capacities are role-specific and linked to governance, infrastructural and commercial features of digital environments at individual, institutional, national and supra-national levels.
>
> As both an individual and collective endeavour, digital sovereignty requires alignment in competences between roles.

Here, **the term "competence" is preferred to "skills".** Competence incorporates *knowledge* (conceptual understanding), *skills* (application of knowledge and understanding), and *attitudes* (underlying dispositions or mindsets) and therefore provides a more holistic view of individual capabilities (see, e.g. Cosgrove & Cachia, 2025, p. 16).

Given the emerging nature of digital sovereignty competence and the complexity of this area, it was necessary first to establish a **conceptual structure** into which digital sovereignty competence indicators could be placed. The conceptual structure distinguishes between **three roles.** These roles are **not intended to be exhaustive**: they were selected to represent three key sets of actors within a digital ecosystem, illustrating ways in which different roles exercise agency in relation to digital sovereignty:

- The **general population** (using digital technologies in daily life, working and learning contexts): Competences primarily support the **exercise** of digital sovereignty through informed choice, critical evaluation of information, decide on how data is collected, used, and shared, and ultimately benefit from their own data and digital identities exercise of rights and the ability to recognise and respond to digital dependencies.
- **Non-technology decision-makers** (in public and private organisations, e.g. department managers, Chief Executive Officers): Competences primarily involve **enabling and**

governing digital sovereignty through strategic, investment, procurement and organisational decisions.

- **Technology decision-makers** (in public and private organisations, e.g. IT managers, Chief Information Officers, Chief Technical Officers). Competences primarily support digital sovereignty through choices relating to **implementing and building**, concerning digital infrastructures, architectures, data, interoperability and technological development.

The conceptual structure is used to identify potential indicators of digital sovereignty competences, which are then mapped back to the conceptual structure (**Figure 56**). Competences are considered from two perspectives to provide a structure onto which to map potential indicators.

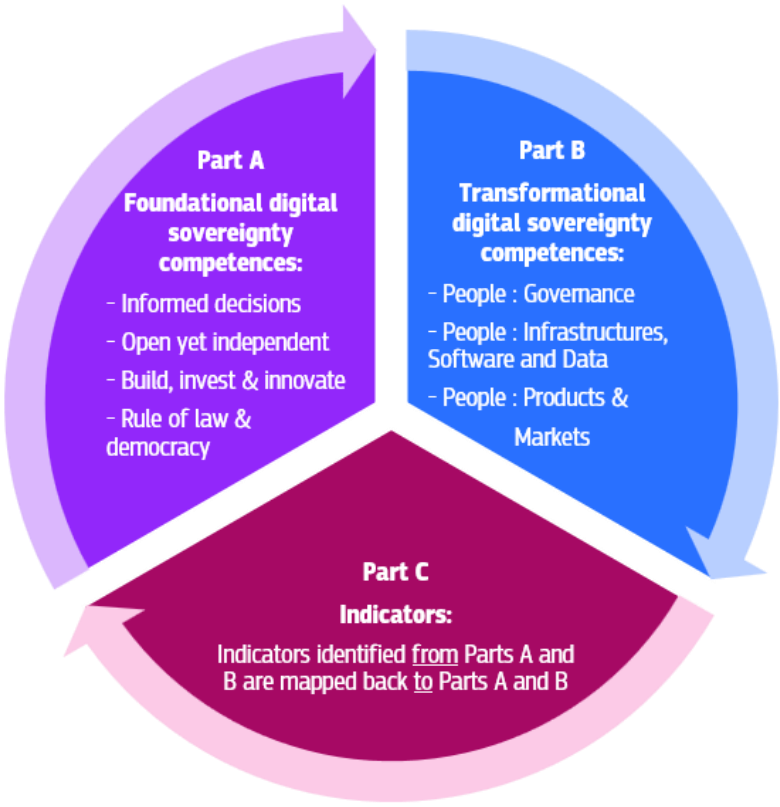
Part A considers **foundational** digital sovereignty capabilities (i.e., core competences) taking four key components of Di Marco et al.'s (2025) model: *informed decisions; open yet independent; build, invest and innovate*; and *rule of law and democracy*.

Part B provides **transformative** competences (i.e., competences that enable movement towards digital sovereignty goals) from the perspective of the four-level model of Di Marco et al. (2025), showing how the *people (skills)* layer links to the other three (*digital governance; digital infrastructures, software and data*; and *digital products and markets*).

Part C describes potential **indicators** and provides some illustrative examples.

The competences in parts A and B are matched to the potential indicators identified in Part C to show which aspects of digital sovereignty competence could be measured through available indicators.

Figure 57. Conceptual and structural overview of the treatment of digital sovereignty competences



Source: JRC

7.1.3. Method

The work was completed using desk-based research and analysis. **Step 1** (conceptualising digital sovereignty competence) was informed through a rapid scoping review in Scopus[71] complemented by a review of EU policy documentation on digital sovereignty and related research of the European Commission's Joint Research Centre (JRC). The process for identifying competences from the literature follows the methodology employed in DigComp 3.0 (Cosgrove & Cachia, 2025, Annex 3). **Step 2** (identification and classification of potential indicators) was informed by findings from the rapid scoping review in Step 1, supplemented by an online search for indicators related to the competences identified in Parts A and B.

7.1.4. Limitations

The main limitation of the research is its nascent stage – it should be regarded as preliminary and exploratory rather than in any way conclusive, and competences described in Parts A and B would ideally be subjected to expert review and validation. Also, the search for potential competence indicators has been largely limited to cross-national sources that include EU countries. It is possible that additional national measures exist. Finally, the indicators themselves, although matched to aspects of digital sovereignty competence, are partial and indirect (proxy) measures, and the viability of some indicators requires further analysis.

7.2. Insights

7.2.1. Foundational digital sovereignty competences (Part A)

Table 19 maps the four foundational digital sovereignty competences to short specific competences derived from relevant literature sources for the three selected roles, also showing in green highlight whether a potentially viable indicator (Part C, **Table 24**) is available for each, and in **bold** the aspects of the competences that are captured by the potential indicator(s). The numbered sources are shown in the References section. Just five of the 12 cells in the matrix have viable indicators, which only partially capture the cells' contents.

[71] Search terms used in Scopus: ("digitally sovereign" OR "digital sovereignty") AND ("skills" OR "competence" OR "competences" OR "competency" OR "competencies" OR "measure" OR "measurement" OR "measures" OR "indicator" OR "indicators"). The timeframe 2020-2026 was applied.

Table 23. Mapping of four foundational digital sovereignty capabilities (based on Di Marco et al., 2025) to three roles and Part C indicators, with specific competences derived from literature

Sovereignty capability area	General population	Non-technology decision-makers	Technology decision-makers
Informed decisions *Exercise independent, informed choice; perceive dependency and power asymmetry.*	• Informed sharing, storage and usage of data • Digital dependencies: identification of technical and commercial risks, power interests and geopolitical dimensions, and dependencies in digital systems one uses • Application of agency and choice in digital services or products • Selection and configuration of digital tools to meet needs **Sources:** 4, 10, 11, 12	• Strategic application of digital-geopolitical landscape knowledge • Judgement, diplomacy and advice-seeking in contested digital contexts • Oversight and monitoring of critical digital dependencies and risks • Oversight of procurement or purchase that embeds digital sovereignty • Monitoring of organisational digital sovereignty goals **Sources:** 10, 11	• Assessment and mitigation of critical digital dependencies and risks • Embedding of digital sovereignty features in procurement or purchase • Application of vendor-independence judgement in vendor selection • Development and implementation of organisational digital sovereignty goals **Sources:** 18
Open yet independent *Retain switching options and interoperability without isolation or protectionism.*	• Recognition of individual and societal benefits of data portability and related concepts (e.g. interoperability, open standards) • Exercise of GDPR and data portability rights • Application of open licences to own digital content **Sources:** 4, 11, 14	• Embedding and monitoring of digitally-sovereign supportive features (e.g. **open source**, EU-made, open standards, interoperability mandates, data-sharing rules) in organisational strategies **Sources:** 11, 16; **Indicators 3 and 4**	• Fostering capacity for interoperable data, processes and systems • Oversight and enablement of build and integration of common components, open data and algorithms • Oversight and enablement of digitally-sovereign supportive features of solutions (e.g. **open source**, EU-made, open standards, interoperability mandates, data-sharing rules) • **Assessment of open source**, open-licensing and proprietary **options** **Sources:** 11, 16; **Indicators 3 and 4**
Build, invest and innovate *Build sovereign products, services and infrastructure; close the innovation-capacity gap.*	• Identification of purposes and benefits of civic participation in digital technological development initiatives • Participation in opportunities to co-shape digital technologies and standards **Sources:** 4, 11	• Implementation of investment and capital deployment strategies that **enhance sovereign digital capacity and skills** • Fostering of **inter-agency collaboration** to support digital innovation and capacity growth	• Active seeking of **inter-agency collaboration** to augment commercialisation and scaling capacity • Support for **development of specialist skills for build and deployment** (e.g. programming, data analysis) that enhance internal capacity • Support for **key technology-build skills needs** (cloud, cyber, AI) where workers

Sovereignty capability area	General population	Non-technology decision-makers	Technology decision-makers
		• Assessment of balance between scaling and R&D • Oversight of intellectual property and licensing to support sovereign innovation **Sources:** 1, 5, 9; **Indicators 2, 5, and 6**	develop or manage critical digital systems • Steering of R&D and software projects towards optimal scope and depth • Strategic management of intellectual property and licensing that supports sovereign innovation **Sources:** 1, 8, 11, 13, 16; **Indicators 2, 5, and 6**
Rule of law and democracy *Assert rights, resist manipulation, and govern by democratic values.*	• Recognition of reasons for and effects of manipulation or interference of digital information and content • Critical assessment of digital contents, sources and processes used to generate them • Identification and assertion of privacy and data protection rights • **Application of cybersecurity tools and processes** • Respect for and application of basic intellectual property rights and obligations • Application of proportionate, lawful and safe processes in data collection, handling and storage (especially in workplaces) **Sources:** 4, 10, 11, 14; **Indicator 1**	• Fostering of transparent and accountable organisational culture • Oversight of measures to strengthen resilience to information manipulation, while protecting individual liberties • Monitoring and enforcement of digital systems, balancing openness, accountability and control • **Sources:** 2, 3, 10, 11	• Prioritising of information integrity in design and oversight of digital systems • Development and oversight of effective data governance strategies - Promotion and oversight of ethical and rights-based data collection, handling and storage - Implementation of measures to strengthen resilience to information manipulation **Sources:** 4, 5, 10, 15, 18

Source: JRC analysis from the literature

Notes: Green highlighted cells denote a potentially viable indicator (Part C), with the aspects of the competences that are captured by the potential indicator(s) in bold. The numbered sources are shown in the References section.

7.2.2. Transformative digital sovereignty competences (Part B)

Table 20 maps the transformative digital sovereignty capabilities to short specific competences derived from relevant literature sources for the three selected roles, also showing in green highlight whether a potentially viable indicator (described in Part C, **Table 24**) is available for each, and in

bold the aspects of the competences that are captured by the potential indicator(s). The numbered sources are shown in the References section.

Table 24. Mapping of transformative digital sovereignty capabilities (based on Di Marco et al., 2025) to three roles and Part C indicators, with specific competences derived from literature

Layer linkage	General population	Non-technology decision-makers	Technology decision-makers
People → Digital Governance *How the skills layer connects to regulation, rule of law and democratic accountability.*	• Recognition and exercise of GDPR/DSA/DMA/AI-Act rights, seeking redress as needed • Application of digital governance rules on algorithmic transparency and accountability (especially in the workplace) **Sources**: 4, 6	• Prioritisation of development of regulatory-adaptability skills in the organisation • Oversight of improvements to address digital governance gaps **Source:** 6	• Identification of digital governance gaps and measures to address them • Enforcement of digital regulations in an inclusive manner • Translation of governance obligations into compliant products or services, accountability practices, communication strategies and end-user supports **Source:** 6
People → Digital Infrastructures, Software and Data *How the skills layer connects to connectivity, interoperability, cloud, cybersecurity and data ecosystems.*	• Recognition of **one's own role in cybersecurity**, and that cyberthreats impact individuals, groups, and digital infrastructure • Application of cybersecurity knowledge and skills (especially social engineering and emerging risks such as in relation to AI), to **protect privacy, personal data** and assets and manage personal data flows • Support-seeking to help verify safety or security of digital infrastructure and tools **Sources:** 4, 6, 7, **Indicator 1**	• Prioritisation of digital investment towards sovereign and sustainable connectivity, cybersecurity and data management • Prioritisation of federation of data and digital infrastructure over duplication • Oversight and monitoring of digital resilience metrics **Source:** 6	• Oversight of data generation, storage, processing and governance • Oversight of builds or upgrades of interoperable, federated data spaces and digital infrastructure • Support for the **development of open source** and cloud/edge engineering **skills** to build sovereign, interoperable infrastructure to reduce hyperscaler dependency • Identification of digital resilience metrics **Sources:** 1, 6, **Indicators 3 and 4**
People → Digital Products and Markets *How the skills layer connects to*	• Identification of digitally sovereign (or sovereign-supporting) digital technologies and elements that sustain their demand	• Promotion of **unique or value-adding digital innovation capabilities** of the organisation • Oversight of strategies to ease R&D and	• Use of in-depth knowledge to purchase or procure digitally sovereign or sustainable products and services • Analysis of digital market trends to shape services

Layer linkage	General population	Non-technology decision-makers	Technology decision-makers
innovation, fair competition and supply-chain autonomy.	• Selection of EU-native / fair-competition digital alternatives according to preferences and needs • Identification of ways in which intellectual property and licensing terms shape digital sovereignty • **Sources:** 6, 13, 14	commercialisation gaps or bottlenecks • Use of intellectual property and patent landscape intelligence to shape innovation, competition and standardisation features • Oversight of strategies to support **development of applied skills needs** • **Sources:** 1, 6, 17**, Indicators 5 and 6**	and products towards demand and vice versa • Analysis of potential causes of and solutions for R&D and commercialisation gaps or bottlenecks • Support for the **development of applied skills needs** in strategic digital technologies (such as semiconductors, cloud, AI) • Management of intellectual property, licensing and freedom-to-operate in procurement and supply chains • **Sources:** 1, 6**, Indicators 5 and 6**

Source: JRC analysis from the literature

Notes: Green highlighted cells denote a potentially viable indicator (Part C), with the aspects of the competences that are captured by the potential indicator(s) in **bold**. The numbered **sources** are shown in the References section.

