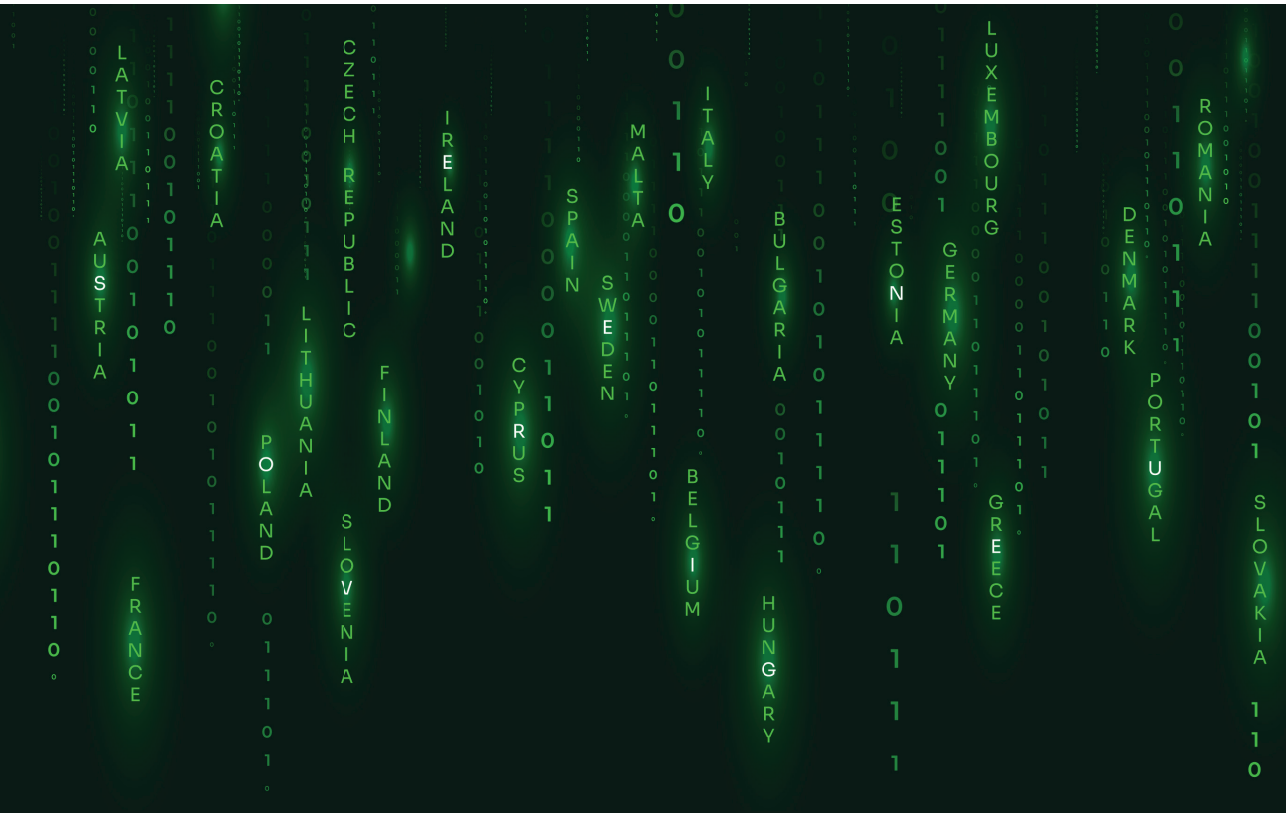
Polish Economic Institute

6/2025

POLICY PAPER



Reforming the Digital Decade: How to Integrate Technological Sovereignty into the EU's Key Digital Strategy?

Citation: Święcicki, I., Witczak, J. (2025), *Reforming the Digital Decade: How to Integrate Technological Sovereignty into the EU's Key Digital Strategy*, Policy Paper, No. 6, Polish Economic Institute, Warsaw.

Policy Paper 6/2025
Warsaw, December 2025
Authors: Ignacy Święcicki, Jakub Witczak
Substantive editing: Paweł Śliwowski
Editorial Work: Jakub Nowak, Małgorzata Wieteska
Graphic Design: Anna Olczak
Typesetting and Layout: Tomasz Gałązka
Polish Economic Institute
Al. Jerozolimskie 87
02-001 Warsaw

Table of contents

Key Findings

- This policy paper contributes to the planned 2026 review of the Digital Decade – a policy framework intended to support digital transformation, enhance competitiveness, and rebuild technological sovereignty in the European Union. Although the issue of digital sovereignty is referenced in the Decision establishing the *Digital Decade Policy Programme 2030* (recital 1 of Decision 2022/2481), **the indicators adopted to measure progress have not sufficiently addressed this objective. We present 12 recommendations regarding areas, goals, and indicators that should be included in next year's review**.

- **The core of our proposal is the integration of Digital Decade objectives and indicators with selected goals of the EU's industrial policy aimed at strengthening European technological sovereignty**. The first five recommendations focus on this issue.

