briefs

No. 26|22 (June 2026)

Federica Marconi

Reframing Open Strategic Autonomy in the EU Digital Ecosystem*

- Digital technologies increasingly shape global economic competition and geopolitical power dynamics.
- The EU's heavy dependence on non-EU actors in such critical sectors as tech and digital production and the use of digital infrastructures, products and services, has made the digital field a fundamental component of the EU's pursuit of Open Strategic Autonomy.
- The EU is moving beyond digital regulation alone towards a more strategic mix of domestic capacity-building, economic security tools and trusted partnerships aimed at strengthening resilience and reducing critical vulnerabilities.

The concept of Open Strategic Autonomy (OSA) has progressively become a guiding principle in EU policymaking, with growing emphasis – particularly since the first term of the Commission led by President Ursula von der Leyen – on technological development and digital transformation.

This sharper focus reflects a broader change in the global environment, where technological capabilities play an ever-greater role in determining geoeconomic and geopolitical power dynamics. The growing weaponisation of trade and investment has exposed the EU's deep dependencies, strategic vulnerabilities and structural weaknesses. Thus, the EU has progressively reoriented its policy framework for the digital ecosystem,[1] moving beyond a predominantly regulatory approach towards a prioritisation of security and the strengthening of domestic production in strategically critical areas.[2]

* This brief was produced in the framework of the research project "European strategic autonomy and the challenge of new green and digital technologies" supported by the Fondazione CSF and Fondazione Compagnia di San Paolo within the Geopolitics and Technology call. The views expressed in this report are solely those of the author.

1 Gehrke, Tobias, "Understanding the EU's New Economic Security Playbook", in *ECFR Policy Alerts*, 4 December 2025, https://ecfr.eu/?p=146688.

2 Demertzis, Maria et al., "Strategic Autonomy and European Competitiveness: Security Now Comes First", in *European Parliament Studies*, December 2025, https://www.europarl.europa.eu/thinktank/en/document/ECTI_STU(2025)764371.

Federica Marconi is a Research Fellow in the 'Multilateralism and global governance' programme at IAI.

f.marconi@iai.it

Emerging and persistent challenges

The challenges for the EU are rooted in specific segments of the digital ecosystem, such as: i) tech/digital-related production and its enabling factors, including access to critical raw materials (CRMs) and semiconductors, as well as investment in research and development (R&D); ii) availability and usage of tech/digital infrastructures, products and services; iii) trans-jurisdictional influence stemming from market and regulatory power.

Production and its enabling factors

» The supply and refining of critical raw materials is highly concentrated abroad

CRMs and semiconductors (microchips) are two pillars of the modern digital ecosystem. The supply and refining of CRMs – vital for digital technologies such as ICT and robotics – is highly concentrated abroad,[3] translating into a heavy reliance for the EU and other global players such as the United States.[4] As for the semiconductors, approximately 75 per cent of value added by the industry is generated by just five economies (China, South Korea, Chinese Taipei, Taiwan, United States),[5] with less than 10 per cent of global semiconductor production taking place in Europe,[6] which imports over 90 per cent of advanced chips.[7] Therefore, any disruption to chips production, or policy decisions made by major supplier countries (e.g. export restrictions or changes in pricing), could trigger widespread shortages, impacting a wide range of downstream industries.

In this context, R&D is a critical enabling factor for tech and digital production, as it not only drives innovation and industrial competitiveness, but also helps attracting firms to frontier activities. While the United States has maintained a stable share of global corporate R&D and China's has steadily increased, the EU has experienced a sustained decline since 2012, resulting in an estimated 740 billion euro investment gap by 2024.[8] What strikes the most is that this deficit is concentrated specifically in high-tech, digital and software sectors. Moreover, the EU's R&D landscape is dominated by ageing incumbents: nearly 60 per cent of spending remains concentrated in firms that were already dominant twenty years ago, while firms founded after 1990 contribute only 28 per cent.[9]

3 European Commission DG for Internal Market website: *Critical Raw Materials*, https://single-market-economy.ec.europa.eu/node/279_en.