Each row in **Table 23** describes competences linking the *People* layer and each of the other three layers, i.e., the skills that people in each role need to build, manage, transform and sustain that layer. The rows depict a two-way dependency between roles: the general population needs skills to use and co-shape the lower layers, while non-technology and technology decision-makers need skills to govern, invest in, build and shape them. This two-way dependency also reflects the different forms of agency associated with the three roles. As noted earlier, the general population primarily *exercises* digital sovereignty through its interactions with digital systems; non-technology decision-makers *enable and govern* the conditions under which digital sovereignty can be exercised; and technology decision-makers *implement and build* those conditions through technological and organisational choices. These forms of agency are interdependent rather than hierarchical, making alignment of competences across roles important.

Four of the nine cells in the matrix have a potentially viable indicator, but, as with the foundational competences (**Table 22**), within-cell coverage is very partial.

7.2.3. Potential indicators (Part C)

The measures in **Table 24** are the closest existing candidates that were possible to identify. Each indicator was categorised by:

Type: *Direct* (directly measures a relevant competence) or *Proxy* (an indirect measure)

Data frequency: *regularly available* or *one-off study*

Relevance: each source's fit to the topic, where *high* = the indicator directly targets a sovereignty-relevant individual competence; *medium* = the indicator is a generic or partial proxy; and *low* = organisational, output or supply-side proxy, which is distant from individual competence.

Each indicator was then assessed in terms of its **viability**. An indicator is deemed *potentially viable* and included in **Table 24** if it (i) has a medium or high **relevance** rating, and (ii) is associated with regularly available data (**data frequency**) which permits extraction of meaningful and robust estimates. Six of 12 identified indicators are potentially viable – however, they offer only **partial** competence coverage (**Table 22** and **Table 23**), and major gaps can be observed by considering the non-shaded and non-bolded parts of Tables 1 and 2: no competence measures relating to core aspects such as digital governance, digital dependencies, procurement or intellectual property were found. Content-wise, the indicators touch on aspects of general cybersecurity skills; cross-country software development collaboration; software development capacity and intensity; ICT specialist counts; and training of workers in ICT skills by organisations. They are:

- Indicator 1: Digital Skills Indicator (DSI) 2.0 safety area (general population's cybersecurity and data protection skills)
- Indicator 2: Github innovation graph *connectedness* (cross-economy software developer collaborations)
- Indicator 3: Github innovation graph *capacity* (number of software developers per million inhabitants)
- Indicator 4: Github innovation graph *intensity* (repositories and git pushes per developer)
- Indicator 5: Eurostat ICT specialists in employment (counts and as a % of workforce by country)
- Indicator 6: Eurostat % of enterprises offering training on ICT skills (by organisation size and sector).

Data from 2025 for indicators 2, 3 and 4 are analysed in more depth in **Chapter 2** in this report. They are included in this chapter to show where software development collaboration and capacity fits within the broader landscape of digital sovereignty competences and indicators.

Table 25. List of potentially viable digital sovereignty competence indicators mapped to foundational and transformative digital sovereignty competences and roles (Tables 1 and 2)

Indicator	What it measures	Matrix cell it links to	Coverage / Notes
Indicator 1: Eurostat Individuals' level of digital – skills, safety area [i_dsk2_sf_bab]	Actions in last 3 months: check website security, read privacy statements, block geolocation, limit social media profile access, refuse use of data for advertising, prevent/limit cookies	Part A – General population, Rule of law and democracy Part B – General population, Digital infrastructure, software and data	Population: EU27 individuals aged 16–74; data available every two years since 2021. **Caveat:** Not a direct or comprehensive measure of cybersecurity skills.
Indicator 2: Github innovation graph – *connectedness* (cross-economy software developer collaborations) **See:** Chapter 4 in this report	Degree to which an economy's developer community is integrated into cross-border software development networks	Part A – Non-technology and Technology decision-makers, Build, invest and innovate	Geographical coverage: EU27; data available quarterly since Q1 2020. **Caveats:** Metrics for countries are only reported when there are 100 or more unique developers performing the activity. Github is by far the largest, but not the only, repository of its kind.

Indicator	What it measures	Matrix cell it links to	Coverage / Notes
Indicator 3: Github innovation graph - *capacity* (software developers per million population) **See:** Chapter 4 in this report	Relative size of the software developer community in relation to its population, indicating extent of software development participation within the population	Part A - Non-technology and Technology decision-makers, Open yet independent Part B – Technology decision-makers, Digital Infrastructures, Software and Data	Geographical coverage: EU27; data available quarterly since Q1 2020. **Caveats:** Metrics for countries only reported when there are 100 or more unique developers performing the activity. Github is by far the largest, but not the only, repository of its kind.
Indicator 4: Github innovation graph - *intensity* (repositories and git pushes per developer) **See:** Chapter 4 in this report	In addition to size of developer community (Indicator 3), Indicator 4 provides an indication of the level of activity	Part A - Non-technology and Technology decision-makers, Open yet independent Part B – Technology decision-makers, Digital Infrastructures, Software and Data	Geographical coverage: EU27; data available quarterly since Q1 2020. **Caveats:** Metrics for economies only reported when there are 100 or more unique developers performing the activity. Github is by far the largest, but not the only, repository of its kind.
Indicator 5: Eurostat ICT specialists in employment [isoc_sks_itspt]	Number and share of ICT specialists in employment (Digital Decade target)	Part A – Non-technology and Technology decision-makers, Build, invest and innovate Part B – Non-technology and Technology decision-makers, Digital Products and Markets	Population: EU27 individuals in employment aged 15 or older; data available annually since 2016. **Caveat:** Headcount rather than skills.
Indicator 6: Eurostat Provision of ICT skills training to workers by organisation size [isoc_ske_itts] and NACE activity [isoc_ske_ittn2]	Percentage of enterprises providing training to (i) ICT specialist workers, (ii) other workers, to improve their ICT skills, by organisation size and NACE activity	Part A – Non-technology and Technology decision-makers, Build, invest and innovate Part B – Non-technology and Technology decision-makers, Digital Products and Markets	Population: EU27 enterprises with 10 or more employees and self-employed persons (micro-enterprises are covered on an optional basis); data available every two years since 2020, annually 2014-2019. **Caveat:** Generic ICT skills training, not specific to sovereignty.

Source: JRC analysis from indicators

Notes: All six indicators are deemed **medium relevance** and all have data status as regularly available: they are derived from comparative data but are proxies, not direct competence measures.

The six additional sources examined but not viable as indicators comprise:

(i) three **one-off studies**: Personal data and privacy literacy metric (Lund et al., 2026); ENISA cybersecurity education maturity assessment (Skouloudi et al., 2024); and self-hosted software solution competence (Hrgarek & Zlatolas, 2025); and

(ii) three measures **with data but non-viable**. Two of these are from the Eurostat ICT usage in enterprises (usage of AI for R&D or innovation, and for software development). In these cases, the data required to report them is held at Member State level only (Eurostat, 2025).

The third is the ISC2 cybersecurity workforce study (ISC2, 2025), which included a workforce skills gap up until 2025. However, the sample is non-representative (based on ISC2 membership) and numbers participating at the country level are too low to provide robust information.

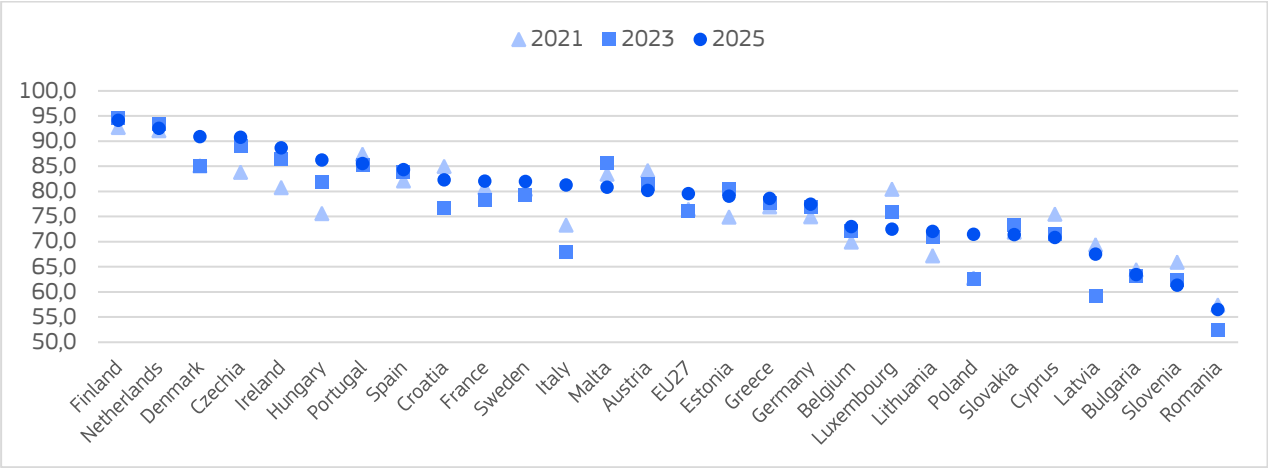
In addition to these sources, there are various **competence frameworks** which contain relevant concepts and content but no data. These include DigComp 3.0 which includes aspects of cybersecurity, agency, rights, and misinformation (Cosgrove & Cachia, 2025); the ENISA cybersecurity skills framework, covering 12 role profiles mapping, translating NIS2 (Network and Information Security Directive 2) duties into workforce roles (ENISA, 2022); the UK Government Digital and Data Profession Capability Framework which describes competences for several IT specialist roles (UK Government, 2026); and the OECD Framework for digital talent and skills in the public sector, covering aspects such as leadership, professional and socio-emotional skills (OECD, 2021).

7.2.4. Indicators visualisation

This section provides illustrative visualisations of three of the six indicators. As noted in **Table 21**, Indicators 2, 3 and 4 are described in detail in **Chapter 2** in this report, so are not considered further here.

Figure 57 shows **Indicator 1** (a proxy for cybersecurity and data protection skills) for the adult population for 2021, 2023 and 2025. It is the only potentially viable indicator identified for the general population. The indicator is robust insofar as it is stable over time and drawn from nationally representative samples every two years. It provides some useful information about variation across countries and over time. However, it is a very partial view of what constitutes general population digital sovereignty competences in the *Rule of law and democracy* and *People → Infrastructures, software and data* aspects (see the bolded text in the 'General population' columns of Tables 1 and 2). Therefore, the use of this indicator - in the absence of any others - risks to convey that general population digital sovereignty competences amount solely to generic cybersecurity behaviours. Also, it does not capture skills to respond to evolving cybersecurity and privacy threats, which has been noted as a key policy concern (Boutemeur et al., 2025; Europol, 2025).

