BRIEFING NOTE No. 209

Sovereignty in European international digital policy

April 2026

By Chloe Teevan, Sasha Pearson, Sabine Muscat

Summary

The concept of **sovereignty** is playing an ever more central role in how the European Union (EU) is positioning itself on digital policy - both internally and externally. The key challenge for the EU's international digital policy is translating its expanding body of internal legislation into a coherent external strategy.

While the EU lacks a single definition of digital or technological sovereignty, policymakers increasingly align around two objectives: reducing critical dependencies across the digital technology stack and strengthening European competitiveness. The upcoming EU tech sovereignty package (expected by Summer 2026) aims to forge a shared understanding of sovereignty.

Europe's incomplete single market continues to constrain the global growth of European firms. In response, policy is moving toward proactive industrial measures, including the proposed €48.5 billion European Competitiveness Fund under the MFF 2028-2034. At the same time, there is a strong emphasis on embedding security, trust, and resilience into critical digital infrastructure. This includes mitigating risks from non-trusted vendors through the EU 5G Toolbox, extending such considerations to subsea telecommunications, and investing in sovereign capacity such as the IRIS² satellite constellation.

This shift is also reflected in the 2025 EU International Digital Strategy, which aligns the EU's traditional focus on global digital governance and rights with geoeconomic priorities. It introduces a **Tech Business Offer** designed to enhance the attractiveness of European businesses by highlighting trust, security, and diversified solutions to global partners. Yet future efforts will need to clarify the role of sovereignty in the Offer, expand use cases across the tech stack to include cloud and AI, and provide strategic support and financing for European infrastructure operators to complement Europe's manufacturing prowess.

Introduction

EU member states are increasingly aligned in striving for greater European competitiveness and sovereignty, if not on how to pursue them. EU member states continue to struggle to jointly position themselves in order to achieve these goals. This has been evident in the growing debates over deregulation and strategic procurement. The upcoming EU tech sovereignty package, expected by Summer 2026, may provide the basis for a shared understanding, with a strong focus on resilience and tackling critical dependencies across different digital technology sectors.

A growing number of policymakers support the need to diversify partnerships and strengthen relationships with non-traditional partners in Asia, Africa and Latin America in order to support Europe's resilience. The sovereignty package is also expected to integrate security concerns into procurement decisions, notably for cloud computing. Already in 2025, the publication of the EU International Digital Strategy aimed to centre the EU's global digital engagement on its geostrategic priorities and to secure the buy-in of EU member states. This has resulted in more intensive digital diplomacy and dialogue with global partners, as we explore in the accompanying policy brief.

This briefing note is part of a four-part series on Digital Connectivity in the European Tech Business Offer. The other three parts of the series explore the European industrial connectivity offer, the evolving European toolbox around international digital connectivity and the evolution of Team Nationals and Team Europe in the area of digital connectivity.

These policy briefs draw on a targeted review of publicly available literature and programme documentation, as well as on approximately 40 semi-structured interviews with stakeholders, including those from public institutions, development partners, private companies and civil society. In addition, the authors participated in the D4D Connectivity Working Group in December 2026, which included presentations and comments from many stakeholders.

From EU competitiveness to global action

Several internal EU dynamics are feeding into the EU's international digital cooperation. As pointed out by the Letta Report on completing the Single Market, and echoed in the Draghi Report on European Competitiveness, Europe's position is greatly hampered by the incompleteness of the Digital Single Market and the lack of a Capital Markets Union, which would support the financing and growth of start-ups on European soil. Indeed, the EU's incomplete telecommunications union makes it difficult for European companies to grow and thus to compete globally. For many European SMEs, simply entering other EU markets amounts to 'internationalisation'. Similarly, Europe's lack of deep capital markets reduces the availability of financing for European companies at home, let alone their ability to expand beyond Europe.