4 Shivakumar, Sujai et al., "A World of Chips Acts: The Future of U.S.-EU Semiconductor Collaboration", in *CSIS Reports*, August 2024, https://www.csis.org/node/111997.

5 OECD, *Economic Security in a Changing World. New Approaches to Economic Challenges*, Paris, OECD, 2025, https://doi.org/10.1787/4eac89c7-en.

6 van Wieringen, Kjeld, "Global Semiconductor Trends and the Future of EU Chip Capabilities", in *ESPAS Ideas Papers*, 2022, https://www.espas.eu/files/Global-Semiconductor-Trends-and-the-Future-of-EU-Chip-Capabilities-2022.pdf.

7 Ginikyte-Kanclere, Vaida et al., "European Software and Cyber Dependencies", in *European Parliament Studies*, December 2025, https://www.europarl.europa.eu/thinktank/en/document/ECTI_STU(2025)778576.

8 Nindl, Elisabeth et al., *The 2025 EU Industrial R&D Investment Scoreboard*, Luxembourg, Publications Office of the EU, 2025, https://doi.org/10.2760/7802619.

9 Andrea Dugo, "Europe's Innovation Gap: Five Charts and Five Takeaways for an Evidence-Based Debate", in *ECIPE Insights*, February 2026, https://ecipe.org/?p=94915.

Availability and usage of infrastructures, products and services

According to the European Parliament resolution on European technological sovereignty and digital infrastructure (22 January 2026),[10] the EU relies on non-EU countries for over 80 per cent of digital products (including tools and platforms used by EU developers),[11] services, infrastructure and intellectual property. This structural reliance is further amplified by the EU's lag behind global competitors – especially United States and China – in key technological domains.[12] For instance, in artificial intelligence (AI), the EU receives only about 6 per cent of global venture capital funding, while it hosts less than 5 per cent of the global capacity in computing infrastructure,[13] with roughly 80 per cent of EU corporate spending on software and cloud services directed to US vendors.[14]

» EU dependencies are especially strong in critical segments like cloud services, enterprise software, consumer platforms and AI tools

These dependencies are especially strong in critical segments like cloud services (both for private and public users), enterprise software, consumer platforms and AI tools, where European alternatives are limited. Telling examples include US cloud giants (Amazon, Microsoft and Google), which together capture over two-thirds of the European market,[15] and AI chatbots like OpenAI's ChatGPT, which, as of January 2026, was used by over 80 per cent of EU users of AI chatbots.[16] As a result, non-EU vendors and providers are deeply embedded across the technology supply chain, from software ecosystems to connectivity infrastructure, often creating forms of vendor lock-in through proprietary standards and ecosystem control.

Trans-jurisdictional influence

The EU's heavy reliance on non-EU companies for essential components of its digital ecosystem gives rise to the additional risk of jurisdictional dependencies.[17] These should be understood as a consequence of the widespread use of non-European technologies subject to extraterritorial legislation, whereby critical elements of the EU's digital infrastructure become exposed to foreign legal regimes. This, in turn, creates a structural imbalance that undermines the EU's ambitions for digital sovereignty and increases its exposure to systemic risks.

10 European Parliament, *Resolution of 22 January 2026 on European Technological Sovereignty and Digital Infrastructure* (P10_TA(2026)0022), https://www.europarl.europa.eu/doceo/document/TA-10-2026-0022_EN.html.

11 Ginikyte-Kanclere, Vaida et al., "European Software and Cyber Dependencies", cit.

12 Schaeder, Peder, "How the EU Became a Digital Colony — and How It Might Break Free", in *The Parliament Magazine*, 26 January 2026, https://www.theparliamentmagazine.eu/news/article/how-europe-became-a-digital-colony-and-how-it-might-escape.

13 Negele, Maximilian et al., *Europe and the Geopolitics of AGI. The Need for a Preparedness Plan*, Santa Monica, RAND Corporation, 2025, https://doi.org/10.7249/RRA4636-1.