Figure 58. Illustrative visualisation of Indicator 1 – General adult population cybersecurity skills (DSI 2.0 Safety area, % with at least basic skills), 2021, 2023 and 2025

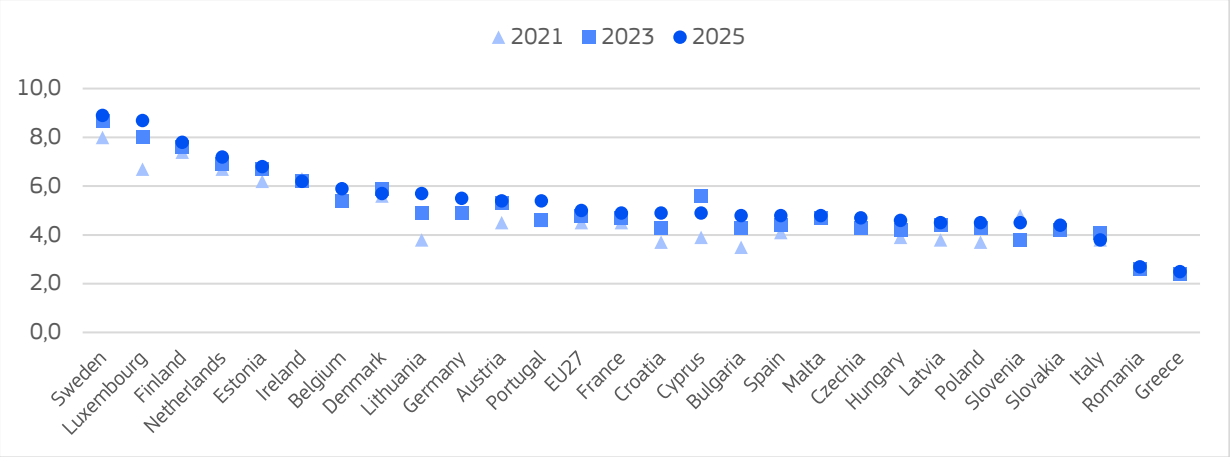


Source: Eurostat https://ec.europa.eu/eurostat/databrowser/view/ISOC_SK_DSKL_I21/default/table [i_dsk2_saf_bab]

Notes: Countries are in descending order for 2025 values. Indicator is based on actions in last 3 months (yes/no): check website security, read privacy statements, block geolocation, limit social media profile access, refuse use of data for advertising, prevent/limit cookies. Data are collected every two years as part of the annual ICT usage in households and individuals survey. Forms part of the basic digital skills indicator that is used in the Digital Decade Policy Programme targets.

Figure 58 shows an illustrative visualisation of **Indicator 5** – share of ICT specialists in employment (the statistic is also available as numbers of ICT specialists in employment). This indicator sits in the *Build, invest and innovate* aspect of non-technical and technical decision-maker roles in Table 2, and the *People→Digital products and markets* aspect of non-technical and technical decision-maker roles in **Table 24**.

Figure 59. Illustrative visualisation of Indicator 5 – Share of ICT specialist workers in employed labour force



Source: Eurostat https://ec.europa.eu/eurostat/databrowser/view/ISOC_SKS_ITSPT/default/table?lang=en

Notes: Countries are in descending order for 2025 values. This indicator is used in the Digital Decade Policy Programme targets.

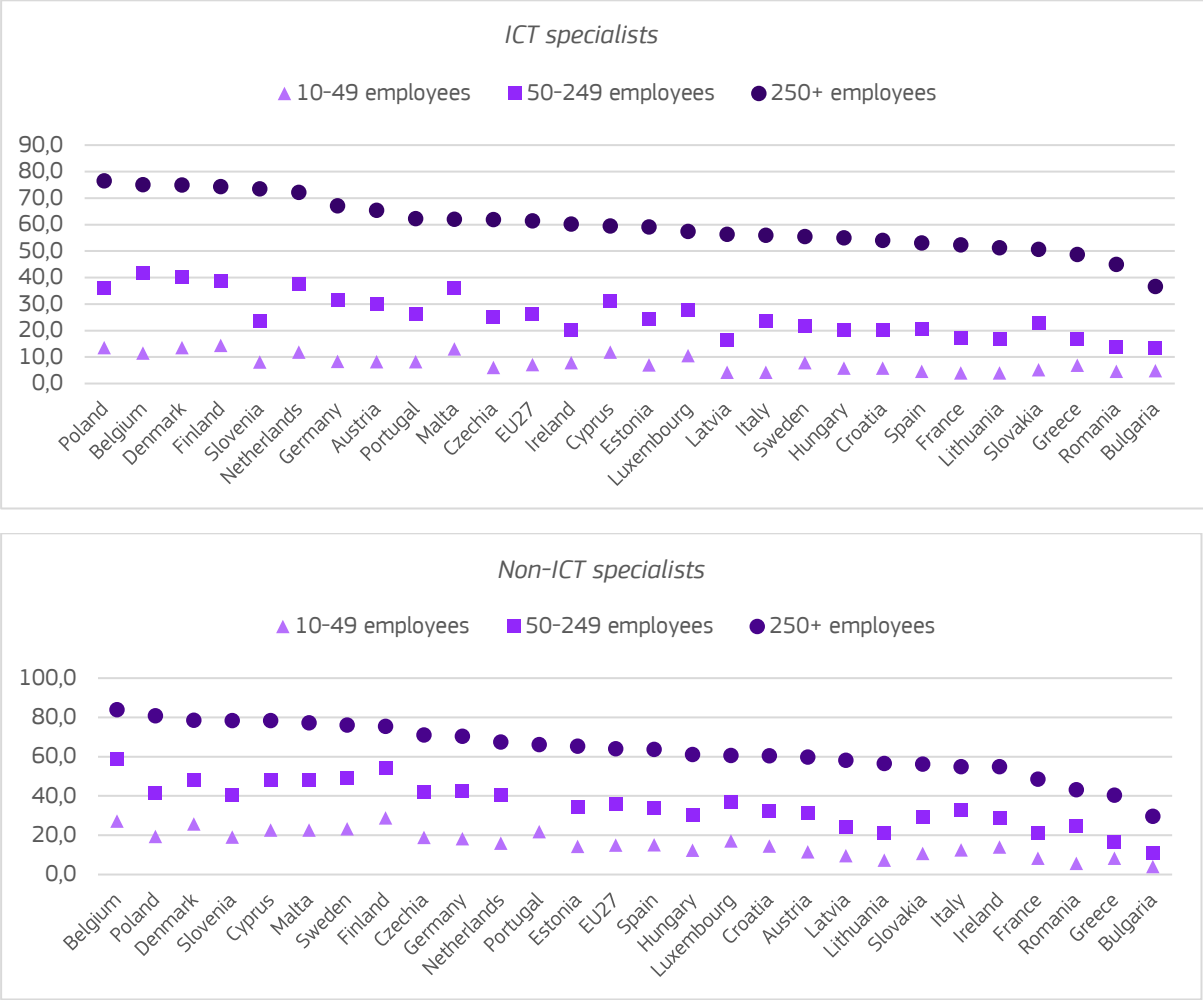
As with Indicator 1, Indicator 5 is robust in its complete coverage of EU27 and available annually. However, it is a generic and indirect measure, as it does not provide information on the extent to which the number of ICT specialists is sufficient to meet needs, and cannot inform us directly about specialist build and deployment skills needs, described in Tables 1 and 2. It should also be noted that ICT specialists in employment is used for one of the Digital Decade targets.

Recently-published trend analyses by Eurofound of ICT specialists, which use the Labour Force Survey and European Working Conditions Survey (Eurofound, 2026), could supplement this indicator providing more context and detail. For example, Figure 2 in Eurofound (2026) shows the percentage change in employment of ICT specialists 2021-2024 by specific occupation; Figure 4 shows the distribution of ICT specialist employment by sector, 2011-2024; and Figure 21 shows skills mismatch and training provision for ICT specialists, 2024. However, the Eurofound report does not specifically relate to digital sovereignty per se.

An illustrative visualisation of Indicator 6 – provision of ICT skills training to ICT specialist employees by organisation size – is shown in **Figure 59.** As with Indicator 5, this indicator is robust, with representative data for EU27 every two years. Also, the statistic is available not only by organisation size (which shows very large differences in rates of ICT skills training across small, medium and large enterprises) but also sector, which provides policy-relevant information. The

availability of the indicator separately for ICT specialist and non-ICT specialist workers is also useful as it is indicative of specialist and generalist ICT skills training. However, the indicator does not inform us of the specific areas in which training was offered, nor the uptake or impact.

Figure 60. Illustrative visualisation of Indicator 6 – % of enterprises providing ICT skills training employees (ICT specialists and non-ICT specialists), by organisation size, 2024



Source: https://ec.europa.eu/eurostat/databrowser/view/isoc_ske_itts/default/table?lang=en *Statistic is also available by sector (NACE)* https://ec.europa.eu/eurostat/databrowser/view/isoc_ske_itts/default/table?lang=en

Notes: Panels are sorted in ascending order by largest organisation size group. Missing data points are due to unreliability and are missing at source.

7.3. Conclusions

We presented a preliminary examination of individual-level digital sovereignty competence – a very recent and emerging topic – through the lens of an existing European model of digital sovereignty developed by the JRC (Di Marco et al., 2025), also drawing on a rapid scoping literature review.

Given the emerging nature of this topic and the complexity and multifaceted nature of digital sovereignty itself, we first conceptualised digital sovereignty competence from two perspectives – **foundational** and **transformative** competences. Within each perspective, we considered of competences specific to three key roles in the digital ecosystem (general population, non-

technology decision-makers, and technology decision-makers), highlighting that competences vary by role, yet should be linked with and aligned to one another. That is, digital sovereignty competence is not seen as a singular competence possessed in different degrees by different people but is, rather, role-differentiated and complementary in nature, where different actors exercise different forms of agency toward digital sovereignty.

By mapping this initial conceptualisation to a set of six potentially viable indicators of individuals' digital sovereignty competence, we show that **existing indicators are sparse and indirect proxies, with much of the literature and identified indicators remaining at a theoretical rather than a practical (applied measurement) level**. For example, no competence indicators were found for digital governance, digital dependencies, procurement or intellectual property. The fact that only six of 12 potential indicators initially identified were viable underlines the information and measurement gap encountered.

Future research in this area could consider this preliminary work as a starting point for further identifying, defining and measuring digital sovereignty competences, since individuals' capabilities form a vital aspect of achieving digital sovereignty objectives.

Conclusions and takeaways for policymakers

The pursuit of digital sovereignty within the European Union requires a comprehensive understanding of the EU's capabilities, dependencies, and strategic positioning across the entire digital ecosystem. Crucially, digital sovereignty does not mean technological isolation or protectionism; rather, it is the EU's capacity to act independently in the digital realm while remaining openly connected to global networks (Di Marco et al., 2025). This report applies a comprehensive framework that provides quantitative evidence and evaluates European digital sovereignty across four interconnected layers: Digital Governance; Digital Infrastructures, Software, and Data; Digital Products and Markets; and People. This concluding chapter synthesises the main findings across these four dimensions, and translates the empirical evidence into practical takeaways for decision-makers.

Main Findings

Digital Governance

The analysis of science, technology and innovation (STI) policies reveals a marked increase in policy attention to strategic digital technologies since the mid-2010s. AI & Autonomous Systems accounts for the largest share of the observed expansion, followed by Data & Compute Infrastructure, while cybersecurity, quantum technologies, semiconductors and connectivity are also increasingly represented in reported policy initiatives. This points to a **growing emphasis on technology-specific policy responses addressing strategic capabilities and dependencies**, beyond more general digitalisation objectives.

The analysis, based on the OECD Protection, Promotion and Projection (3Ps) framework, shows that **digital sovereignty is addressed through a combination of policy orientations**. Protection is the most prevalent, appearing in more than 90% of eligible initiatives across all technology groups and reflecting concerns related to technological autonomy, security, resilience and risk governance. However, the relative emphasis on other orientations varies across technologies. Quantum Technologies and Data & Compute Infrastructure show stronger orientations towards Research Promotion, while Semiconductors & Photonics stands out for Business Promotion, highlighting different approaches to strengthening technological capabilities.

At the country level, the findings reveal **considerable heterogeneity in national policy portfolios**, including among EU Member States. Some place greater relative emphasis on research capacity, others on business development or the management of strategic dependencies. These

differences highlight the diversity of national approaches to digital sovereignty and point to potential complementarities, as well as areas requiring further investigation, across European policy portfolios. For the EU, the findings underline the **importance of examining how national policy priorities collectively contribute to strengthening critical technological capabilities**, managing strategic dependencies and supporting international cooperation.

Digital Infrastructures, Software, and Data

The analysis of the infrastructure, software, and data layer reveals several key findings. First, the investigation of European alternatives to incumbent digital solutions highlights the importance of substitutability in achieving digital sovereignty. The study finds that **only one in five solutions reports at least one explicit technical mechanism capable of lowering switching costs**—such as interoperable interfaces, deployment autonomy, or data portability. Deployment autonomy (e.g., self-hosting or on-premises use) is the most reported mechanism, while Interface substitutability is less common and concrete Portability mechanisms are rarely reported. The analysis also shows that solutions positioned against the largest incumbent ecosystems, such as Google, Microsoft, and Amazon, are more likely to report substitutability mechanisms. These findings highlight the importance of assessing technical substitutability within the European digital offer, moving beyond the availability of alternative solutions to examine whether they provide concrete mechanisms that enable users to switch providers and reduce lock-in.