European businesses, academia, and think tanks have increasingly called for a proactive industrial policy as key to boost both Europe's competitiveness and to address digital sovereignty concerns. Various initiatives have pushed for a large boost in European spending on digital industrial policy, and for the introduction of "Europe first" or "buy European" rules in public procurement. This has stimulated a vibrant debate both in Brussels and national capitals. France and Germany joined forces to host a Summit on European Digital Sovereignty. Germany and the Netherlands, traditionally close to the United States, have recently become more concerned about dependencies on US big tech and have both included language about digital sovereignty in recent coalition agreements.

Although progress in meeting the ambitions of the Draghi report has been slow, there is an increased focus on how to finance priority areas, including digital infrastructure. This is visible in the EU's new Multiannual Financial Framework (MFF) 2028-2034, in which the Commission proposed the European Competitiveness Fund. This identifies the digital sector as one of four priority sectors, with an overall budget of €48.5 billion. Article 61 is fully dedicated to the issue of 'secure connectivity,' highlighting that secure connectivity starts at home and expands abroad. EU companies that are competitive in the internal market should be better equipped to exploit international market opportunities.

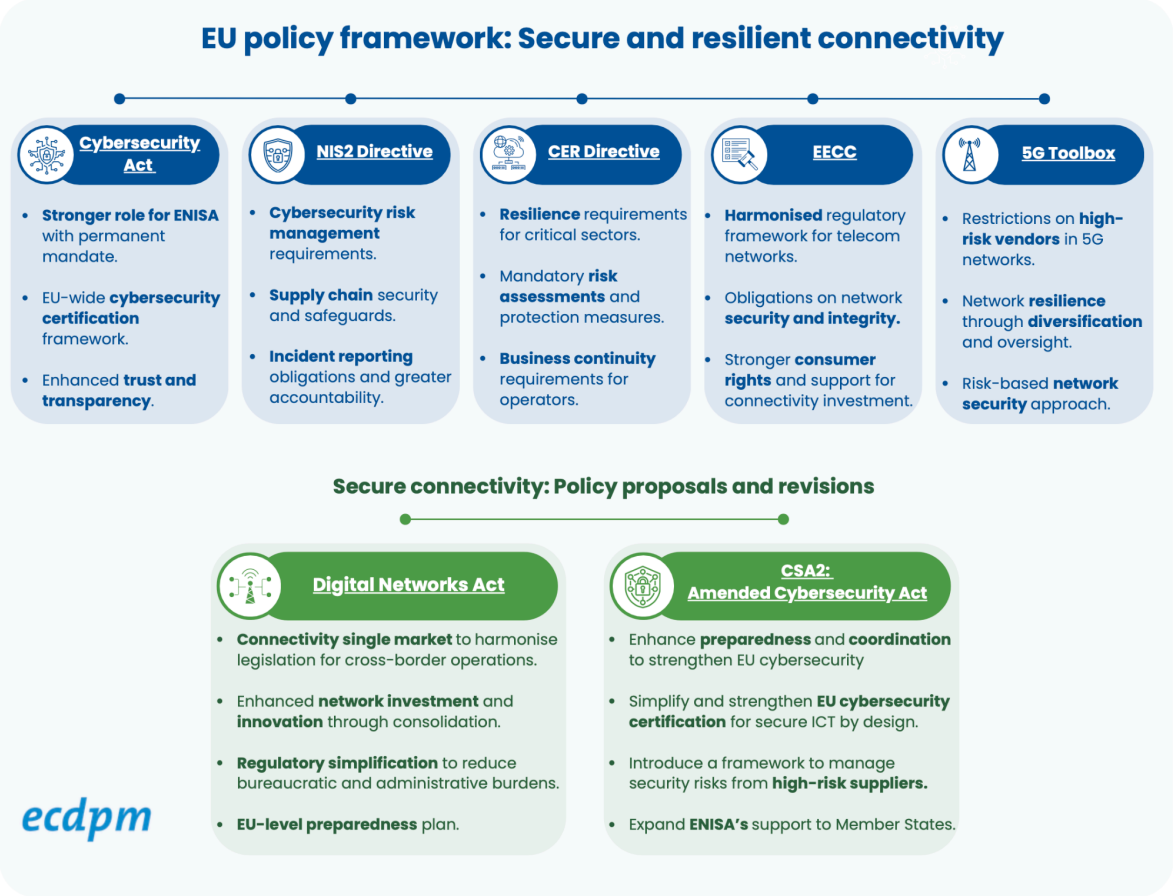
The question of strategic procurement is currently high on the European political agenda, and although there is certainly no consensus, there is a clear push away