14 Asterès, *Technological Dependence on American Cloud Software: An Estimate of the Economic Consequences for Europe*, April 2025, https://www.calameo.com/cigref/books/0058692358486c4690102.

15 Haeck, Pieter and Mathieu Pollet, "Europe's Dream to Wean Off US Tech Gets Reality Check", in *Politico EU*, 5 June 2025, https://www.politico.eu/?p=6705831.

16 Hongyu, Tangf, "AI Chatbot Market Share 2026: ChatGPT Drops to 68% as Google Gemini Surges to 18.2%", in *Vertu Blog*, 8 January 2026, https://vertu.com/lifestyle/ai-chatbot-market-share-2026-chatgpt-drops-to-68-as-google-gemini-surges-to-18-2.

17 Ginikyte-Kanclere, Vaida et al., "European Software and Cyber Dependencies", cit.

A clear example is the already mentioned dependence on US-based cloud infrastructure, which raises concerns about control over European data. Although the EU-US Data Privacy Framework (2023) allows data to be transferred legally, US laws – such as the CLOUD Act, the Patriot Act, and the Foreign Intelligence Surveillance Act (FISA) Section 702 – can require US companies to grant access to data, regardless of where it is stored.[18] As a result, data held in European data centres by US firms may still be accessed by US authorities, potentially conflicting with EU data protection rules like the GDPR.

EU's digital response along three axes: Protecting, promoting and regulating

To address these challenges, the EU has developed a comprehensive strategy for OSA in the digital domain that can be understood along three main axes: protecting, promoting, and regulating.

Protective tools: Secure critical infrastructures and strategic assets

» The EU has developed a trade and investment toolkit to manage external risks in sensitive sectors and critical technologies

The EU has developed a trade and investment toolkit to manage external risks in sensitive sectors and critical technologies. Key initiatives include advancing discussions on outbound investment oversight, ensuring a stronger EU coordination of export controls under the Regulation (EU) 2021/821 on dual-use items[19] (i.e. sensitive goods, software and technology that can be used for both civilian and military applications), and strengthening the EU framework for the screening of foreign direct investment (FDI). In this regard, Regulation (EU) 2019/452 is currently under revision[20] (expected to be fully applicable by the end of 2026), with the aim to improve harmonisation and extend mandatory screening for FDI targeting areas such as critical infrastructure, dual-use technologies (including AI and quantum), supply chains and sensitive data. In parallel, the 2026 Industrial Accelerator Act identifies new areas relevant for FDI control, including the extraction, processing and recycling of critical raw materials. While traditionally used sparingly due to their protectionist nature, these instruments reflect a more assertive and security-oriented EU approach.

The Anti Coercion Instrument (ACI) is the dedicated legal tool of the EU aimed at shielding the Union and its Member States from political pressure exerted by third countries through economic coercion. Its relevance in the digital domain is particularly significant, as economic coercion increasingly targets digital services, critical technologies and data flows. For instance, the Trump administration has threatened higher tariffs and restrictions on chip exports against the EU in an effort to pressure it into abolishing digital taxes targeting

18 OpenCloud, "US Law in European Data Centres? The CLOUD Act Makes It Possible", in *OpenCloud blog*, 24 July 2025, https://opencloud.eu/en/the-cloud-act-makes-it-possible.

19 European Parliament and Council of the EU, *Regulation (EU) 2021/821 of 20 May 2021 Setting Up a Union Regime for the Control of Exports, Brokering, Technical Assistance, Transit and Transfer of Dual-Use Items*, https://eur-lex.europa.eu/eli/reg/2021/821/oj/eng.

20 European Commission DG for Trade, *Revision of the EU's Foreign Investment Screening Mechanism*, 11 December 2025, https://policy.trade.ec.europa.eu/node/1939_en.

major US tech companies such as Google, Meta and Amazon.[21] Established by Regulation (EU) 2023/2675,[22] the ACI allows the European Commission to assess potentially coercive actions and propose countermeasures, including restrictions on trade, services, public procurement or foreign investment. Primarily conceived as a deterrent, the ACI has not yet been formally activated. However, debate over its potential use has intensified[23] in response to recent geopolitical tensions, such as threatened tariffs and high-profile coercive cases.