- First, we recommend using **the concept of the technology stack** to measure sovereignty and identifying specific sovereignty levels for the individual layers of the stack (e.g. semiconductors, cloud computing, software). **A policy objective may include increasing Europe's market share in a given layer** (e.g. doubling it – similar to the existing semiconductor goal) **or reducing high-risk dependencies** (e.g. the share of services or products coming from a single supplier or a single country) (→ Recommendation 1).

- In the area of public services, we propose focusing on healthcare and **increasing sovereignty in the storage and processing of Europeans' medical data**. Existing European Commission guidelines on cloud sovereignty may be used for this purpose. Healthcare is also indicated as a priority area for many of the AI factories in Europe (→ Recommendation 2).

- We recommend moving from assessing the availability of medical data to launching active solutions that use such data. Our proposal is **to deploy predictive tools for a defined number of disease categories** (while maintaining sovereignty over data and models), enabling improvements in preventive healthcare and early warnings of severe illnesses (→ Recommendation 3).

- In the crucial long-term **area of education and digital skills, we suggest launching public support for certification of skills in open-source IT systems**. Such a programme could include funding for courses leading to certification at secondary and higher education levels, followed by acceptance of these certificates by public-sector employers to strengthen their use in practice (→ Recommendation 5) (Klekowski, 2025).

- The last recommendation directly related to digital sovereignty is the introduction of local-level measurement of digital sovereignty – in local government units, educational institutions, and healthcare facilities (→ Recommendation 4). This institutional layer is currently not subject to systematic monitoring, yet its role appears crucial both in terms of vulnerability to potential disruptions and in supporting domestic or European technological solutions.

- In addition to integrating digital sovereignty concerns, we also propose **changes to other goals** – either because existing goals are close to being achieved (and the 2035 perspective requires new targets) or because they must be adapted to evolving EU policies.

- Proposed modifications in the area of **connectivity** include focusing on major transport corridors (→ Recommendation 6, a target already mentioned in the communication *Towards a European Gigabit Society*, yet still unmet) and abandoning the costly and unfeasible goal of connecting all households via fibre-optic fixed networks (→ Recommendation 7).

- In terms of **digital transformation of firms**, our proposed indicators aim to measure the actual outcomes of support for innovative enterprises. For example, Europe's challenge lies not in the absence of promising start-ups, but in the fact that young, high-growth firms relocate overseas; therefore, **attention should be paid to where the so-called exit occurs** (→ Recommendation 8). The existing gap between European companies and leaders in digital innovation can be assessed through R&D expenditure among digital-sector firms (→ Recommendation 9). We also recommend including micro-enterprises in the measurement framework, as they represent the numerical majority of the European economy (→ Recommendation 10).

- We also propose expanding the Digital Decade to include cybersecurity goals and indicators, an essential area that has so far been missing from the programme. Existing metrics developed by ENISA (2025) may be used (→ Recommendation 12). Drawing on Poland's experience with the *Cybersecure Local Government* programme, we additionally recommend assessing cybersecurity levels in local government units.

Introduction

A review of the *Path to the Digital Decade* policy programme, which sets the European Union's digital transformation targets for 2030, is currently under way. The review stems not only from formal requirements[1] but also from changes taking place in public policies in the area of digitalisation. The new composition of the European Commission, together with the re-defined work priorities and mission of the College of Commissioners, naturally leads to a reassessment of previously adopted strategic directions. At the same time, growing pressure to strengthen Europe's technological and digital sovereignty makes it necessary to update the targets and to select new indicators used to measure their achievement.

Although the Decision establishing the *Digital Decade Policy Programme 2030* (Recital 1 of Decision 2022/2481) refers to digital sovereignty, the indicators adopted for monitoring progress did not sufficiently capture this objective. The extent of EU Member States' dependence on external cloud-service providers, highlighted, among others, in the Draghi Report (2024), and dependencies observed across several layers of the so-called digital stack (Bria, Timmers, Gernone, 2025) lead to the conclusion that indicators measuring only business digitalisation, digital skills, start-up development or the digitalisation of public administration are not adequate. A focus limited to such metrics[2] may perpetuate or deepen technological dependencies and maintain the European Union's weak position in the global digital economy. In our assessment, the only indicator currently in use that is directly linked to rebuilding sovereignty is the EU share in the global semiconductor market.

For these reasons, we propose specific changes to both the Digital Decade targets and the indicators used to measure them. It should be emphasised that modifying indicators is a natural part of multi-year strategic frameworks: it results from the exhaustion of certain measures (e.g. approaching an already-set target), evolving public-policy priorities (such as the increasing importance of technological sovereignty) and the need to incorporate new policy domains.

[1] Art. 4(2) of the Decision of the European Parliament and of the Council (EU) 2022/2481.
[2] A full description of the Digital Decade indicators, albeit without reference to the issue of digital sovereignty, was presented in the study by Święcicki and Witczak (2023).