from open procurement. Commission President Ursula von der Leyen alluded to the introduction of Made in Europe requirements in her latest State of the EU (SOTEU) - both with regard to internal and international investment, and there have been some moves in this direction with the New Industrial Accelerator Act, although the focus is on clean industries. In the digital domain, it is likely that the upcoming Cloud and AI Development Act, and the other elements of the Tech Sovereignty package due in May 2026, will begin to integrate stricter security considerations into procurement rules. Externally, the procurement and eligibility rules in Article 20 of the proposal for the Global Europe Instrument, inspired by Article 11 of the regulation establishing the Ukraine Facility, place an explicit preference on European providers. This suggests a more strategic approach to public procurement that could serve European economic interests.

Connectivity: Security, trust and resilience

Alongside competitiveness, security considerations are likely to play an ever more important role in European strategic procurement. Noting the growing importance of cybersecurity and physical resilience for communication technologies and critical infrastructure amid geopolitical turbulence, the European Commission's 2024 White Paper on digital infrastructure reinforces the "need to rely on **diversified and trusted suppliers** to prevent **vulnerabilities** and **dependencies.**" This concern is reflected across a constellation of EU policy instruments which, read collectively, point towards an emerging policy orientation: embedding resilience, trusted supply chains, and cybersecurity standards into the foundations of Europe's critical digital infrastructure.

Figure 1: EU policy framework: Secure and resilient connectivity



Source: ECDPM

Cybersecurity concerns have emerged most strongly in the connectivity layer of the tech stack, where protecting digital networks is increasingly linked to the security of the broader digitally connected infrastructure. This emerged most clearly in the context of Europe's 5G infrastructure, where concerns around Chinese suppliers' dominance led to the development of the 2020 EU Toolbox of risk mitigating for the Cybersecurity of 5G networks. Building on findings from the comprehensive EU-coordinated risk assessment,[1] the Toolbox sets out a range of strategic and technical measures, complemented by supporting actions.

Those same security concerns are now being extended across the broader spectrum of digital infrastructure. The 2026 Submarine Cable Security Toolbox applies the same logic of vendor risk mitigation and supply-chain resilience to

[1] Published in 2019, the risk assessment was completed by EU member states with support from the European Commission, European Union Agency for Cybersecurity (ENISA) and the Body of European Regulators for Electronic Communication (BEREC).

strengthen the protection, monitoring, and overall robustness of subsea telecommunications infrastructure. The forthcoming Cloud and AI Development Act is expected to bring cloud infrastructure and computing facilities into the same policy framework, reinforcing the emergence of cloud and data-centre infrastructure as a core component of Europe's digital backbone. A number of actors from industry and the policy community argue that these systems should now be treated as critical digital infrastructure, in line with the EU's broader push to tighten security and resilience requirements.

The EU is now seeking to advance this agenda with the proposed Cybersecurity Act, which would completely exclude certain vendors considered 'high-risk' from European networks. Yet even as Brussels intensifies pressure on 'trusted connectivity', implementation remains uneven: as of 2025, the Commission estimated that only ten Member States had fully implemented the framework. National patterns vary widely, with Germany sourcing 59% of its 5G RAN infrastructure from China, compared with around 30% in Italy, Spain, and Finland; 13% in France; 3% in Sweden; and 0% in the Baltic states, according to Strand Consult. Although Germany established a legal basis to exclude Huawei as early as 2019, implementation was delayed until 2024, when the government opted for a phased removal of equipment from Huawei and ZTE. In late 2025, it took a more forceful stance, with an updated information security law enabling the Interior Ministry to order the removal of insecure 5G components. Chancellor Friedrich Merz also announced that China would be excluded from Germany's 6G network.