Proactive tools: Building domestic capacity

To strengthen domestic capacity for strategic goods and services, the EU is moving toward a more active industrial policy, targeting key choke points where critical external dependencies are most pronounced. The Critical Raw Materials Act (CRM Act) sets targets for domestic extraction (10 per cent of EU demand), processing (40 per cent within the bloc), and recycling (25 per cent), supported by 47 strategic projects in the EU and 13 abroad, with a total estimated investment 22.5 billion euros.[24] In addition to that, the European Chips Act aims to double the EU's global semiconductor manufacturing capacity to 20 per cent by 2030, with a total investment of at least 43 billion euros (including 3.3 billion from the EU budget). Under Pillar I, the Chips Joint Undertaking supports five pilot lines bridging research and industrial production; under Pillar II, the Commission has already approved seven state aid decisions for first-of-a-kind facilities for advanced semiconductor technologies, representing over 31.5 billion euros in combined public and private investment.

» Despite their initial ambitions, both the CRM Act and the European Chips Act have fallen short of expectations

Despite their initial ambitions, both the CRM Act and the European Chips Act have fallen short of expectations, prompting discussions on how to revise them to address gaps and inefficiencies. In December 2025, the European Commission adopted the RESourceEU action plan[25] to accelerate progress toward the CRM Act's objectives and proposed amendments. The Commission has recently revised the Chips Act following a public consultation in 2025 to seek a more competitive and strategically focused approach.[26] The so-called Chips Act 2.0 was released in June 2026,[27] as part of the EU's flagship Tech Sovereignty Package, initially expected in early 2026 but then later several times.[28]

21 Sweney, Mark, "Trump Threatens Tariffs on Countries that 'Discriminate' against US Tech", in *The Guardian*, 26 August 2026, https://www.theguardian.com/p/x33qmj.

22 European Parliament and Council of the EU, *Regulation (EU) 2023/2675 of 22 November 2023 on the Protection of the Union and its Member States from Economic Coercion by Third Countries*, https://data.europa.eu/eli/reg/2023/2675/oj/eng.

23 Corlin, Peggy and Maria Tadeo, "What Is the EU's Anti-Coercion Instrument, and How Does It Work?", in *Euronews*, 18 January 2026, https://www.euronews.com/my-europe/2026/01/18/what-is-the-eus-anti-coercion-instrument-and-how-does-it-work.

24 European Commission, *Commission Selects 47 Strategic Projects to Secure and Diversify Access to Raw Materials in the EU*, 25 March 2025, https://ec.europa.eu/commission/presscorner/detail/en/ip_25_864.

25 European Commission, *Factsheet: RESourceEU Action Plan*, 3 December 2025, https://ec.europa.eu/commission/presscorner/detail/en/fs_25_2888.

26 Semicon Sweden, *Europe's Semicon Future – Industry Recommendations for EU Chips Act 2.0*, 16 November 2025, https://semiconductorsweden.com/?p=5104.

27 European Commission DG for Communications Networks, *Proposal for the Chips Act 2.0*, 3 June 2026, https://digital-strategy.ec.europa.eu/en/node/16825.

28 European Commission, *2026 Commission Work Programme. Europe's Independence*

The package also includes the Cloud and AI Development Act (CADA),[29] which aims to strengthen Europe's high-performance computing and digital infrastructure for AI, with the goal of closing the gap with global leaders – including by reinforcing R&D in the field. CADA defines cloud and AI "sovereignty" and streamlines regulatory requirements for data centres development, focusing on key bottlenecks such as permitting, site selection and access to essential resources, thereby accelerating infrastructure deployment and enabling EU industry to provide sovereign solutions across strategic use cases. Although this initiative could mark a turning point in European technology policy – shifting from a primarily rhetorical focus on digital sovereignty to concrete legislative and operational measures – it faces significant scepticism. Past failures, such as GAIA-X and CloudWatt, and a persistent "sovereignty paradox",[30] in which member states favour bilateral agreements with US hyperscalers over collective European solutions, continue to cast doubt on its potential success.