Second, the geographical analysis of open source software (OSS) ecosystems provides valuable insights into digital sovereignty. The study of OSS development on GitHub demonstrates that the **EU holds a vibrant but unevenly distributed OSS developer ecosystem**. Some Member States exhibit high developer capacity and activity intensity, often supported by mature domestic institutions, culture of openness and public-sector initiatives, while others act as highly interconnected nodes in international networks. These differences highlight the importance of adopting a differentiated approach to public support, tailored to countries' specific ecosystem profiles. **Strategically targeted public investment could help to leverage existing strengths**, address gaps and strengthen areas where private investment remains insufficient, thereby contributing to a more resilient and competitive European OSS ecosystem. The need for strategic intervention is reinforced by the **structural asymmetries observed in the global collaboration structure, which remain heavily concentrated and dominated by the United States.** While the EU acts as a major source of open source contributions, a substantial share of global and European OSS contributions flows toward projects based in the US, highlighting a structural asymmetry in the global open source ecosystem. At the same time, considering the EU as a single entity shows that it is the second major pole of international open source collaboration in the world.

Finally, the analysis of the cloud computing and data technologies domain highlights the importance of understanding the EU's position in the global digital ecosystem. The study finds that **the EU remains scientifically strong in cloud computing and data technologies**, but its lead is under pressure from other global players, such as China and the US. EU-based authors contributed 22% of scientific publications in cloud computing and data technologies between 2009 and 2025, matching China's share. However, the analysis also shows that the EU's innovation base is **not translating into comparable proprietary technological assets—**with only 2% of the global patent filings in cloud and data involving at least an EU applicant, compared to China's 84%—, and that the EU's venture market is much smaller than the US market. **European firms**

become highly reliant on foreign investors, predominantly from the US, which provides 43% of the funding received by EU scale-ups. This financial dependency poses a long-term risk to the EU's ability to retain ownership and strategic control over its successful digital infrastructure enterprises.

Markets

Digital sovereignty understood through the lens of markets and production networks is characterised by a complex dynamic of strengths and vulnerabilities. Two key chapters have contributed to this understanding: the first examines the control exerted by multinationals in digital production networks, while the second investigates asymmetric trade dependencies in products underpinning digital sovereignty.

The analysis reveals that digital production networks are highly influenced by **multinational corporations that control digital production both within and beyond the territories of their parent countries**. For example, in the IT and information services sector, US parent corporations control over 80% of the non-EU corporate production hosted within the European Union. In telecommunications, UK multinationals account for more than 56% of the EU's inward production footprint. The analysis demonstrates that **power and interdependency are closely intertwined** where the most dominant countries are highly connected to global networks while still maintaining strong influence—a strategy of being "open but not powerless". In this context, the EU acts as a major global player, despite significant variation across Member States. Some EU countries, such as Germany and France, exhibit strong power positions, with varying degrees of interdependency, but most individual Member States have low international power and limited global integration. The findings also show that **having a large amount of production at home does not automatically guarantee international influence, just as expanding corporate activity abroad does not necessarily create domestic vulnerability**. Productive scale, outward influence, and network resilience are distinct capabilities that require separate policy attention.

The subsequent research strand unpacks these dependencies by assessing whether a trading partner is important for the EU and, conversely, whether the EU is equally important for that partner; in other words, it distinguishes economic interdependencies that support an open and competitive European economy from dependencies that may give rise to vulnerabilities. **The analysis identifies 31 products, accounting for EUR 18.6 billion in EU imports, for which the EU is potentially vulnerable to at least one third-country supplier.** These vulnerabilities are concentrated in a narrow set of high-value products, predominantly in Asia, and especially in Taiwan, China, and Malaysia. **Conversely, the EU exhibits asymmetric strengths across a much broader and more diversified product base** (125 products exported to 188 partners, accounting for EUR 72.8 billion), largely comprising core and broad products accounting for much of the wider product base across almost all countries, and thus reflecting the more diversified EU industrial capabilities. The chapter also examines the evolution of asymmetric dependencies over time, revealing that potential EU vulnerabilities have increased in value and become more concentrated in a few Asian suppliers. In contrast, potential EU strengths have evolved more gradually, with a broader and more stable base of products and partners.

People

The realization of digital sovereignty ultimately relies on the capabilities of individuals—citizens, entrepreneurs, and technical leaders—to navigate, shape, and govern digital environments. Digital sovereignty competences extend beyond basic digital literacy; they encompass the capacity to understand geopolitical dependencies, exercise data rights, make independent technological choices, and implement secure, interoperable infrastructures. The analysis shows that **these competences are role-specific, varying among the general population, non-technology decision-makers, and technology decision-makers**.

A primary finding regarding the People layer is a data gap. Digital sovereignty skills are an emerging concept, largely absent from standard competency frameworks and existing demographic metrics. **Current viable indicators are limited to indirect proxies, with no robust, regularly available data to measure critical individual competencies** related to digital governance, the identification of digital dependencies, sovereign procurement practices, or intellectual property management, with much of the literature and identified indicators remaining at a theoretical rather than a practical (applied measurement) level.

Key Takeaways for Policymakers

The pursuit of digital sovereignty within the European Union requires a comprehensive understanding of the EU's capabilities, dependencies, and strategic positioning across the entire digital ecosystem. To assist European decision-makers in translating multi-layered empirical insights into actionable knowledge, the report identifies the following practical takeaways:

- **Digital sovereignty requires multidimensional metrics:** Achieving sovereignty in the digital domain requires a holistic approach spanning four interconnected layers: (i) Digital Governance, (ii) Infrastructures, Software and data, (iii) Markets, and (iv) People. Observing metrics over time and across these layers provides critical analytical value by distinguishing policy intentions from strategic outcomes. For example, governance indicators reveal which strategic technologies policymakers prioritise, while production, trade, and substitutability metrics assess whether these priorities correspond to actual observed capabilities or vulnerabilities. Furthermore, evidence suggests that each technological domain possesses distinct risk profiles; frontier technologies like quantum computing may require sustained research promotion, whereas mature sectors like semiconductors demand supply chain security.
- **Sovereignty extends beyond protectionism:** EU Digital sovereignty should not be treated merely as a question of technological protectionism; it also necessitates strong domestic capacity-building and strategic international projection. The importance of this "*open but not powerless*" approach is evidenced in global corporate production, where leading global actors combine domestic production autonomy with deep international interconnectedness. Digital governance policies reinforce this paradigm through the Protection, Promotion, and Projection (3Ps) framework, demonstrating that while protective measures to reduce dependency vulnerabilities are highly prevalent, they must be actively paired with the capacity to innovate and collaborate internationally.

- **Availability does not guarantee substitutability:** The availability of European or open source software alternatives is insufficient if customers remain technically locked into incumbent systems. The analysis of the European digital offer in the Eurostack Directory revealed that nearly 80% of solutions lacked a description of technical exit mechanisms. Public procurement can play a key role in this context by translating interoperability and switching goals into specific criteria mandating concrete switching mechanisms in line with the Data Act. Tenders could require verifiable features such as drop-in interface compatibility, customer-controlled deployment options (like self-hosting), and standardized data export pathways to guarantee operational autonomy.
- **Leveraging the collective weight of the EU:** The integration and scale of the EU single market are essential for achieving global leverage. In corporate production networks, individual Member States often have limited standalone power and global integration, but their collective weight elevates the bloc to a highly interconnected "Global Influencer". The importance of a unified scale is equally evident in open source ecosystems; while the global collaboration structure remains heavily concentrated and dominated by the United States, considering the EU as a single entity reveals it as the second major pole of international open source collaboration, highlighting how unified scale promotes a cohesive and resilient European presence globally.
- **Bridging the gap from research excellence to commercial scale-up.** While the EU maintains a strong scientific research base, it struggles to bridge the gap from research excellence to commercial scale-up, failing to translate scientific leadership into proprietary technological assets and scaled market champions. For example, in cloud and data technologies, the EU matches China in scientific publications (22% of the global share) but accounts for only 2% of patent filings. Furthermore, European scale-ups face a critical domestic funding gap, driving a heavy reliance on foreign capital—with US investors providing 43% of the funding for EU scale-ups in this sector. Policy attention could therefore pivot toward commercialisation, patent valorisation, and late-stage capital availability to prevent the loss of ownership, intellectual property, and strategic control over high-growth European tech firms.
- **Identify and manage asymmetric dependencies:** The EU is potentially vulnerable to at least one third-country supplier across 31 products, accounting for EUR 18.6 billion in EU imports, which may require targeted supply-chain resilience and diversification strategies. However, the EU also holds significant asymmetric strengths across a much broader and more diversified base of 125 core and broad products exported to 188 partners, accounting for EUR 72.8 billion. European trade and industrial strategy would benefit from two main considerations. Frist, distinguishing normal mutual interdependence from one-sided strategic exposure where supply-chain resilience and diversification measures can be applied. Second, the EU's core competitive advantages (i.e., strategic indispensability) should be protected and scaled up, using these outward strengths as strategic leverage in international partnerships.
- **A foundation for continuous monitoring:** While this report provides a multi-layered foundation, significant measurement gaps remain across the digital sovereignty framework. For example, while current trade data effectively tracks physical products, trade data on services remains very limited failing to capture dependencies in non-tangible assets related to software, cloud infrastructure, and algorithmic design among others. Similarly, measures around people's competences for digital sovereignty remain undefined in official monitoring systems, despite being a fundamental aspect of digital sovereignty. The development of dedicated indicators across all layers of the digital sovereignty framework remains therefore a key need for future policy action.

Future Research

While this report establishes a comprehensive baseline for understanding EU digital sovereignty**, it only represents a first step in quantifying a highly complex and dynamic landscape.** To ensure that strategic decisions remain effective, there is a need to build upon this foundation with continuous, additional empirical analysis that can accurately track the rapid evolution of digital markets, infrastructures, and human capabilities over time.

Future research could expand beyond physical goods and structural proxies to **capture intangible and service-based dependencies and opportunities**. Tracking the trade of physical goods effectively maps product vulnerabilities but fails to capture dependencies in non-tangible assets, such as software, cloud infrastructures, and algorithmic design. Similarly, data on multinational production networks measure corporate ownership and gross output, but they do not capture direct control over data, critical technologies, and public-sector capabilities. Future **frameworks must integrate trade in services with metrics on technological capabilities and policy design** to provide a complete picture of strategic dependencies.

In addition, future studies could evolve **from assessing documented information to verifying actual technical and market characteristics of digital products**. Future evaluations of the European digital offer could **verify actual technical substitutability directly from technical documentation** and develop further measures around costs and viability of portability. Concerning the governance aspects, future studies could connect these governance inputs directly to observed market outcomes and dependency measures.

Community and human capital metrics would also require additional research. Analyses of innovation, start-ups, and open source software face platform-specific biases and publication lags, necessitating future data triangulation with alternative repositories and broader socioeconomic indicators. Finally, because digital sovereignty fundamentally depends on human agency, future research could develop dedicated, direct **indicators to measure sovereign decision-making competencies.**

References

Aaronson, S. A. (2019), 'What are we talking about when we talk about digital protectionism?', *World Trade Review*, Vol. 18, Issue 4, pp. 541–577.

Atlassian (2026), 'Bitbucket', Bitbucket website, accessed 16 October 2026, https://bitbucket.org/.

Arjona, R., Connell, W. and Herghelegiu, C. (2023), 'An enhanced methodology to monitor the EU's strategic dependencies and vulnerabilities', Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs (European Commission), WP2023/14, Chief Economist Team.

Bellini, P., Campanella, E. and Piccioni, A. (2025), 'The impact of artificial intelligence and data on political power and geopolitical equilibria', *Socio-economic Impact of Artificial Intelligence: A European Management Perspective*, Springer Nature Switzerland, Cham, pp. 15–22.

Berkel, F., Bohm, D., Wulff, H., Reith, G. and Wendeborn, T. (2025), 'Digital sovereignty of physical education teachers in Germany: a situation analysis (2017–2021) on the gap between educational policies and practical implementation in further physical education teacher trainings', *Frontiers in Education*, Frontiers Media SA, p. 1544886.

Berger, M., Calligaris, S., Dechezleprêtre, A., Dernis, H. et al. (2026), 'The OECD Start-ups Database'.

Blind, K., Böhm, M., Grzegorzewska, P., Katz, A. et al. (2021), 'The impact of Open Source Software and Hardware on technological independence, competitiveness and innovation in the EU economy', https://doi.org/10.430161.

Boehm, M. (2022), 'Economics of Open Source', *Open Source Law, Policy and Practice*, https://doi.org/10.1093/oso/9780198862345.003.0015.

Bonnet, P, Di Girolamo, E, Pagano, A, Velazquez, B and Zaurino, E (2026), 'EU foreign dependencies: Assessment of trade and geopolitical vulnerabilities', 2, DG Trade, March.

Bonnet, P., Ciani, A., Molnar, J. and Nardo, M. (2025), *EU's strengths and weaknesses in the global semiconductor sector*, Publications Office of the European Union, Luxembourg, https://archive.ph/o/wa0Yl/doi, 10, 6302476.