Box 1: Unpacking 'Trusted Connectivity'

'Trusted connectivity' emerged as an organising framework among Western democracies in response to growing concerns about the security of global connectivity. Driven by concerns of authoritarian state investments that can 'open potential vectors for coercion, disruption, or attack in times of crisis or conflict,' the framework called on like-minded democracies to cooperate to ensure connectivity infrastructure reflects shared values of openness, freedom, and human dignity.

This was set against the backdrop of China's expanding global digital footprint and concerns about its 2017 Cybersecurity Law and 2021 Data Security Law, which extend state reach over data held by Chinese firms, as well as Huawei's proposals at the ITU for a more centralised internet architecture.

The concept gained formal traction at the September 2021 Tallinn Digital Summit, where participating nations established the Tallinn Consensus on Trusted Connectivity to deepen cooperation among aligned partners. In practice, however, consensus has proved elusive. Adoption across multilateral fora and EU Member States has been uneven, shaped by diverging threat perceptions, varying degrees of supplier dependency, and differing domestic legal frameworks.

Beyond cybersecurity and the management of trusted vendors, EU policy is now explicitly shaping the physical and operational design of Europe's digital backbone. **Route diversification and redundancy**[2] have become central components of the EU's strategy to enhance the security and resilience of subsea cable infrastructure. Identified as priorities in the 2024 Commission Recommendation and the 2025 Action Plan on Cable Security, these principles underpin the Cable Security Toolbox and the framework for Cable Projects of European Interest (CPEIs). In early February 2026, the Submarine Cable Expert Group[3] - established to support the implementation of the EU's cable security agenda - published its second report identifying 13 priority areas for CPEIs, marking a key step toward operationalising the EC's strategy.

Meanwhile, Elon Musk's threats to pull Starlink out of Ukraine in 2022 (a position he has since reversed by denying Starlink access to the Russian military) similarly drew attention to the lack of a European alternative for high-speed and low-latency internet connectivity from space. Starlink is currently the only provider able to offer this at scale with a dense constellation of more than 10,000 satellites. Their position in low Earth orbit (LEO) reduces the transmission time to Earth

[2] Redundancy refers to the provision of alternative cables, routes, and network capacity that allow data traffic to be rerouted in the event of damage, failure, or disruption to a primary subsea cable, thereby ensuring continuity of service.

[3] The expert group is composed of the Commission, Member States and the European Union Agency for Cybersecurity (ENISA).

compared to satellites in medium Earth and geostationary orbit, which cover larger parts of the Earth but from a much greater distance. France's Eutelsat does provide LEO services to telecom operators via One Web and cooperates with SES for multi-orbital constellations, but it does not have the same scale as Starlink. The recognition of the strategic vulnerability of an overreliance on Starlink has added urgency to the project to build a sovereign EU satellite constellation in multiple orbits (combining GEO, MEO, and LEO), IRIS².

The EU is increasingly framing network resilience around the consolidation of sovereign capacity in the public interest, aiming to reduce dependencies and strengthen the continuity of critical connectivity. Initiatives such as the Framework for Cable Projects of European Interest (CPEIs) and IRIS² illustrate this approach at the EU level, while GÉANT-led projects provide a concrete case of its application in cross-border research and education connectivity.

Box 2: Strategic GÉANT initiatives in secure connectivity

As the non-profit operator of Europe's research and education network, GÉANT plays a strategic role in European digital sovereignty. In several Global Gateway projects, GÉANT serves as the primary technical partner for intercontinental research and education connectivity. By securing 'sovereign lanes' in global subsea cable infrastructure, GÉANT facilitates secure knowledge exchanges and large-scale data sharing. This opens avenues for cross-border research collaborations on science and emerging technologies such as AI.

A flagship example is the EU-funded BELLA Programme, through which GÉANT and RedCLARA secured a long-term IRU of 40 optical channels on the EllaLink cable, directly linking European and Latin American research and education networks and supporting the Copernicus Programme. Building on this model, GÉANT, with the support of EIB Global, is expanding sovereign research connectivity corridors through projects such as the Medusa cable under EUMEDplus, integrating North African research networks with Europe, and the Blue-Raman system, developed with UbuntuNet Alliance, which will connect Europe to India via the Middle East, bypassing key chokepoints.