Our starting point is the latest Communication on the State of the Digital Decade (European Commission, 2025a), which presents the degree of progress towards all existing targets. Therefore, this paper does not provide a systematic assessment of the current state of play. At the same time we situate our proposals within the broader landscape of EU public policies, highlighting interlinkages across domains and the cross-cutting importance of digital transformation. Therefore we treat the Digital Decade targets not only as mere numerical targets, but as policy-creating instruments, aimed at focusing policymakers' attention towards specific, long-term effects of public policies.

Proposed Indicators Related to Sovereignty

Using the Concept of the Technology Stack to Assess the Level of Digital Sovereignty

In discussions on embedding technological-sovereignty measures into the framework of the Digital Decade, it is useful to draw on the concept of the technology stack (Bria, Timmers, Gernone, 2025). This approach describes the dependencies and interlinkages among foundational products (semiconductors), services (cloud computing), infrastructure (networks, data centres), platforms and applications. It makes it possible to identify levels of dependence and to monitor the effects of policy interventions. It is estimated that 80% of the EU cloud-computing market is served by non-European companies (Draghi, 2024), and that dependence on the supply of mobile devices is close to total. **Within the Digital Decade, the only element currently monitored in this context is the share of EU entities in the global semiconductor market (currently 10.5%, with a target of 20%)** (European Commission, 2025a).

There are currently no widely accepted metrics for technological sovereignty. As noted by Święcicki and Witczak (2025b), the European Commission has developed a methodology for assessing dependencies in goods trade (Garcia, Ho, 2025), which is useful, for example, for analysing dependencies in the semiconductor or network-equipment sectors. However, it is more difficult to precisely determine the level of dependence (or its opposite, sovereignty) in those layers of the stack that consist of services.

RECOMMENDATION 1.

Use the technology-stack concept to measure sovereignty and specify concrete sovereignty levels for each layer of the stack (e.g. semiconductors, cloud computing, software). The target may be to increase Europe's market share in a given layer (e.g. a twofold increase, similar to the current formulation for semiconductors) or to limit high-risk dependencies (e.g. the share of services/products coming from a single supplier or a single country).

Operationalisation

To estimate current dependence levels in layers such as semiconductors, raw materials or devices, the existing EXVI methodology and the assessments already conducted by the JRC (Bonnet, Ciani, 2023) can be used. For other layers, preliminary estimation may rely on market data (e.g. cloud-market shares) or trade data (with a caveat regarding their much lower granularity compared with goods-trade statistics). Existing indicators such as the Digital Dependence Index or established measures such as the Herfindahl–Hirschman Index for import concentration may also be used.

To define critical dependence thresholds and target levels, it is possible to refer to benchmarks adopted in the *Critical Raw Materials Act* (Regulation (EU) 2024/1252), which sets, for example, a target of limiting dependence on a single supplier country to no more than 65% of total supply.

In the longer term, it may be necessary to develop a separate methodology for assessing dependencies in services trade, including the collection of more detailed trade data.

Link with other EU policies

Technological sovereignty is now one of the central themes of debates on EU industrial policy and security. Its importance is reflected, among other things, in the appointment of a Vice-President of the European Commission whose portfolio explicitly covers technological sovereignty, and the presence of this topic in speeches by Commission officials and Member State representatives. The need to strengthen autonomy is also emphasised by Mario Draghi (2024). A similar objective underpins the Critical Raw Materials Act mentioned above, and in one of the recent cloud-services procurement procedures the European Commission, for the first time, presented a set of criteria for assessing the sovereignty level of services being procured.

Digital Public Services

Practical efforts to rebuild digital sovereignty can be implemented in the development of digital public services, where policymakers have the most direct influence over technological choices. Ensuring control over data, adopting strategies to avoid dependencies in critical processes, and supporting the growth of the European technological ecosystem are all measures that can set an example for the private sector and increase awareness of the benefits of relying on sovereign solutions.

At the same time, it is worth noting that **the indicators measuring targets in the digital public services pillar are already at high levels of achievement, i.e. exceeding 80% of their intended values**. In such circumstances, it may be advisable to move from more general metrics, focused on central-government activities, toward more detailed goals related to the digitalisation of Member States. This deeper approach could include sector-specific objectives and a shift toward lower administrative levels, such as local government. **Local administrations are often less digitally advanced and more vulnerable to disruptions in access to and functioning of technologies, as they have limited resources to respond quickly to emerging problems**.

Among the current goals of the Digital Decade is to ensure full access to electronic medical data for all citizens. The target is close to being achieved (82.7% of the intended level), but its fulfilment within the original 2030 deadline still requires monitoring. Looking toward 2035, it is reasonable to define new objectives that reflect Europe's growing ambitions relating to security and sovereignty. Under this approach, the existing goal could serve as a technical indicator, to be phased out in the future once the expected 100% level is reached.

We recommend taking steps toward establishing stronger oversight of medical data stored within healthcare systems by using the European Commission's guidelines for determining the sovereignty level of cloud-computing infrastructure (European Commission, 2025b). These guidelines incorporate best practices from EU Member States, recognise risks in international trade in goods and services, and stress the need to verify the safeguards declared by cloud-service providers. Given the sensitivity of medical data, it is worth considering the introduction of guidelines aimed at increasing the sovereignty of the associated cloud infrastructure, in line with the Commission's recommendations. Such action would also raise awareness among Member States that infrastructure is not neutral and that decisions concerning it must account for oversight requirements.