Regulation as a strategic tool

» *The EU is increasingly using regulation as a strategic tool to shape the global digital order and maintain a technological edge*

The EU is increasingly using regulation as a strategic tool to shape the global digital order and maintain a technological edge.[31] By leveraging the scale of its single market, the EU seeks not only to govern its internal digital space, but also to project its rules externally, influencing firms and third countries. This dynamic – often described as the "Brussels effect" – has already been demonstrated by the global uptake of the General Data Protection Regulation (GDPR), with foreign firms often voluntarily adopting GDPR-compliant rules to maintain market access, and is now being extended to the broader digital ecosystem. This strategic shift is anchored by key legislation: the Artificial Intelligence (AI) Act, the Digital Markets Act (DMA), the Digital Services Act (DSA) and the Data Governance Act (DGA) as complemented by the Data Act.

Main features and goals

These pieces of legislation share several foundational characteristics, most notably a human-centric approach that prioritises the protection of citizens' fundamental rights and democratic values within the digital sphere. Despite the commonalities, each addresses the goal of Open Strategic Autonomy through distinct mechanisms. The AI Act – the first binding regulation on AI at the global level – utilises a risk-based approach: it bans "unacceptable" AI uses and imposes strict requirements on "high-risk" systems.[32] In doing so, it aims to support EU technological sovereignty by ensuring that AI is developed and deployed according to EU ethical and safety standards. The DMA and DSA

Moment (COM/2025/870), 21 October 2025, annex II, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:52025DC0870; Henning, Maximilian, "EU's Tech Sovereignty Package Delayed for Third Time", in Euractiv, 19 May 2026, https://www.euractiv.com/?p=2400828.

29 Digital Watch Observatory, "EU Prepares New Data Strategy for AI Growth", in *Digwatch Updates*, 11 April 2025, https://dig.watch/?p=210203.

30 Simon, Julien, "The EU Cloud and AI Development Act (CADA): A Last Shot at Cloud Sovereignty, or Another Expensive Debacle?", in *Medium*, 3 February 2026, https://julsimon.medium.com/74ccc1a4007c.

31 Csernatoni, Raluca, "Charting the Geopolitics and European Governance of Artificial Intelligence", in *Carnegie Papers*, March 2024, https://carnegieendowment.org/research/2024/03/charting-the-geopolitics-and-european-governance-of-artificial-intelligence.

32 Madiega, Tambiama, "Artificial Intelligence Act", in *EPRS Briefings*, September 2024, https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)698792.

limit the unilateral control that big tech exert over the EU public and commercial spheres.[33] In particular, the DMA introduces ex-ante rules for large platforms (i.e. gatekeepers), imposing a series of "dos and don'ts" to prevent unfair practices and to ensure that digital markets remain contestable and open to EU competitors. The DSA focuses on creating a safer online environment by establishing a clear set of rules across the EU with responsibilities for online intermediaries. In addition, the Digital Fairness Act is currently in the pipeline and is expected to be adopted in 2026,[34] with the aim of modernising digital consumer protection rules to address manipulative online practices. Finally, the DGA and the Data Act contribute to build data sovereignty by treating data as a strategic asset that must remain accessible and governable under EU jurisdiction, thereby reducing the structural liability caused by reliance on foreign providers and extraterritorial laws.