Beyond subsea infrastructure, through AfricaConnect, GÉANT strengthens national and regional research and education networks (NRENs), terrestrial

backbones, and campus connectivity across Africa. Under the AfricaConnect4 phase, GÉANT recently secured an additional €40 million under the Global Gateway Strategy to enhance digital connectivity infrastructure and research capabilities across Sub-Saharan Africa.

The European Commission and selected European governments have thus begun to emphasise trust, security and resilience not only within the EU single market, but also externally. The EU's strategic application of trusted connectivity is central to its international partnerships, particularly through the Global Gateway and the 2025 International Digital Strategy. The Global Gateway initiative, launched in 2021, sought to merge a geostrategic approach with financial resources to promote "secure and trusted connectivity," focusing on infrastructure investment while promoting the adoption of data protection laws, the 5G Toolbox, and the EU's regulatory model. More recently, the EU has also highlighted the importance of diversifying suppliers and routes to support digital resilience and sovereignty.

Sovereignty in International digital policy

In line with shifts in the EU's internal concerns, the narrative about the EU's international digital engagement has evolved to incorporate sovereignty and the pursuit of the EU's own geoeconomic interests. In addition to the EU's traditional focus on digital governance, democracy and sustainable development, European technologies are presented as complementing partners' quest for sovereignty by offering opportunities for diversification and access to trusted, secure and sovereign solutions.

This has been visible in the evolving European policy landscape. In 2021, the Global Gateway communication had already sought to orientate European development cooperation against the backdrop of a more strategic and geopolitical environment. Alongside the launch of the Global Gateway, European digital diplomacy and international cooperation highlighted its 'human-centric' approach to the digital transformation, combining support for human rights, security, sustainability, fair competition and citizens' empowerment in the digital age.

By introducing the Tech Business Offer in the EU's 2025 International Digital Strategy, the EU very clearly elaborates its intention to better represent Europe's geoeconomic interests alongside its normative and regulatory goals, while also highlighting that its digital technologies can support partner countries in achieving their goals: "has the capacity to provide integrated technology solutions to partner countries seeking to uphold their digital sovereignty and to implement a human-centric digital transformation." Member states provided political endorsement through the Council of the European Union in November 2025, endorsing the idea that international partnerships can play a role in advancing Europe's own digital transformation, reinforcing its sovereignty, and strengthening its "own open digital ecosystem."

EU and member state diplomats, officials and private sector actors highlight the importance of tailoring the narrative to different contexts and partnerships.[4] Given the strategic ambiguity that many global partners pursue with regard to the US-China digital technology rivalry, some important global partners like Brazil are hesitant to engage with measures that might appear to target China, including the narrative around 'trusted connectivity.' However, at the same time, several European companies operating in Latin America mentioned that the appeal to sovereign and secure solutions appeared to be strong there. In contrast, a number of interviewees mentioned that in some countries in Africa, the narrative around sovereignty has not always been successful due to suspicions about the intentions of at least some EU member states and their private sector operators.

Conclusion and recommendations

Team Europe is making progress toward realising the International Digital Strategy's mandate to combine secure connectivity under the Global Gateway with a competitive EU tech business offer. This is demonstrated by a developing narrative and approach to tech sovereignty, combined with the more specific push to promote 'trusted connectivity' both at home and abroad. On connectivity, the European Commission and member states are shifting gear to take more decisive actions to exclude non-trusted vendors, supported by EU tools like the proposed Cybersecurity Act, the 5G Toolbox, and the newly introduced Submarine Cable Toolbox. Translating this growing internal cohesion into a consistent

[4] See accompanying brief for more on EU digital diplomacy: Karaki et al. 2026

external message and financing instruments for supporting sovereign solutions and 'trusted vendors' across Europe's connectivity offer remains a challenge.