RECOMMENDATION 2.

Increase sovereignty in the storage and processing of Europeans' medical data by introducing a methodology for assessing the sovereignty level of cloud-computing infrastructure in the healthcare sector and achieving a high sovereignty level (e.g. SEAL3[3] or higher, in line with European Commission *Cloud Sovereignty Framework*, 2025b).

Operationalisation

Member State reporting of the share of cloud systems used in public healthcare for processing medical data that comply with European Commission framework at SEAL3 or higher.

Additionally, when refining objectives in the healthcare domain, it should be noted that the current target (100% of citizens having electronic access to their medical data) may be achieved as early as 2027 (European Commission, 2025c). It therefore seems reasonable to take the next step and focus on concrete outcomes of the digital transformation of healthcare. One such outcome could be strengthening preventive healthcare using medical data and AI algorithms to improve population health and reduce healthcare-system costs.

RECOMMENDATION 3.

Modify the target for digital health services: shift away from measuring the availability of medical data (or retain this as a technical indicator with a 2030 deadline) and introduce a 2035 target for the deployment of predictive tools (for a defined number of disease entities, while maintaining sovereignty at the levels of data and models) to support preventive healthcare and early warning against serious illnesses.

Operationalisation

The target could be the number of disease entities for which predictive tools have been implemented in the healthcare system (e.g. 100 by 2035). Such data are currently unavailable; their collection would require an additional survey as well as the use of standards defining sovereignty levels of IT solutions.

[3] The SEAL3 level of cloud sovereignty, according to the European Commission's guidelines, means that EU law applies and is enforceable, entities from the European Union exert significant but not full control, and the services, technologies or operations involved are subject to only marginal oversight by non-EU third parties.

Link with other EU policies

Strengthening European digital sovereignty in healthcare aligns with EU's ambitions reflected in the specialisations of a number of AI factories (i.e. in Poland, Jupiter AI Factory in Germany or 1HealthAI in Spain). These recommendations are also consistent with the assumptions of the *European Health Data Space* (EHDS) Regulation, which places strong emphasis on medical-data security, and are aligned with the NIS2 supply-chain security requirements. Using predictive tools in healthcare systems will enable practical use of medical data collected under the EHDS and will additionally motivate the digitalisation of medical institutions.

Building European digital sovereignty requires, to a large extent, an understanding of existing dependencies. Only then is it possible to assess the risks arising from those dependencies and to design actions aimed at minimising them. One potential measure is the introduction of regular reporting by local government units and their subordinate entities regarding the presence of digital dependencies. Such reporting could take the form of self-assessment based on harmonised frameworks enabling an evaluation of existing digital dependencies in areas such as: IT systems (assessment of software providers), computing and cloud infrastructure (assessment of cloud-service and server providers and of data-access rules), and ICT hardware (assessment of suppliers of computers and mobile devices). Reporting should also include an assessment of an entity's ability to switch suppliers of particular devices and services. An example of an existing framework with a similar purpose is Austria's Digital Sovereignty Compass (Bundesministerium Finanzen, Bundesministerium Inneres, Digital Austria, 2023).

The introduction of digital-dependency assessments would not aim at full decoupling from non-European providers of digital technologies, but rather at understanding where critical dependencies occur, enabling awareness-building and further decision-making such as enhancing system interoperability, creating backup solutions, seeking secure and sovereign alternatives, or ultimately designing public policies based on data. Such a standardised assessment would therefore generate benefits at the local, national, and EU-wide levels.

RECOMMENDATION 4.

Introduce measurement of digital sovereignty at the local level - in local government units, educational institutions, and healthcare providers, by developing harmonised frameworks and assessment criteria. For example, the measurement could cover issues such as cybersecurity in local governments, office-software tools used in educational programmes, or methods of data storage in the healthcare sector.

Operationalisation

Measurement could be carried out on an annual cycle, but with a rotation of institutions (similar to the e-Government Benchmark, where a different set of public services is assessed each year), thus limiting administrative burdens. Data should be collected in a way that ensures comparability across countries. One example of a measurable indicator could be the presence of modules on open-source application suites in educational curricula (Klekowski, 2025).

Link with other EU policies

The recommendation aligns with broader EU-level efforts to rebuild European digital sovereignty and complements measures and indicators applied at both EU and national levels. It is also consistent with initiatives related to digital-skills development (including the use of open-source tools or alternatives to currently dominant solutions) and the digitalisation of healthcare.

Digital Skills

In the area of digital skills, following Klekowski (2025), we draw attention primarily to ICT specialists - individuals who are largely responsible for decisions concerning the technologies used within European companies and institutions.