Boutemeur, J., Lella, I., Bakatsis, I., Chatzichristos, G., Foley, K. et al. (2025), *ENISA threat landscape 2025*, ENISA, Athens, https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Threat%20Landscape%202025_v1.2.pdf.

Bria, F., Timmers, P. and Gernone, F. (2025), *EuroStack–A European alternative for digital sovereignty*, Bertelsmann Stiftung, Gütersloh.

Bridson, B. (2026), 'What is digital sovereignty and why does it matter?', accessed 16 October 2026, https://www.ie.edu/uncover-ie/digital-sovereignty-master-in-public-policy/.

Bryson, J., Danneels, L., Di Marco, D., Dobbe, R., Grimmelikhuijsen, S. et al. (2026), 'Advancing EU Digital Sovereignty in Public Administrations: Navigating Opportunities, Trade-Offs and Open Questions'.

Burwell, F. and Propp, K. (2026), 'Digital Sovereignty: Europe's Declaration of Independence'. The Atlantic Council of the United States.

Cadestin, C., De Backer, K., Desnoyers-James, I., Miroudot, S., Rigo, D. et al. (2018), 'Multinational enterprises and global value chains: the OECD analytical AMNE database', *OECD Trade Policy Papers*.

Calza, E., DALLA, B. A., Kostić, U., Mitton, I., Moraschini, M. et al. (2023), 'Analytical insights into the global digital ecosystem (DGTES)'.

Calza, E., DALLA, B. A., Kostić, U., Mitton, I., VAZQUEZ-PRADA, B. M. et al. (2022), 'A policy oriented analytical approach to map the digital ecosystem (DGTES)'.

Caraiani, P., Dima, A. M., Păun, C., Stamule, T. and Vargas, M. V. (2024), 'Production networks and resilience: How dense production networks shield economies in financial crisis', *Plos one*, Vol. 19, Issue 4, p. e0302012.

Chiang, J. T. (1990), 'Producing 'national champions' in technology through deliberate strategic decisions', *Technology in Society*, Vol. 12, Issue 3, pp. 235–254.

Codeberg News (2025), 'Letter from Codeberg: Onwards and upwards!', accessed 16 October 2026, https://blog.codeberg.org/letter-from-codeberg-onwards-and-upwards.html.

Coe, N. M. and Yeung, H. W. C. (2019), 'Global production networks: mapping recent conceptual developments', *Journal of economic geography*, Vol. 19, Issue 4, pp. 775–801.

Cosgrove, J. and Cachia, R. (2025), *DigComp 3.0: European digital competence framework*, Publications Office of the European Union.

De la Cueva, J. and Méndez, E. (2022), *Open Science and Intellectual Property Rights. How can they better interact? State of the art and reflections*, Publications Office of the European Union, Luxembourg.

Dechezleprêtre, A., Ménière, Y. and Mohnen, M. (2017), 'International patent families: from application strategies to statistical indicators', *Scientometrics*, Vol. 111, Issue 2, pp. 793–828.

Deutsche Telekom AG (2024), 'Annual report 2023: Business activities', Deutsche Telekom AG.

Di Marco, D., Thabit Gonzalez, S., Kotsev, A., Friis-Christensen, A., Minghini, M. et al. (2025), 'Open but not powerless: Towards a common understanding of eu digital sovereignty', European Commission.

EC-OECD (2025), 'Overarching analysis of the 2025 EC–OECD STIP Survey data', STIP Data Lab, accessed 16 October 2026, https://stiplab.github.io/R5r/main.html.

EC-OECD (2026), 'STIP Compass: International Database on Science, Technology and Innovation Policy (STIP)', European Commission and OECD, accessed 16 October 2026.

Edler, J. and Fagerberg, J. (2017), 'Innovation policy: what, why, and how', *Oxford Review of Economic Policy*, Vol. 33, Issue 1, pp. 2–23.

Edler, J., Blind, K., Kroll, H. and Schubert, T. (2023), 'Technology sovereignty as an emerging frame for innovation policy. Defining rationales, ends and means', *Research policy*, Vol. 52, Issue 6, p. 104765.

Elmallakh, N., Walczak, N., Pagano, A., Di Girolamo, F., Isaraj, L. and Kotsev, A. (2026), 'Products Underpinning Digital Sovereignty (HS6 Classification)', European Commission, Joint Research Centre [Dataset], https://doi.org/10.2905/JRC.4VYC1KR

ENISA (European Union Agency for Cybersecurity) (2022), 'European Cybersecurity Skills Framework (ECSF)', https://www.enisa.europa.eu/topics/skills-and-competences/skills-development/european-cybersecurity-skills-framework-ecsf.

Eurofound (2026), *IT sector in focus: Evolution of the EU's digital workforce*, Publications Office of the European Union, Luxembourg, https://www.eurofound.europa.eu/en/publications/all/it-sector-in-focus-evolution-digital-workforce.

European Commission (2026a), 'Commission reaches preliminary position that Amazon's and Microsoft's market-leading cloud services should be designated under the DMA', 25 June, accessed 16 October 2026.

European Commission (2026b), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on European Tech Sovereignty, accompanied by an EU Open Source Strategy, COM(2026) 503 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52026DC0503.

European Commission (2026c), 'Results of the study on interoperability of data processing services', 23 February, https://digital-strategy.ec.europa.eu/en/library/results-study-interoperability-data-processing-services,https://publications.jrc.ec.europa.eu/repository/handle/JRC144908.

European Commission, Joint Research Centre, accessed 15 October 2026, https://data.jrc.ec.europa.eu/collection/id-00468.

European Parliament,Council of the European Union (2016), Directive (EU) 2016/943 of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, Official Journal of the European Union, https://eur-lex.europa.eu/eli/dir/2016/943/oj.

European Parliament,Council (2023), Regulation (EU) 2023/2854 on harmonised rules on fair access to and use of data (Data Act), Official Journal of the European Union.

European Political Strategy Centre (2025), *The future of European competitiveness (Part A)*, European Commission, Brussels, https://doi.org/10.2872/9356120.

Europol (2025), 'IOCTA: internet organised crime threat assessment 2025', Europol, https://data.europa.eu/doi/10.2813/4926508.

EuroStack Directory Project (2026), 'EuroStack – European Open Solutions for Digital Sovereignty', accessed 16 October 2026, https://euro-stack.com/.

Eurostat (2025), 'ICT usage in enterprises: Reference metadata', Eurostat, accessed 16 October 2026, https://ec.europa.eu/eurostat/cache/metadata/EN/isoc_e_esms.htm.

Eurostat (2024–2026), *ICT specialists in employment (isoc_sks_itspt); Digital skills indicator (isoc_sk_dskl_i21); Digitalisation in Europe – 2026 edition*, Publications Office of the European Union, Luxembourg, https://ec.europa.eu/eurostat/web/digital-economy-and-society.

Farrell, H. and Newman, A. L. (2019), 'Weaponized interdependence: How global economic networks shape state coercion', *International security*, Vol. 44, Issue 1, pp. 42–79.

Farrell, J. and Klemperer, P. (2007), 'Coordination and lock-in: Competition with switching costs and network effects', *Handbook of industrial organization*, pp. 1967–2072.

European Commission, Fratini, S., Pohle, J., Di Marco, D., Thabit Gonzalez, S. et al. (2026), 'Digital Sovereignty as a Geopolitical Strategy-Navigating Dependencies, Power, and Democratic Resilience in a Changing Global Order', JRC146878.

Gineikytė-Kanclerė, V. and Eggert, M. (2025), 'European Software and Cyber Dependencies', PE 778.576, Policy Department for Transformation, Innovation and Health, December.

Gitee (2026), 'About Gitee', Gitee website, accessed 16 October 2026, https://gitee.com/about_us.

GitHub (2025), 'Octoverse 2025: A new developer joins GitHub every second as AI leads TypeScript to #1', The GitHub Blog, accessed 16 October 2026, https://github.blog/news-insights/octoverse/octoverse-a-new-developer-joins-github-every-second-as-ai-leads-typescript-to-1/.

GitHub (2026), 'GitHub Innovation Graph', GitHub Innovation Graph, accessed 16 October 2026.

GitLab (2026), 'About GitLab: GitLab by the numbers', GitLab website, accessed 16 October 2026, https://about.gitlab.com/company/.

Görnemann, E. (2024), *Digital Sovereignty*, Weizenbaum Institute, https://doi.org/10.34669/wi.fund/2.de.web.

Government of Canada (2025), 'Digital sovereignty: A framework to improve digital readiness of the Government of Canada', accessed 16 October 2026, https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/digital-sovereignty/digital-sovereignty-framework-improve-digital-readiness.html.

Grasso, M., Trapani, F., Sellerio, A. and Checchi, E., 'Taxonomical and Temporal Alignments of Trade and Production Data'.

Hartmann, E. A. and Shajek, A. (2023), 'New digital work and digital sovereignty at the workplace–an introduction', *New digital work: digital sovereignty at the workplace*, Springer International Publishing, Cham, pp. 1–15.

Hoffmann, M., Nagle, F. and Zhou, Y. (2024), 'The value of open source software', 24-038.

Howlett, M. (2000), 'Managing the "hollow state": Procedural policy instruments and modern governance', *Canadian public administration*, Vol. 43, Issue 4, pp. 412–431.

Hrgarek, L. and Nemec Zlatolas, L. (2025), 'A Model of Factors Influencing Continuance Intention and Actual Usage of Self-Hosted Software Solutions', *Sustainability*, Vol. 17, Issue 22, p. 10009, https://doi.org/10.3390/su172210009.

Isaraj, L. (2026a), 'Mapping Science, Technology and Innovation Policies by Strategic Digital Technology and Policy Orientation', European Commission, Joint Research Centre [Dataset], https://doi.org/10.2905/JRC.ECW86J8

Isaraj, L. (2026b), 'EuroStack Digital Solutions: Substitutability Indicators (2026)', European Commission, Joint Research Centre [Dataset], https://doi.org/10.2905/JRC.4W274Z8

Isaraj, L., Thabit Gonzalez, S., Cerulli, G. (2026), 'Corporate Control in Digital Production Networks'. European Commission, Joint Research Centre [Dataset] doi: 10.2905/JRC.VCP5RJ8 PID: http://data.europa.eu/89h/4df8dcc5-da0a-41d2-bcfe-0ee8d02b6850

ISC2 (2025), 'Cybersecurity professionals navigate evolving workplaces while seizing new opportunities', ISC2, 20 December, accessed 16 October 2026, https://www.isc2.org/Insights/2025/12/2025-ISC2-Cybersecurity-Workforce-Study.

ISTAT (2026), 'L'apertura internazionale dell'economia', Istituto Nazionale di Statistica.

Jansen, B., Kadenko, N., Broeders, D., Van Eeten, M., Borgolte, K. et al. (2023), 'Pushing boundaries: An empirical view on the digital sovereignty of six governments in the midst of geopolitical tensions', *Government Information Quarterly*, Vol. 40, Issue 4, p. 101862.

Jeon, D. S., Menicucci, D. and Nasr, N. (2023), 'Compatibility choices, switching costs, and data portability', *American Economic Journal: Microeconomics*, Vol. 15, Issue 1, pp. 30–73, https://doi.org/10.1257/mic.20200309.

Kim, J. Y. (2026), 'Data portability and interoperability between digital platforms', *Journal of Economics & Management Strategy*, Vol. 35, Issue 2, pp. 219–232, https://doi.org/10.1111/jems.12643.

Krämer, J. and Stüdlein, N. (2019), 'Data portability, data disclosure and data-induced switching costs: Some unintended consequences of the General Data Protection Regulation', *Economics Letters*, Vol. 181, pp. 99–103, https://doi.org/10.1016/j.econlet.2019.05.015.

Linåker, J. and Muto, S. (2026), 'Advancing digital government through open source indicators', *Journal of Systems and Software*, p. 113031.

Linux Foundation (2025), 'State of the Global Open Source 2025'.

Liu, Y. and Zhao, Y. (2025), 'Intellectual property information literacy education: Evidence from 30 Chinese National IP Demonstration Universities', *Humanities and Social Sciences Communications*, Vol. 12, p. 366, https://doi.org/10.1057/s41599-025-04679-1.

Lund, B. D., Brown, N., Roeschley, A. and Hossain, G. (2026), 'PDPL metric: validating a scale to measure personal data privacy literacy among university students', *Behaviour & Information Technology*, pp. 1–11, https://doi.org/10.1080/0144929X.2026.2614050.

March, C. and Schieferdecker, I. (2023), 'Technological sovereignty as ability, not autarky', *International Studies Review*, Vol. 25, Issue 2, p. viad012.

Mayer, M. and Lu, Y. C. (2025), 'Global structures of digital dependence and the rise of technopoles', *New Political Economy*, Vol. 30, Issue 5, pp. 755–774, https://doi.org/10.1080/13563467.2025.2497766.

Nindl, E., Confraria, H., Rentocchini, R., Napolitano, L., Georgakaki, A. et al. (2023), *The 2023 eu industrial r&d investment scoreboard*, Publications Office of the European Union.