The path toward implementation

» The implementation of EU digital acts is already reshaping the competitive landscape of digital markets

The implementation of these acts is already reshaping the competitive landscape of digital markets. The AI Act entered into force on 1 August 2024, with its first prohibitions on systems posing "unacceptable risk" taking effect in February 2025.[35] Governance rules for general-purpose AI models were applied in August 2025; while full compliance for most high-risk requirements is mandated by August 2026, the EU AI Office is already active in developing codes of practice and supporting national authorities. Simultaneously, the DMA has entered a robust enforcement phase: following the compliance deadline for designated gatekeepers in March 2024, the Commission initiated significant legal actions in 2025, including major fines[36] against Apple and Meta.[37] The DSA has followed a similar trajectory, becoming directly applicable to all intermediaries in February 2024 and leading to proceedings in 2025 against platforms like TikTok and AliExpress to address systemic risks and protect minors, as well as the more recent preliminary findings against META.[38] The DGA has established the necessary institutional structures, such as the European Data Innovation Board, and the Data Act completed its primary implementation grace period in September 2025.

Nevertheless, implementation has generated multiple layers of friction. Legal and compliance tensions have emerged as companies challenge

33 Ginikyte-Kanclere, Vaida et al., "European Software and Cyber Dependencies", cit.

34 European Parliament, *Legislative Train Schedule: Digital Fairness Act*, as of 20 April 2026, https://www.europarl.europa.eu/legislative-train/theme-protecting-our-democracy-upholding-our-values/file-digital-fairness-act.

35 Treude, Matthias and Lea Ossmann-Magiera, "EU Digital Rulebook. A New Phase of Digital Regulation in Europe", in *YPOG Briefings*, 8 January 2026, https://www.ypog.law/en/insight/eu-digital-rulebook.

36 European Parliament DG for Communication, *EU Digital Markets Act and Digital Services Act Explained*, updated 26 June 2025, https://www.europarl.europa.eu/pdfs/news/expert/2021/12/story/20211209STO19124/20211209STO19124_en.pdf.

37 European Commission, *Commission Finds Apple and Meta in Breach of the Digital Markets Act*, 23 April 2025, https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1085.

38 European Commission, *TikTok Commits to Permanently Withdraw TikTok Lite Rewards Programme from the EU to Comply with the Digital Services Act*, 5 August 2024, https://ec.europa.eu/commission/presscorner/detail/en/ip_24_4161; Chapman, Peter, "Lessons from AliExpress' Binding Commitments Under EU's Digital Services Act", in *Tech Policy Press*, 2 July 2025, https://www.techpolicy.press/lessons-from-aliexpress-binding-commitments-under-eus-digital-services-act; European Commission, *Commission Preliminarily Finds Meta in Breach of Digital Services Act for Failing to Prevent Minors under 13 from Using Instagram and Facebook*, 29 April 2026, https://ec.europa.eu/commission/presscorner/detail/en/ip_26_920.

designations, contest fines and face rising costs from overlapping rules. At the institutional level, coordination gaps and uneven enforcement have further complicated implementation across the EU. To manage the resulting complexity, the Commission introduced the 2025 Digital Omnibus package to simplify reporting obligations and better align existing rules. A recent political agreement between the European Parliament and the Council on more innovation-friendly AI rules[39] follows the same logic, aiming to provide clearer governance and reduce duplicative requirements for businesses.

At the same time, geopolitical tensions have intensified. Although formally neutral, these measures impact most strongly large, often non-European tech companies, which are likely to fall under the DMA and DSA. This has translated into political pressure: the Trump administration has criticised the EU's rules, portraying it as discriminatory toward US firms and warning of potential retaliation through tariffs or restrictions on critical technologies such as semiconductors.[40]

So far, the European Commission has maintained that its core acts are not open to negotiation in the context of transatlantic trade discussions. Nevertheless, more recently, it has signalled openness to structured dialogue with the United States on tech rules to strengthen cooperation on digital technologies and markets[41] – a move that could potentially open a back door for the Trump administration into the EU's flagship digital legislation.[42]

Autonomous, but through trusted partnerships

This comprehensive implementation effort was further anchored by the European Declaration on Digital Sovereignty in November 2025, which provides a unified governance roadmap to ensure that these regulations effectively support Europe's OSA through the end of the decade.