The indicators adopted to date for ICT specialists do not account for the dimension of technological dependencies. Today's leading digital-market players also dominate the field of ICT training and offer trainees widely recognised certification programmes attesting to their skills (Klekowski, 2025). Software providers, by ensuring accessible and widely accepted training offers and by partnering with public institutions or universities, effectively support digitalisation, yet simultaneously pursue their own business objectives, including increasing the visibility of their solutions and building user familiarity among trained professionals. The result is a greater likelihood that ICT specialists will later choose precisely those technologies.

To build a counterweight to the most widespread solutions, which are, to a significant degree, offered by non-European providers, it is advisable to promote the dissemination of certification related to open-source systems and to encourage employers to recognise such credentials. A promising approach would involve promoting and subsidising this type of certification in technical secondary schools, higher-education institutions, and public administration, as well as offering preferential conditions for ICT specialists seeking to upgrade their skills.

RECOMMENDATION 5.

Introduce public support for the certification of skills related to open-source IT systems, including funding for certified training courses in secondary and higher education, and the subsequent recognition of such certificates by public-sector employers, in order to consolidate their use.

Operationalisation

A suitable indicator is currently lacking; it is necessary to conduct an inventory of desirable certificates and of the number of specialists who hold them. Klekowski (2025) points to the use of an OpenStack-based approach. Such information can then be related to the total number of ICT specialists currently published by Eurostat. A key challenge at this stage is the data-collection method: the number of ICT specialists is derived from the LFS, whose structure does not allow for questions regarding the type and number of certificates obtained.

Link with other EU policies:

The European Union and its Member States support open-source solutions and emphasise their importance for strengthening European companies and reducing costs for digital-services users. However, the last comprehensive strategy in this area covered the years 2020–2023 (European Commission, 2020), and current support is dispersed across various sectoral initiatives.

Modifications to the Remaining Digital Decade indicators

Digital Infrastructure

In the area of digital infrastructure, the target values for two indicators have been nearly achieved: 5G coverage (94% in 2024) and coverage with very high-capacity networks – VHCN (82.5% in 2024). The first indicator refers to populated areas, yet the communication *Connectivity for a Competitive Digital Single Market: Towards a European Gigabit Society* (European Commission, 2016) underlined the need to ensure coverage also along major transport corridors. Currently, however, such data are not collected (European Commission, 2024; 2025c), even though the problem of insufficient connectivity along transport routes remains unresolved. Access to fast mobile networks improves the comfort of travellers, supports the digitalisation of European logistics (including real-time fleet management), and enables the development of connected and autonomous mobility (CAM) (www1).

As for the second indicator, **achieving 100% coverage entails very high costs and is economically inefficient**. For households that still lack access to such networks because they are located in remote areas, radio links or high-quality mobile network coverage should serve as alternatives (Ledzion et al., 2025). From the perspective of social welfare, the desirable goal is to ensure functionally adequate internet access, irrespective of whether the underlying technology is wired or wireless. As such solutions include radio and mobile networks, indoor coverage quality should also be taken into account.

RECOMMENDATION 6.

Introduce a target to ensure 5G coverage along all major transport corridors in the EU, enabling effective internet use on trains, in road vehicles and along inland waterways.

Operationalisation

Introduce a classification of transport corridors to identify those covered by the measurement[4]. Collect baseline and regular follow-up data, for example, through datasets gathered by national telecommunications regulators. A possible indicator: the length of priority corridors covered by 5G networks as a share of the total length of priority transport corridors in a given country.

RECOMMENDATION 7.

Revise the target of achieving 100% coverage of households with VHCN and 100% FTTB/DOCSIS 3.1 coverage. The target should be to ensure functional internet access for all households, regardless of technology. This objective should be met by 2030, and not postponed to 2035.

Operationalisation

Define the minimum parameters of functional access to the internet (technical thresholds[5] or a list of essential services that must be fully usable[6]). Data should be collected by national telecommunications regulators and complemented by field tests in diverse localities.

Link with other EU policies

Ensuring high-quality connectivity along the main transport corridors aligns with the priorities of strengthening the EU Single Market and is consistent with the planned development of the European high-speed rail network (Letta, 2024). Currently, within CEF-Digital, the EU supports the deployment of 5G infrastructure along selected cross-border transport corridors of the Trans-European Transport Network (www3).

[4] In Poland, for the coverage obligations accompanying spectrum auctions for mobile networks, a distinction was made between national and regional roads, and specific railway lines were also identified on which network coverage must be ensured. https://bip.uke.gov.pl/konsultacje-i-wyniki-konsultacji/prezes-uke-oglasza-konsultacje-aukcji-na-7-rezerwacji--czestotliwosci-z-pasm-ponizej-1-ghz,3158.html [accessed 14.11.2025].
[5] The approach adopted, for example, in the frequency auction in Poland [link as above].
[6] The approach used in the European Electronic Communications Code.

Digital Transformation of Business

In the area of digital business transformation, much remains to be done to meet the currently defined targets. However, **we recommend modifying the existing goals to place greater emphasis on the effects of ongoing efforts (start-up exits), to strengthen the focus on future technologies (R&D), and to provide fuller monitoring of the entire business population, including micro-enterprises**.