Green, R., Liyanage, S., Pitsis, T., Scott-Kemis, D. and Agarwal, R. (2010), *The OECD innovation strategy: Getting a head start on tomorrow*, https://doi.org/10.1787/9789264083479-en.

OECD (2019), *Measuring the Digital Transformation: A Roadmap for the Future*, OECD Publishing, Paris, https://doi.org/10.1787/9789264311992-en.

OECD (2021), *Mapping Data Portability Initiatives, Opportunities and Challenges*, OECD Publishing.

OECD (2021), *The OECD framework for digital talent and skills in the public sector*, OECD Publishing.

OECD (2023), *OECD Science, Technology and Innovation Outlook 2023: Enabling Transitions in Times of Disruption*, OECD Publishing, Paris, https://doi.org/10.1787/0b55736e-en.

OECD (2024), 'OECD Inter-Country Input-Output Database: Methodology and documentation', accessed 16 October 2026.

OECD (2025), *OECD Science, Technology and Innovation Outlook 2025: Driving Change in a Shifting Landscape*, OECD Publishing, Paris, https://doi.org/10.1787/5fe57b90-en.

OECD (2026), 'Analytical Activities of Multinational Enterprises (Analytical AMNE): Dataset and documentation', accessed 16 October 2026.

OpenLogic (2026), 'State of Open Source Report 2026'.

Pannier, A. (2022), *Software Power: The Economic and Geopolitical Implications of Open Source Software*, Ifri.

Pasimeni, F. and Georgakaki, A. (2020), 'Patent-Based Indicators: Main Concepts and Data Availability', European Commission, JRC121685, accessed 16 October 2026, https://setis.ec.europa.eu/patent-based-indicators-main-concepts-and-data-availability_en.

Pawellek, S., Estorff, I., Wulff, H. and Wendeborn, T. (2026), 'The Digital Competences of Exercise Therapists in Obesity Care: A Step Towards Digital Sovereignty Assessed with the DigCompThExO Questionnaire', *Healthcare*, Vol. 14, Issue 8, p. 1037, https://doi.org/10.3390/healthcare14081037.

Pohle, J. and Thiel, T. (2020), 'Digital sovereignty', *Internet Policy Review*, Vol. 9, Issue 4, https://doi.org/10.14763/2020.4.1532.

SAP (2026), 'What is digital sovereignty? A practical guide', accessed 16 October 2026, https://www.sap.com/resources/what-is-digital-sovereignty.

SkillsFuture Singapore, Workforce Singapore, & Intellectual Property Office of Singapore (2024), 'Skills Framework for Intellectual Property', Government of Singapore, https://jobsandskills.skillsfuture.gov.sg/resources/skills-framework-sector/Intellectual-Property.pdf.

Skouloudi, C., Kantas, E., Drugeot, S., Lopes Goncalves, D., Principe, F. et al. (2024), *Cybersecurity education maturity assessment*, ENISA, Athens, https://doi.org/10.2824/3832.

Synergy Research Group (2025), 'European Cloud Providers' Local Market Share Now Holds Steady at 15%', 24 July.

Thabit Gonzalez, S., Isaraj, L., Kotsev, A. and Friis-Christensen, A. (2026), *Digital Sovereignty Metrics [dataset collection]*, European Commission, Joint Research Centre, JRC Data Catalogue, https://data.jrc.ec.europa.eu/collection/id-00468, accessed 3 November 2026.

Thomson, W (1883), 'Electrical Units of Measurement', *Popular Lectures and Addresses, Volume 1*.

Timmers, P. (2024), 'Sovereignty in the Digital Age', in: Werthner, H., Ghezzi, C., Kramer, J., Nida-Rümelin, J., Nuseibeh, B., Prem, E. and Stanger, A. (eds), *Introduction to Digital Humanism : A Textbook*, Springer Nature Switzerland, pp. 571–592, https://doi.org/10.1007/978-3-031-45304-5_36.

UK Government (2026), 'Digital and data profession capability framework', UK Government, accessed 16 October 2026, https://ddat-capability-framework.service.gov.uk/.

Wachs, J., Nitecki, M., Schueller, W. and Polleres, A. (2022), 'The Geography of Open Source Software: Evidence from GitHub', *Technological Forecasting and Social Change*, https://doi.org/10.1016/j.techfore.2022.121478.

WIPO (World Intellectual Property Organization) (2025), *World Intellectual Property Indicators 2025*, WIPO, https://www.wipo.int/en/web/ip-statistics.

Wire (2025), 'The state of digital sovereignty in Europe 2025', Wire, accessed 16 October 2026, https://wire.com/en/blog/state-digital-sovereignty-europe.

Xu, H., Yu, K., He, H., Fang, H., Vasilescu, B. et al. (2025), 'The Structure of Cross-National Collaboration in Open-Source Software Development', *Proceedings of the 34th ACM International Conference on Information and Knowledge Management (CIKM '25)*, ACM, New York, https://doi.org/10.1145/3746252.3761237.

List of figures

Figure 1 The Digital Sovereignty Framework: four layers shaping EU independence in the digital domain (Di Marco et al., 2025) 10

Figure 2 Multidimensional analysis across four layers of digital sovereignty 12

Figure 3. Workflow for classifying STIP policies 16

Figure 4. 3Ps Framework 18

Figure 5. Evolution of STI policies for strategic digital technologies by primary technology group 20

Figure 6. Prevalence (up) and specialization (down) of policy orientations across digital technologies, 2014–2025 22

Figure 7. Strategic digital technology policy orientations across EU Member States, 2014–2025 24

Figure 8. Strategic digital technology policy orientations across non-EU countries, 2014–2025 25

Figure 9. Country positioning under scope weighting (left) and intensity weighting (right). Projection versus Protection and Research versus Business Promotion, 2014–2025. 28

Figure 10. Country positioning under scope weighting (left) and intensity weighting (right), Projection versus Protection and overall Promotion emphasis, 2014–2025 29

Figure 11. Overview of substitutes, open source share and country-data coverage by layer 34

Figure 12. Eight-state ladder of documented technical substitutability 38

Figure 13. Category-target links (A) and above-baseline target specialization (B) 40

Figure 14. Cumulative breadth of reported substitutability mechanisms by target group 42

Figure 15. Predicted probability of reported *Deployment autonomy*, by target group and open source status 44

Figure 16. Open source share and country-data coverage by target profiles 45

Figure 17. Country composition among solutions with recorded country information 46

Figure 18. Country composition of open source and non-open source solutions by target profile 46

Figure 19. Maps illustrating Capacity, Intensity and Connectedness scores and Clusters, EU-27 55

Figure 20. Evolution of GitHub indicators in the EU and selected comparator countries (2020–2025) 60

Figure 21. Top 20 countries by collaboration weight (EU27 disaggregated), 2025 62

Figure 22. Top 20 countries by collaboration weight (EU27 aggregated), 2025 62

Figure 23. Top 20 countries by GitHub international collaboration with top 5 partnerships (EU-27 aggregated), 2025 63

Figure 24 Top 20 countries by GitHub International Collaboration with top 5 partnerships, 2025 64

Figure 25. International GitHub collaboration network, 2025 65

Figure 26. EU-27 GitHub collaboration network, 2025 66

Figure 27. The DGTES analytical approach applied to measure EU's digital strengths and dependencies from research to scale-up. 71

Figure 28. Share of research activities (left), number of research activities by year (centre), research activities per capita (right) in cloud computing and data technologies 74

Figure 29. Share of innovation activities (left), number of innovation activities by year (centre), innovation activities per capita (right) in cloud computing and data technologies 76

Figure 30. Startups - Number of venture capital deals by year (left), venture capital funding amount by year (centre), venture capital investment flows (right) in cloud computing and data technologies. 78

Figure 31. Scaleups - Number of venture capital deals by year (left), venture capital funding amount by year (centre), venture capital investment flows (right) in cloud computing and data technologies 78

Figure 32. Power-interconnectedness quadrants definition 87

Figure 33. Geographical composition of EU inward and outward multinational production, 2023 .. 89

Figure 34. Evolution of parent-controlled sector output by major economies, 2000–2023 90

Figure 35. Countries power and interconnectedness levels in the IT and Information Services sector, 2023 91

Figure 36. EU countries power and interconnectedness levels in the IT and Information Services sector, 2023 92

Figure 37. Country profiles of key non-EU (left) and EU (right) countries in the IT and Information Services sector, 2023 95

Figure 38. Countries power and interconnectedness levels in the Telecommunications sector, 2023 97

Figure 39. EU countries power and interconnectedness levels in the Telecommunications sector, 2023 99

Figure 40. Country profiles of top non-EU (left) and EU (right) countries in the Telecommunications sector (2023) 101

Figure 41. Countries power and interconnectedness levels in the Computer Electronic and Optical Products sector, 2023 102

Figure 42. EU countries power and interconnectedness levels in Computer Electronic and Optical Products sector (2023) 104

Figure 43. Country profiles of top non-EU (left) and EU (right) countries in Computer Electronic and Optical Products sector (2023) 106

Figure 44. Workflow for the identification and validation of the HS6 codebook. Source: own elaboration. 112

Figure 45. Cross-classification of HS6 codes by digital stack layer and analytical relevance category. Note: labels at the end of each bar report the total number of HS6 codes in the digital stack layer and its percentage share of the final codebook. 113

Figure 46. Distribution of HS6 codes by analytical relevance category 114

Figure 47. EU27 extra-EU imports and exports of products relevant for digital sovereignty, by value-chain position and relevance category, 2024. 116

Figure 48. EU27 trade balance with third countries for products underpinning digital sovereignty, 2024 116

Figure 49. Distribution of bilateral trade dependence indicators from the EU perspective 120

Figure 50. Geographical distribution of asymmetric trade dependency in product underpinning digital sovereignty, 2024 123

Figure 51. EU27 trade value with selected partners 126

Figure 52. Number of EU27 traded products with selected partners 126

Figure 53. EU asymmetric dependence on Taiwan and vice versa (Taiwan asymmetric dependence on the EU) 130

Figure 54. EU asymmetric dependence on China and vice versa (China asymmetric dependence on the EU) 133

Figure 55: EU asymmetric dependence on the US and viceversa (US asymmetric dependence on the EU) 135

Figure 56. Conceptual and structural overview of the treatment of digital sovereignty competences 142

Figure 57. Illustrative visualisation of Indicator 1 – General adult population cybersecurity skills (DSI 2.0 Safety area, % with at least basic skills), 2021, 2023 and 2025 150

Figure 58. Illustrative visualisation of Indicator 5 – Share of ICT specialist workers in employed labour force 151

Figure 59. Illustrative visualisation of Indicator 6 – % of enterprises providing ICT skills training employees (ICT specialists and non-ICT specialists), by organisation size, 2024 152

Figure 60: EU trade value with selected parter by technological layer 184

Figure 61: Number of EU traded products with selected parter by technological layer 184

List of tables

Table 1. Substitutability indicators 35

Table 2. Comparison groups derived from “Alternative to” 37

Table 3. Indicators by layer 41

Table 4. Clustering of comparison countries and heatmap of the Capacity, Intensity and Connectedness scores 59

Table 5. Possible policy directions for each OSS cluster 68

Table 6. Research metrics 73

Table 7. Affinity matrix: research in cloud computing and data technologies 74

Table 8. Innovation metrics 75

Table 9. Affinity matrix: innovation in cloud computing and data technologies 76

Table 10. Startup and scaleup metrics 77

Table 11. Definition of Power and Interconnectedness Indicators 84

Table 12. EU outward and inward ownership-based production footprints, 2023 88

Table 13. Leading economies and EU27 benchmark by production volume in the IT and Information Services sector, 2023 91

Table 14. Ownership structure of IT services production in selected EU host economies, 2023 93

Table 15. Power, Interconnectedness, and Total Production Volume in EU countries in the IT and Information Services sector, 2023 93

Table 16. Leading economies and EU27 benchmark by production volume in the Telecommunications sector, 2023 98

Table 17. Power, Interconnectedness, and Total Production Volume in EU countries in the Telecommunications sector, 2023 99

Table 18. Leading economies and EU27 benchmark by production volume in the Computer Electronic and Optical Products sector, 2023 102

Table 19. Power, Interconnectedness, and Total Production Volume in EU countries in the Computer Electronic and Optical Products sector, 2023 104

Table 20: Approach for identifying potential EU vulnerabilities and strengths in trade positions 121

Table 21 : Asymmetric dependence, by partner country, 2024 124

Table 22 : Asymmetric dependence by partner country, 2017 127

Table 23. Mapping of four foundational digital sovereignty capabilities (based on Di Marco et al., 2025) to three roles and Part C indicators, with specific competences derived from literature 144

Table 24: Mapping of transformative digital sovereignty capabilities (based on Di Marco et al., 2025) to three roles and Part C indicators, with specific competences derived from literature 146

Table 25. List of potentially viable digital sovereignty competence indicators mapped to foundational and transformative digital sovereignty competences and roles (Tables 1 and 2) 148

Table 26. Scope and intensity by instrument type 178

Table 27. Comparison of LLM and rule-based classification results 181

Table 28. Interface 182

Table 29. Deployment autonomy 182

Table 30. Portability 183

Annexes

Annex 1. Mapping Science, Innovation and Technology Policies: Protection, Promotion and Projection in the Digital Domain

This annex makes explicit the analytical workflow used to move from the full STIP policy universe to the corpus analysed in this chapter. It is intended to support transparency and reproducibility.