The Declaration stresses that the EU remains open to cooperation with trusted international partners, based on shared values and mutual trust. In this context, digital sovereignty is reframed from a political slogan into a concrete policy objective, aimed at creating the conditions for Europe to act autonomously, engage effectively in negotiations, and foster innovation without being constrained by technological, industrial or legal dependencies that are difficult to control. This approach aligns with the EU's broader International Digital Strategy for the European Union (June 2025),[43] which aims to shape global digital rules while strengthening cooperation in key areas, including AI, connectivity (5G/6G), semiconductors, quantum technologies and digital platforms.

» The European Declaration on Digital Sovereignty stresses that the EU remains open to cooperation with trusted international partners, based on shared values and mutual trust

39 European Commission, *EU Agrees to Simplify AI Rules to Boost Innovation and Ban 'Nudification' Apps to Protect Citizens*, 7 May 2026, https://ec.europa.eu/commission/presscorner/detail/en/ip_26_1024.

40 Datta, Anupriya, "US Tells EU to 'Roll Back' Digital Rules against US Tech Companies", in *Euractiv*, 25 November 2025, https://www.euractiv.com/?p=2330365.

41 Henning, Maximilian, "Commission Confirms 'Dialogue' with US after Its Attacks on EU Tech Rules", in *Euractiv*, 1 April 2026, https://www.euractiv.com/?p=2383719.

42 Wälde, Milena, "Fatal Decision': EU Slammed for Caving to US Pressure on Digital Rules", in *Politico EU*, 1 April 2026, https://www.politico.eu/?p=8211398.

43 European Commission, *The EU Sets Out Its International Digital Strategy*, 5 June 2025, https://digital-strategy.ec.europa.eu/en/node/13744.

Conclusions and recommendations

The EU's approach to the digital domain reflects an evolving process of self-awareness that is still unfolding. Through OSA, the EU has progressively developed a comprehensive strategy aimed at reducing vulnerabilities and dependencies, but significant challenges across all layers of the digital ecosystem remain. In this regard, the EU should:

- *Strengthen the EU's industrial and technological base*. Move beyond a predominantly regulatory approach by increasing domestic capacity. At the same time, reinforce trusted partnerships to foster strategic cooperation.
- *Enhance cross-border coherence in economic security instruments*. Ensure their consistency, proportionality and coordination, to protect strategic assets without undermining the openness of the Single Market.
- *Improve coordination across member states*. Address implementation gaps by aligning national initiatives with EU-level objectives, with monitoring and enforcement mechanisms to maximise the impact of EU programmes.
- *Ensure effective enforcement of digital regulations while safeguarding the EU approach from external pressures*. Prioritise compliance with key instruments and clarify how overlapping rules apply to avoid regulatory uncertainty and fragmentation.
- *Simplify the EU's digital regulatory framework*. The rapid and extensive expansion of digital legislation has complicated effective enforcement. The EU should ensure greater alignment across regulatory instruments making them speak to each other. In this regard, the planned EU Digital Fitness Check is a step in the right direction.

IAI Istituto Affari Internazionali

The Istituto Affari Internazionali (IAI) is a private, independent non-profit think tank, founded in 1965 on the initiative of Altiero Spinelli. IAI seeks to promote awareness of international politics and to contribute to the advancement of European integration and multilateral cooperation. Its focus embraces topics of strategic relevance such as European integration, security and defence, international economics and global governance, energy, climate and Italian foreign policy; as well as the dynamics of cooperation and conflict in key geographical regions such as the Mediterranean and Middle East, Asia, Eurasia, Africa and the Americas. IAI publishes an English-language quarterly (*The International Spectator*), an online webzine (*AffarInternazionali*), two book series (*Trends and Perspectives in International Politics* and *IAI Research Studies*) and some papers' series related to IAI research projects (*Documenti IAI*, *IAI Papers*, etc.).

Via dei Montecatini, 17
I-00186 Rome, Italy
T +39 06 6976831
www.iai.it

Latest IAI Briefs

Interim Editor: **Riccardo Alcaro** (r.alcaro@iai.it)
ISSN 3103-4071 | DOI 10.82088/IAIbrief2622