The Path to the Digital Decade programme currently assumes that closing the innovation gap between the European Union and the United States and China will foster digital innovation and technological sovereignty. Progress toward this objective is measured by the target of doubling the number of European 'unicorns', that is, start-ups and scale-ups valued at over USD 1 billion. The number of such firms is treated as a proxy for the EU's ability to create an innovation-friendly environment by promoting technology transfer, deploying public funding, and attracting private capital.

However, this indicator fails to capture a crucial issue highlighted in the latest report on the state of the EU's Digital Decade (European Commission, 2025a): the Union's limited ability to prevent innovative firms from relocating outside the EU. Ensuring that such companies remain in Europe, by creating favourable conditions for doing business, is essential for strengthening European technological sovereignty.

An alternative indicator to the number of unicorns could be the share of European technology start-ups that complete their exit within Europe, rather than in markets outside the EU (e.g. in the United States). Although imperfect, such a measure would allow a relative assessment of the EU's attractiveness for innovative enterprises, instead of merely tracking the nominal number of firms.

RECOMMENDATION 8.

Replace the indicator based on the number of European unicorns with the share of start-ups that complete their exit on European markets. Exit is defined here as either an IPO or the sale of the company to an entity with European capital.

Operationalisation

The baseline and target values may be determined using data from datasets already used by the European Commission, such as Dealroom or Crunchbase. A possible ambition level would be, for example, doubling the indicator calculated for 2024.

Link with other EU policies

The EU has adopted the *EU Startup and Scaleup Strategy* (European Commission 2025e), with the aim of creating a thriving startup and scaleup ecosystem in Europe. The Strategy includes measures to alleviate problems related to scaling and increasing the availability of suitable exit options for successful companies. Achieving these goals (and the proposed indicator) requires the deepening of the capital market in Europe—developing stock exchanges and improving access to capital in major corporations. It is therefore directly linked to the creation of a Union of Savings and Investments. The European Commission's strategy presented in spring 2025 (European Commission, 2025d) diagnoses the challenges facing Europe's innovative firms, including insufficient exit opportunities, and sets out actions designed to overcome these barriers.

Europe's lag in the global technology race manifests itself not only in the level of adoption of digital technologies, but also - and perhaps above all - in the scale of private investment in the creation of new solutions in the fastest-growing sectors. Regular research conducted by the JRC (Nindl et al., 2024) shows that European firms fall behind particularly in the sectoral structure of R&D expenditure (Święcicki, 2025). In 2023, companies from the EU accounted for only 8% of global R&D spending in the sectors Computer software and services and Technology hardware & equipment, compared with 15.2% for Chinese firms and as much as 66.4% for US firms. By contrast, the largest European companies originate primarily from the automotive sector. Given the importance of breakthrough digital technologies, it is essential to stimulate a substantial increase in European private R&D outlays in this area.

RECOMMENDATION 9.

Introduce an indicator measuring the share of R&D expenditure in the area of computer software, services and hardware incurred by European firms, together with a specific target, for example, doubling the current value (from 8% to 16%).

Operationalisation

Relevant data are collected and published annually by the JRC (www2), and subsequently presented by country, world region and sector. Our proposal focuses on R&D expenditure for EU countries (region: EU) in the categories Computer software and services and Technology hardware & equipment, compared with total R&D expenditure of all classified firms in these two sectors. Optionally, this category could be extended to include telecommunications (Fixed line telecommunications, Mobile telecommunications).

Link with other EU policies

Any strategies aimed at stimulating the European digital market, from the *Apply AI Strategy* and the *EU Chips Act* to the IPCEI projects (such as IPCEI ME/CT) (www8), will directly support the achievement of this goal.

Analysing the remaining indicators used to measure the digital transformation of businesses (the share of firms using AI, cloud computing and data analytics), it should be noted that the current targets do not incorporate a sovereignty component. While the dissemination of digital technologies will drive productivity growth in Europe in the short term (Święcicki, Witczak, 2025a; www3), long-term security requires strengthening the digital resilience of all sectors of the economy. At this stage we recommend keeping the existing indicators and supplementing the portfolio of targets with the technology-stack-based approach, as discussed earlier in this paper.

A key modification to improve the monitoring of digitalisation levels in the EU is the inclusion of micro-enterprises in official surveys. Current mandatory surveys cover only firms with at least 10 employees, thereby excluding a substantial portion of the economy responsible for 19.2% of value added and 30.1% of employment (www7).

RECOMMENDATION 10.

Extend mandatory surveys on the level of business digitalisation to include micro-enterprises (0–9 employees).

Operationalisation

The survey could be incorporated into the regular statistical programme or carried out separately at longer intervals. It should follow existing Eurostat (2023) guidelines for the optional survey on the digitalisation of micro-enterprises to ensure consistency and comparability of data.

Link with other EU policies

This recommendation is consistent with the Digital Decade programme and enhances the accuracy of monitoring Europe's digital transformation. It also complements the framework of European ICT usage statistics in business, which currently leave the measurement of ICT adoption among enterprises with up to 9 employees optional for Member States.