1.1 Reproducibility prompt

SYSTEM / TASK

You are classifying science, technology and innovation (STI) policy initiatives for a comparative analysis of digital sovereignty. Use only the policy text supplied below. Do not use external knowledge about the country, institution or programme. Be conservative: do not infer a technology or sovereignty mechanism from vague language.

INPUT FIELDS

Textual Fields

NameEnglish	ShortDescription	
Objectives1	Objectives2	Objectives3
Objectives4	Objectives5	Objectives6
Background	Tags	

Structured variables

Use structured columns supplied with the policy record, including thematic classifications (TH*), target-group variables (TG*), and the explicit instrument field “InstrumentTypeLabel”. These variables may corroborate or clarify the policy mechanism, target population, implementation mode or instrument type, but they must not override contradictory or absent textual evidence.

STEP 1 — CRITICAL DIGITAL TECHNOLOGY

Identify a technology only when it is a substantive object, capability, infrastructure, target, regulatory concern or strategic dependency of the policy. Incidental mentions are insufficient. Base this step primarily on NameEnglish, ShortDescription, Objectives1–6, Background and Tags.

Allowed technology labels:

- Artificial intelligence
- Robotics and autonomous systems
- Cloud, edge & HPC
- Data technologies & data infrastructure
- Open-source & foundational software
- Cybersecurity & cryptography
- Blockchain/DLT
- Digital identity & trust technologies
- Quantum technologies
- Semiconductors & microelectronics
- Photonics & optoelectronics

- Advanced connectivity & telecommunications
- IoT, embedded systems & advanced sensing
- Satellite communications and positioning/navigation
If none is defensible, return: no critical digital technology.

If several are substantive, return all relevant labels separated by semicolons.

STEP 2 — PRIMARY TECHNOLOGY GROUP

Assign each policy to one and only one primary technology group, based on the technology that is most central Assign each policy to one and only one primary technology group, based on the technology that is most central to the policy's objectives, instruments and intended outcomes. Use textual evidence and the technology labels identified in Step 1. Use the following categories:

AI & Autonomous Systems: Artificial intelligence; robotics and autonomous systems.

Data & Compute Infrastructure: Cloud, edge & HPC; data technologies and data infrastructure; open-source and foundational software.

Cybersecurity & Digital Trust: Cybersecurity and cryptography; blockchain/DLT; digital identity and trust technologies.

Quantum Technologies: Quantum computing, communication, sensing and related quantum technologies.

Semiconductors & Photonics: Semiconductors and microelectronics; photonics and optoelectronics.

Connectivity & Intelligent Edge. Advanced connectivity and telecommunications; IoT, embedded systems and advanced sensing; satellite communications and positioning/navigation.

Digital Technologies (General/ICT): Use only when the policy substantively targets digital or ICT capabilities but no single strategic technology group above can be identified as its primary focus.

No Digital Technologies — Use when the policy does not substantively address digital technologies.

Decision rules: assign only one primary group; select the group that best represents the main technological focus; do not infer a primary technology from incidental mentions; use Digital Technologies (General/ICT) for genuinely broad digital policies rather than as a fallback; and use No Digital Technologies when substantive digital relevance is not supported.

STEP 3 — POLICY-ORIENTATION FAMILIES

For each of the following 16 policy families, assign 1 when there is substantive evidence that the policy addresses that dimension; otherwise assign 0. Multiple families may be coded 1 for the same policy.

Evidence rule. For Step 3, consider all information available for the policy. This includes the textual fields and all structured STIP variables. Give greater weight to explicit textual evidence when determining the substantive objectives and orientation of the policy. Structured variables should primarily support, contextualise or clarify the textual evidence.

PROTECTION

1. Technological sovereignty & autonomy

"The policy seeks technological sovereignty, strategic autonomy, or greater domestic control over critical digital technologies."

"The policy aims to reduce dependence on foreign technologies or external suppliers and strengthen independent technological capabilities."

"The policy addresses sovereign technological capacity, strategic technological independence, or control over essential digital capabilities."

2. Cybersecurity & secure infrastructure

"The policy strengthens cybersecurity, information security, cyber resilience, or protection against digital threats."

"The policy protects critical digital infrastructure, communications networks, data systems, or essential technological infrastructure."

"The policy develops secure, trusted, resilient or protected digital systems and infrastructure."

3. Strategic dependencies & resilience

"The policy addresses strategic dependencies, supply-chain vulnerabilities, or dependence on critical foreign technological inputs."

"The policy strengthens resilience of critical technology supply chains, components, infrastructure or strategic industrial capacities."

"The policy seeks security of supply and continuity of access to critical technologies, components or digital capabilities."

4. Trust, risk & technology governance

"The policy addresses technology risks, responsible technology use, ethical safeguards, accountability or oversight."

"The policy promotes trustworthy technologies, privacy, safety, certification, standards or regulatory safeguards."

"The policy establishes governance, oversight or risk-management arrangements for emerging digital technologies."

PROJECTION

5. International cooperation

"The policy promotes international cooperation or cross-border collaboration in science, technology or innovation."

"The policy supports multinational research, technology collaboration, international initiatives or cooperation with other countries."

"The policy seeks collaborative international development of strategic or emerging technologies."

6. Strategic partnerships & alliances

"The policy creates strategic partnerships, alliances or bilateral and multilateral technology relationships."

"The policy strengthens international technology partnerships with strategic partners or allied countries."

"The policy develops joint initiatives, agreements, memoranda or institutional partnerships with foreign partners."

7. Global technological leadership

"The policy seeks global or international technological leadership in strategic digital technologies."

"The policy aims to strengthen the country's international competitiveness and global position in advanced technologies."

"The policy seeks to become a leading international actor or technology leader in emerging technological fields."

8. International standards & markets

"The policy promotes participation in international standards, standard setting or global technology governance."

"The policy supports exports, internationalisation, foreign market access or expansion into global markets."

"The policy seeks influence over international technology rules, standards, markets or global value chains."

RESEARCH PROMOTION

9. Research infrastructure

"The policy develops research infrastructure, laboratories, scientific facilities or advanced research equipment."

"The policy invests in computing, experimental or technical infrastructure for scientific research."

"The policy strengthens shared research facilities, scientific infrastructure or technical platforms for researchers."

10. Scientific excellence & frontier research

"The policy supports scientific excellence, frontier research, fundamental research or advanced knowledge creation."

"The policy funds centres of excellence or high-quality scientific research in advanced technologies."

"The policy promotes basic research, exploratory research or long-term scientific discovery."

11. Research talent & scientific skills

"The policy develops researchers, doctoral students, scientific talent or research careers."

"The policy supports fellowships, postgraduate training, PhD education or advanced scientific skills."

"The policy attracts, trains or retains scientific and technical research talent."

12. Universities & public research capacity

"The policy strengthens universities, public research organisations or higher-education research."

"The policy builds public scientific capacity, research institutes or collaborative academic research networks."

"The policy supports knowledge creation, open science or research cooperation among scientific institutions."

BUSINESS PROMOTION

13. Technology adoption & diffusion

"The policy promotes adoption, diffusion or deployment of digital technologies by firms."

"The policy supports business digital transformation, technology uptake or implementation of new technologies."

"The policy helps firms integrate advanced technologies into products, processes or business operations."

14. Commercialisation & scale-up

"The policy supports commercialisation of research, market uptake, scale-up or business growth."

"The policy helps startups and innovative firms bring technologies from research to commercial markets."

"The policy promotes technology transfer, product commercialisation or scaling innovative companies."

15. SMEs, innovation hubs & firm support

"The policy provides technology or innovation support to SMEs, companies or enterprises."

"The policy supports digital innovation hubs, business advisory services or technology extension services."

"The policy provides practical assistance, innovation services or vouchers to firms adopting new technologies."

16. Industrial deployment & value chains

"The policy promotes industrial deployment, manufacturing capacity or development of strategic technology value chains."

"The policy strengthens firms, industrial ecosystems, production capacity or technology-related value chains."

"The policy provides finance, procurement, loans, equity or incentives for business innovation and industrial deployment."

OUTPUT

policy_id:
technology_labels:
primary_technology_group:
Protection:
  Technological sovereignty & autonomy: 0/1
  Cybersecurity & secure infrastructure: 0/1
  Strategic dependencies & resilience: 0/1
  Trust, risk & technology governance: 0/1
Projection:
  International cooperation: 0/1
  Strategic partnerships & alliances: 0/1
  Global technological leadership: 0/1
  International standards & markets: 0/1
Research Promotion:
  Research infrastructure: 0/1
  Scientific excellence & frontier research: 0/1
  Research talent & scientific skills: 0/1
  Universities & public research capacity: 0/1
Business Promotion:
  Technology adoption & diffusion: 0/1
  Commercialisation & scale-up: 0/1
  SMEs, innovation hubs & firm support: 0/1
  Industrial deployment & value chains: 0/1
evidence:
classification_note:

1.2 Policy-instrument coding: Scope and Intensity

We adjust descriptive comparisons for differences in the reach and intervention intensity of policy instruments. The STIP instrument taxonomy distinguishes broad instrument types including governance, direct and indirect financial support, guidance/regulation/incentives and collaborative infrastructures. The analytical scores below translate these instrument types into two simple 1–3 scales. They are not OECD scores.

Scope captures the breadth of the intervention: 1 = targeted, actor-level or narrow programme; 2 = intermediary, sectoral, network or capacity-building intervention; 3 = system-wide, structural or framework-setting intervention. Intensity captures the substantive resource or authority intensity of the instrument: 1 = mainly information, coordination, advice or procedural action; 2 = rules, indirect incentives, institutional capacity or enabling infrastructure; 3 = direct financial resources, procurement, equity, loans or major physical/research infrastructure. The logic is consistent with resource-based policy-instrument approaches that distinguish information/nodality, authority, treasure and organisation as different governing resources (Howlett, 2000; Eliadis et al., 2005).

Table 26. Scope and intensity by instrument type

STIP policy instrument	Scope	Intensity
Strategies, agendas and plans	3	1
Grants for business R&D and innovation	2	3
Project grants for public research	2	3
Dedicated support to research and technical infrastructures	3	3
Networking and collaborative platforms	2	2
Creation or reform of governance structure or public body	3	2
Science and technology regulation and soft law	3	2
Formal consultation of stakeholders or experts	2	1
Policy intelligence (e.g. evaluations, benchmarking and forecasts)	3	1
Public awareness campaigns and other outreach activities	2	1
Institutional funding for public research	3	3
Technology extension and business advisory services	1	1
Information services and access to datasets	2	1
Regulatory oversight and ethical advice bodies	3	2
Standards and certification for technology development and adoption	3	2
Horizontal STI coordination bodies	3	2
Fellowships and postgraduate loans and scholarships	1	3
Labour mobility regulation and incentives	2	2
Procurement programmes for R&D and innovation	2	3
Centres of excellence grants	2	3
Science and innovation challenges, prizes and awards	1	2
Loans and credits for innovation in firms	2	3
Innovation vouchers	1	3
Equity financing	2	3
Tax or social contributions relief for firms investing in R&D and innovation	2	2
Intellectual property regulation and incentives	3	2
Debt guarantees and risk sharing schemes	2	2
Ta relief for individuals supporting R&D and innovation	1	2

Source: JRC

1.3 Quality assurance and limitations of LLM-assisted coding

To assess the reliability of the LLM-assisted coding, a stratified manual validation was conducted on 96 policies, covering the six strategic digital technology groups and all 16 policy-orientation families. The validation deliberately included both clear cases and policies located close to the boundaries between categories. For the technology classification, 48 policies were manually reviewed, with 46 classifications confirmed (95.8%). The two less clear cases concerned policies addressing several interdependent technologies, where the identification of a single *primary* technology group was necessarily judgement-based—for example, initiatives combining AI with cloud/HPC infrastructure or connectivity with advanced sensing. For the 16 policy-family classification, a further 48 policies were reviewed across Protection, Projection, Research Promotion and Business Promotion. 45 of the 48 classifications (93.4%) were consistent with the manual assessment. The remaining cases were primarily matters of conceptual overlap rather than clear misclassification, particularly between *Research infrastructure* and *Scientific excellence & frontier research*, between *International cooperation* and *Strategic partnerships & alliances*, and between *Technology adoption & diffusion* and *Industrial deployment & value chains*. Overall, the validation

indicates a high degree of correspondence between the LLM-assisted coding and human interpretation, while also confirming that a small degree of ambiguity is unavoidable for multi-purpose policy initiatives. The classifications are therefore considered sufficiently robust for aggregate portfolio-level analysis, while individual policy assignments—particularly borderline and multi-dimensional cases—should be interpreted with appropriate caution.