Cybersecurity

Cybersecurity is one of the areas currently not included in the Digital Decade, but it is analysed within separate initiatives, including those carried out by ENISA (2024a). This area is unquestionably essential for the effective digital transformation of the EU, both from an economic and a societal perspective. Cybersecurity issues are covered in other studies; in the context of EU security, it is particularly important to highlight the research conducted by ENISA (2024a). The proposed set of indicators (ENISA, 2024b) includes data on cybersecurity activities undertaken by firms, citizens' skills, R&D expenditure, and the maturity level of national administrations in the area of cybersecurity. Although publicly available reports do not provide complete results, in our view creating a parallel measurement system for cybersecurity would not be justified.

At the same time, one dimension missing from these studies is the level of cybersecurity measured at the level of local governments. This is the administrative level at which most citizens interact with public authorities, and it may become a weak link in defence structures against cyber threats.

A best practice example comes from Poland, which implemented the programme *Cyberbezpieczny samorząd* (Cyber-secure Local Government), co-financed by European Funds for Digital Development aimed at raising the level of information security in public administration by funding activities within local government units (www4). The programme produced guidelines for LGUs and introduced the requirement for all participating units (in practice, almost all LGUs in Poland) to undergo an audit.

RECOMMENDATION 11.

Introduce an assessment of cybersecurity maturity at the level of local governments.

Operationalisation

A suitable indicator is currently lacking, but the experience of the *Cyberbezpieczny samorząd* project, including the audit of local government units participating in the programme, may be used as a foundation.

RECOMMENDATION 12.

Use the EU-Cybersecurity Index developed by ENISA as an additional indicator measuring the level of cybersecurity at EU level (ENISA, 2025).

Operationalisation

The index is measured and publicly available at the EU level every two years (first measurement in 2024) (ENISA, 2025). Detailed country-level values, which enable the formulation of targeted recommendations, are available to designated national authorities; this element of translating strategy into action would likely have to remain non-public.

As an alternative approach, we propose including cybersecurity in a more limited scope, based on data that are publicly available. This approach would focus on training and certification of specialists, with the aim of improving the security posture of enterprises. This approach is also recommended by ENISA experts (www5).

RECOMMENDATION 12A.

Use indicators measuring the level of cybersecurity skills (confirmed by certifications) in line with the European Cybersecurity Skills Framework (ECSF) (www6), among employees holding relevant certificates.

Operationalisation

A suitable indicator is currently lacking; measurements could rely on the number of certificates issued in line with ECSF profiles. A possible target value could be 600,000 certified individuals (reflecting the estimated shortage of cybersecurity specialists in 2024, based on Święcicki, Karolak, 2025).

Link with other EU policies

Ensuring a high level of cybersecurity in the EU is the subject of numerous initiatives and policy goals, including the NIS2 Directive, the establishment of the European Cybersecurity Competence Centre, and the Cybersecurity Act.

Bibliography

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

Bonnet, P., Ciani, A. (2023), *Applying the SCAN methodology to the Semiconductor Supply Chain*, JRC Working Papers in Economics and Finance, No. 8, European Commission, Ispra.

Bundesministerium Finanzen, Bundesministerium Inneres, Digital Austria (2023), *Digitaler Aktionsplan: Digitale Souveränität für Österreich*, Vienna.

Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Policy Programme *Path to the Digital Decade 2030* (OJ L 323, 19.12.2022), https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32022D2481 [accessed: 24.11.2025].

Draghi, M. (2024), *The Future of European Competitiveness — A Competitiveness Strategy for Europe*.

ENISA (2024a), *2024 Report on the State of the Cybersecurity in the Union*, https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union [accessed: 14.11.2025].

ENISA (2024b), *EU Cybersecurity Index: Framework and methodological note*, https://www.enisa.europa.eu/sites/default/files/2024-12/eu_csi_methodological_note_v1-0.pdf [accessed: 14.11.2025].

ENISA (2025), *THE EU-Cybersecurity Index 2024: EU-level insights and next steps*, https://www.enisa.europa.eu/sites/default/files/2025-06/The%20EU%20Cubersecurity%20Index%202024_en_0.pdf [accessed: 14.11.2025].

European Commission (2016), *Connectivity for a Competitive Digital Single Market: Towards a European Gigabit Society*, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2016) 587 final, Brussels.

European Commission (2024), *How to master Europe's digital infrastructure needs?*, White Paper, COM(2024) 81 final, Brussels.

European Commission (2025a), *State of the Digital Decade 2025: Keep building the EU's sovereignty and digital future*, Communication from the Commission, COM(2025) 290 final, Brussels.

European Commission (2025b), *Cloud Sovereignty Framework*, Version 1.2.1, Luxembourg, https://commission.europa.eu/document/download/09579818-64a6-4dd5-9577-446ab6219113_en?filename=Cloud-Sovereignty-Framework.pdf [accessed: 14.11.2025].

European Commission (2025c), *5G Observatory*, Report, https://digital-strategy.ec.europa.eu/en/policies/5g-observatory [accessed: 14.11.2025].