Annex 2. Substitutability of the European Digital Offer: A Digital Sovereignty Perspective

2.1. Prompt used to score the three substitutability indicators

The following prompt is reproduced verbatim from the scoring instruction implemented through the Joint Research Centre's GPT@EC platform via API using GPT-5.4. A temperature of 0.0 was used to minimise stochastic variation and promote consistent classification across observations, while retaining the default nucleus-sampling setting (top_p = 1). As with other generative-model applications, setting the temperature to zero reduces, but does not fully eliminate, the possibility of run-to-run variation.

You are an expert in substitutability of digital solutions.

Evaluate only the supplied "Description", "Features" and "Benefits" textual info. Do not use external knowledge or infer missing technical capabilities from open-source status, product category, provider name, or marketing claims.

- Score 1 only if text documents a specific interoperable interface, protocol, format, API compatibility, or drop-in interface that can facilitate replacement of an existing solution. Generic integrations or API availability without replacement-relevant compatibility do not qualify.
- Score 1 only if text explicitly states customer-run installation, self-hosting, on-premises operation, or deployment on customer-controlled infrastructure. Generic cloud availability, privacy, sovereignty or open-source status alone do not qualify.
- Score 1 only if text describes a concrete mechanism for migrating data/workloads/configuration or switching providers (e.g. standardised export/import with cross-provider context, documented provider-neutral portability, or cross-cloud migration). A bare no-lock-in claim, interoperability without movement, or self-hosting alone does not qualify.

For each indicator return 1=explicit supporting evidence; 0=no sufficient evidence in supplied text. Zero means not documented, not capability absent. If ambiguous, return 0 and flag review. For each score of 1 copy the shortest complete verbatim supporting sentence(s), without paraphrasing, and state Description, Features or Benefits. For 0 leave evidence blank and explain why any borderline sentence does not qualify. Return a unique excel file with the existing columns and added columns of per-row output schema:: interface_score; interface_evidence; interface_source; interface_reason; deployment_score; deployment_evidence; deployment_source; deployment_reason; portability_score; portability_evidence; portability_source; portability_reason; ambiguity_flag.

For each indicator, the score is paired with (i) a verbatim evidence span, (ii) the source field, and (iii) a short reason. This design allows to reconstruct why a positive decision was made and to inspect borderline negatives. The ambiguity flag provides an additional review channel.

2.2. Rule-based text-classification benchmark

To assess the added value of the LLM-based classification, a deterministic rule-based benchmark was implemented using the same three text fields. The benchmark segmented the text into sentences and applied indicator-specific regular expressions and contextual rules, without using an LLM or external information. This provides a transparent and reproducible comparator that performs particularly well when qualifying evidence is expressed through stable lexical cues, such as "self-hosted" or "on-premises". Its main limitation is that it is less able to distinguish substitutability-relevant statements from generic references to compatibility, APIs, import/export functions or migration.

The two approaches were evaluated in two stages. First, rule-based and LLM classifications were compared across the full set of 1,593 solutions. Agreement was very high for deployment autonomy (99.3%) and portability (96.9%), and lower for interface substitutability (90.1%). These figures should be interpreted as measures of concordance rather than accuracy, since neither automated method constitutes a human gold standard.

Second, a targeted manual review was conducted on cases where the two approaches disagreed. The original indicator definitions were used as the adjudication criteria, with ambiguous cases assigned to zero in line with the conservative scoring protocol. For interface and portability, 20 disagreement cases were reviewed; for deployment autonomy, all 11 disagreements were assessed. This produced a 51-case validation sample deliberately concentrated on difficult classifications and therefore not representative of the full dataset.

Table 27. Comparison of LLM and rule-based classification results

Indicator	Full-sample agreement	Automated disagreements	Manually reviewed	LLM preferred after manual review	Rule-based preferred after manual review
Interface	90.1%	158	20	15 (75.0%)	5 (25.0%)
Deployment autonomy	99.3%	11	11	7 (63.6%)	4 (36.4%)
Portability	96.9%	50	20	12 (60.0%)	8 (40.0%)
Total manual disagreement	—	—	51	34 (66.7%)	17 (33.3%)

Source: JRC

Within this disagreement sample, the LLM classification was preferred after manual review in 34 cases (66.7%), compared with 17 cases (33.3%) for the rule-based method. The difference was most pronounced for interface substitutability, where interpretation depends more heavily on whether a stated protocol, format or compatibility feature is genuinely relevant to replacement. The results therefore suggest that deterministic rules are effective for lexically explicit cases and remain useful as an audit and sensitivity tool, while the LLM provides greater value where classification depends on contextual and semantic interpretation.

2.3. Illustrative evidence

This appendix provides a small set of examples to illustrate how the LLM translated the operational definitions of the three substitutability indicators into observable evidence in the text fields. The examples are drawn from positive classifications in the scored dataset and are intended to show the type of textual information that triggered a score of 1. Solution names are withheld because the purpose is methodological validation rather than assessment of individual providers. The examples should be read as evidence of the classification logic, not as representative cases for the population as a whole.

Table 28. Interface

Layer	Source	Evidence sentence	Why it qualifies
Cloud & Infrastructure	Description	It is an Open Source object storage server that is **compatible with Amazon S3**.	Explicit compatibility with the Amazon S3 interface directly supports replacement and interoperability.
Developer Tools	Description	With seamless integration through **OpenAI-compatible endpoints**, it enables developers to build secure, resilient AI applications without the typical enterprise overhead.	The statement documents API-level compatibility with an incumbent interface rather than generic API availability.
Communication & Collaboration	Description	It is committed to open standards like **CalDAV and CardDAV**, ensuring data portability and vendor independence.	Named open protocols provide a specific interoperability mechanism relevant to replacement.

Source: JRC

Table 29. Deployment autonomy

Layer	Source	Evidence sentence	Why it qualifies
Security & Identity	Features	Can be **self-hosted**, providing full control.	Self-hosting explicitly places operation under customer control.
Communication & Collaboration	Benefits	Option for **on-premise deployment** for ultimate control over data.	The on-premises deployment option directly meets the customer-controlled deployment criterion.
Security & Identity	Description	It's available as both software for **deployment on your own hardware** and as a virtual appliance for cloud environments, offering flexibility for various deployment scenarios.	Running the software on the customer's own hardware is an explicit customer-controlled deployment mechanism.

Source: JRC

Table 30. Portability

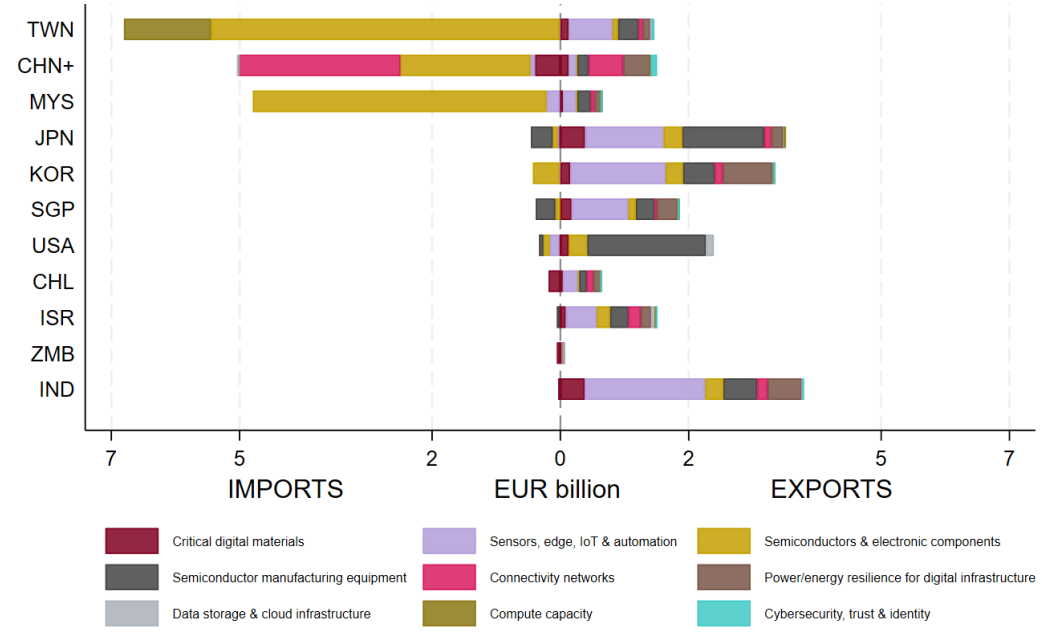
Solution (layer)	Source	Evidence sentence	Why it qualifies
Data & Analytics	Benefits	Easy **migration from existing DNS providers via zone import** and intuitive dashboard.	The sentence names both the origin context (existing providers) and a concrete transfer mechanism (zone import).
Productivity & Office	Features	Risk-free **migration process** with no forced cutover, supporting gradual transition from existing platforms.	A documented migration process from existing platforms is a direct switching mechanism.
Productivity & Office	Features	It offers easy integration through a simple HTML snippet and supports **comment import from other platforms**.	Import from other platforms provides an explicit cross-platform data migration path.

Source: JRC

The three sets of examples also illustrate why the indicators differ in their degree of semantic complexity. Deployment autonomy is often identifiable through relatively stable terminology, while interface substitutability and especially portability require greater attention to context and replacement relevance. For this reason, the retained evidence sentence is useful both for quality control and for human validation of the metric.

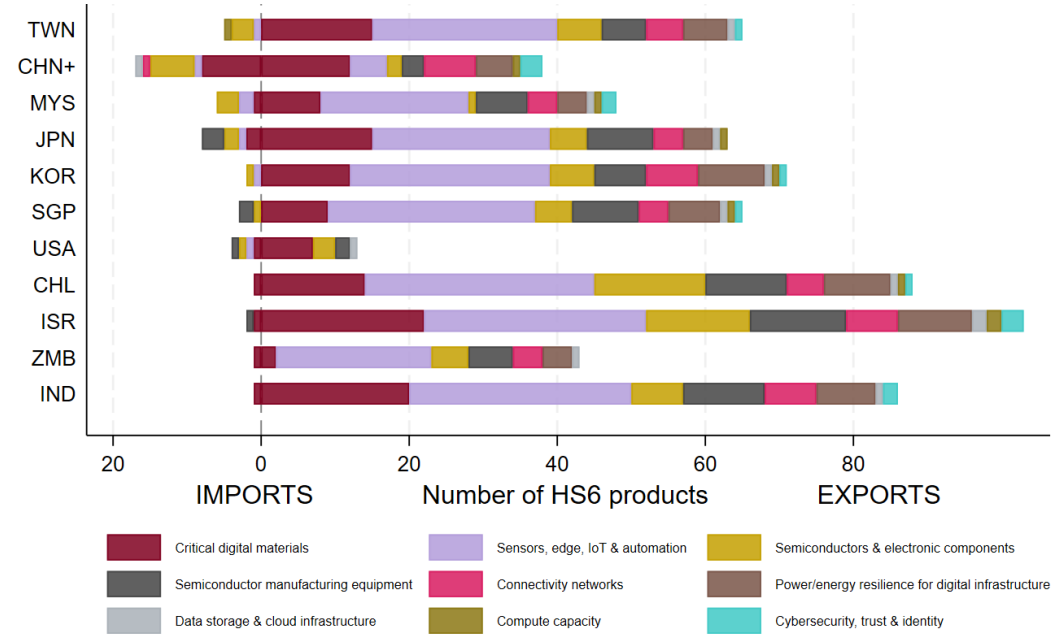
Annex 3. Asymmetric dependence in products underpinning digital sovereignty

Figure 61. EU trade value with selected parter by technological layer



Source: JRC

Figure 62. Number of EU traded products with selected parter by technological layer



Source: JRC

Getting in touch with the EU

In person

All over the European Union there are hundreds of Europe Direct centres. You can find the address of the centre nearest you online (european-union.europa.eu/contact-eu/meet-us_en).

On the phone or in writing

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

— by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),
— at the following standard number: +32 22999696,
— via the following form: european-union.europa.eu/contact-eu/write-us_en.

Finding information about the EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website (europa.eu).

EU publications

You can view or order EU publications at op.europa.eu/en/publications. Multiple copies of free publications can be obtained by contacting Europe Direct or your local documentation centre (european-union.europa.eu/contact-eu/write-us_en).

EU law and related documents

For access to legal information from the EU, including all EU law since 1951 in all the official language versions, go to EUR-Lex (eur-lex.europa.eu).

Open data from the EU

The portal data.europa.eu provides access to open datasets from the EU institutions, bodies and agencies. These can be downloaded and reused for free, for both commercial and non-commercial purposes. The portal also provides access to a wealth of datasets from European countries.

Science for policy

The Joint Research Centre (JRC) provides independent, evidence-based knowledge and science, supporting EU policies to positively impact society

Scan the QR code to visit:

Joint Research Centre
https://joint-research-centre.ec.europa.eu

Publications Office
of the European Union
Law | Data | Publications