European Commission (2025d), *Union of Savings and Investment. A Strategy to Increase the Wealth of Citizens and the EU's Economic Competitiveness*, Communication from the Commission, COM(2025) 124 final, Brussels.

European Commission (2025e) *The EU Startup and Scaleup Strategy. Choose Europe to start and scale*, Communication from the Commission, COM (2025) 270 final, Brussels

Eurostat (2023), *European businesses statistics compilers' manual for ICT usage and e-commerce in enterprises*, Luxembourg, https://ec.europa.eu/eurostat/documents/3859598/18369750/KS-GQ-23-012-EN-N.pdf/20fb6a79-2c43-df3d-1551-7366c72f5f8c?version=2.0&t=1706102581439 [accessed: 28.11.2025].

Garcia, W.C., Ho, V. (2025), *EXternal Vulnerability Index (EXVI)*, Single Market Economics Briefs, No. 14, European Commission, Brussels.

Klekowski, T. (2025), *W dążeniu do suwerenności cyfrowej: Mapa technologicznych zależności Polski i Europy*, THINKTANK.

Ledzion, B., Miller, A., Kwinta, J., Krygowska, N., Święcicki, I. (2025), *Ewaluacja ex post realizacji celów Programu Operacyjnego Polska Cyfrowa na lata 2014–2020*, Final Report, https://www.rozwojcyfrowy.gov.pl/media/156083/POPC_Raport_koncowy_expost_14082025.pdf#page=182.08 [accessed: 14.11.2025].

Letta, E. (2024), *Much More Than a Market. Speed, Security, Solidarity. Empowering the Single Market to Deliver a Sustainable Future and Prosperity for All EU Citizens*, https://www.consilium.europa.eu/media/ny3j24sm/much-more-than-a-market-report-by-enrico-letta.pdf [accessed: 27.11.2025].

Nindl, E., Napolitano, L., Confraria, H., Rentocchini, F., Fako, P., Gavigan, J., Tuebke, A. (2024), *The 2024 EU Industrial R&D Investment Scoreboard*, Publications Office of the European Union, Luxembourg, https://data.europa.eu/doi/10.2760/0775231, JRC140129 [accessed: 21.11.2025].

Regulation (EU) 2024/1252 of the European Parliament and of the Council of 11 April 2024 establishing a framework to ensure a secure and sustainable supply of critical raw materials and amending Regulations (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1724 and (EU) 2019/1020 (OJ L 2024/1252, 3.5.2024), https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX:32024R1252 [accessed: 27.11.2025].

Święcicki, I. (2025), *Europa pozostaje w tyle za USA i Chinami w dziedzinie B+R*, "Tygodnik Gospodarczy PIE", No. 1, Polski Instytut Ekonomiczny, Warsaw, https://pie.net.pl/wp-content/uploads/2025/01/Tygodnik-PIE_1-2025.pdf [accessed: 21.11.2025].

Święcicki, I., Witczak, J. (2023), *Jak osiągnąć cele cyfrowej dekady w Polsce?*, Policy Paper No. 6, Polski Instytut Ekonomiczny, Warsaw, https://pie.net.pl/wp-content/uploads/2024/03/PP-6-2023_Cyfrowa-dekada-w-PL.pdf [accessed: 24.11.2025].

Święcicki, I., Witczak, J. (2025a), *W poszukiwaniu priorytetów rozwoju AI w Polsce*, Policy Paper No. 5, Polski Instytut Ekonomiczny, Warsaw, https://pie.net.pl/wp-content/uploads/2025/06/PIE_Policy-Paper_W-poszukiwaniu-priorytetow-rozwoju-AI-w-Polsce.pdf [accessed: 24.11.2025].

Święcicki, I., Witczak, J. (2025b), *Europa próbuje odbudować suwerenność technologiczną*, "Tygodnik Gospodarczy", No. 45, Polski Instytut Ekonomiczny, Warsaw, https://pie.net.pl/wp-content/uploads/2025/11/Tygodnik-PIE_45-2025.pdf [accessed: 24.11.2025].

(www1) https://digital-strategy.ec.europa.eu/en/policies/connected-and-automated-mobility [accessed: 14.11.2025].

(www2) https://iri.jrc.ec.europa.eu/rd_monitoring [accessed: 21.11.2025].

(www3) https://digital-strategy.ec.europa.eu/en/policies/cross-border-corridors [accessed: 14.11.2025].

(www4) https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad2 [accessed: 14.11.2025].

(www5) https://www.enisa.europa.eu/sites/default/files/2025-10/Cybersecurity%20Skills%20Panel%20-%20Expert%20Perspectives.pdf [accessed: 14.11.2025].

The Polish Economic Institute

The Polish Economic Institute is a public economic think tank dating back to 1928. Its research primarily spans macroeconomics, energy and climate, foreign trade, economic foresight, the digital economy and behavioural economics. The Institute provides reports, analyses and recommendations for key areas of the economy and social life in Poland, taking into account the international situation.

Polish
Economic
Institute