- **Clarify tech sovereignty ambitions and strategy.** A clearer definition of tech sovereignty in the upcoming EU tech sovereignty package should help to better shape the European narrative at the international level. This should frame sovereignty not only as protection against external threats but also as the ability to operate independently, securely, and continuously under any circumstances. Europe needs to support systems that are redundant by default, with backup capabilities, robust infrastructure, and sovereign data channels operated within trusted European frameworks. This moves sovereignty from a defensive concept to an active capability, ensuring continuity of critical services.
- **Expand tech sovereignty ambitions to more sectors.** Europe can become a real model for secure sovereign infrastructure by developing an offer that integrates cybersecurity across more of the stack and treats the security of digital infrastructure in a more holistic manner. The evolving European framework for tech sovereignty is expected to focus not only on the traditional connectivity sector but also to provide a framework for cloud computing, with the potential to develop similar frameworks for other layers of the tech stack.
- **Acknowledging partners' sovereignty priorities.** Given the strategic ambiguity that many global partners pursue with regard to the US-China digital technology rivalry, a European framework that does not clearly take sides will be of great interest to global partners. While Europe and partners will continue to maintain their own strategic assessments with regard to the US-China rivalry, acknowledging partners' concerns with regard to both global powers is essential to strengthening partnerships. By integrating the pursuit of trusted connectivity within a wider framework on tech sovereignty, the EU can communicate that it is serious about developing sovereign solutions across the tech stack.
- **Addressing the weakness of European digital infrastructure operators.** Although Europe has a strong industrial base in hardware manufacturing, it has weaker financial and regulatory instruments to allow for thriving operators. While this in part depends on the development of the DSM and the CMU, the European Commission and member states should develop a more strategic approach to supporting operators in the face of growing

strategic, competitive and financial pressures.[5] This will require joint action, including measures to combine domestic and EU financing - both within Europe and beyond - as well as specific support to address security threats.

Provide clear policy guidance on procurement under the next MFF. By integrating clear policy framing and definitions in the MFF, the EU can lay the groundwork for a more coherent approach to public procurement and financing digital infrastructure that adheres to European concerns around security and trust - both internally via the European Competitiveness Fund and internationally via the Global Europe instrument. Including such a definition in EU financial regulations would provide clarity and more room for engagement for European financial institutions.

Acknowledgements

The authors would like to thank Alberto Rizzi for peer reviewing. We are also grateful to those who provided us with constructive feedback. In addition, we would like to thank Annette Powell and Joyce Olders for formatting support and Isabell Wutz for communications support. We are also deeply grateful to the many people who consented to be interviewed for this work.

The views expressed in this briefing note are those of the authors and do not necessarily represent those of ECDPM or any other institution. Any errors or omissions remain the responsibility of the authors. For comments and feedback, please contact Chloe Teevan (cte@ecdpm.org), Sasha Pearson (sap@ecdpm.org) and Sabine Muscat (smu@ecdpm.org).

[5] ECDPM recently published work exploring these dynamics in the subsea cable sector (Pearson, 2026).

References

Arha, K. (2021). Trusted connectivity: A framework for a free, open, and connected world. Atlantic Council.

BELLA Programme (n.d.). Building the Europe Link to Latin America: Project Impact and Network Evolution.

BMDV (2025b). Summit for greater digital sovereignty starts in Berlin. Press release 27/2025, November 17 2025.

Bria, F., Timmers, P. and Gernone, F. (2025). EuroStack: A European Alternative for Digital Sovereignty. Bertelsmann Stiftung.

BSI (2025). Act on the Federal Office for Information Security (BSI-Gesetz). Bonn: Federal Office for Information Security.

Christlich Demokratische Union Deutschlands (CDU), Christlich-Soziale Union in Bayern (CSU) and Sozialdemokratische Partei Deutschlands (SPD) (2025). Verantwortung für Deutschland: Koalitionsvertrag 2025–2029.

Clark, S. (2025). EU tech chief sounds alarm over Spain's Huawei contract. Brussels: Politico Europe.

Clark, S. (2026). Brussels plans to force governments to block Huawei from 5G. Brussels: Politico Europe.

Council of the European Union (2025). Council Conclusions on Advancing the International Digital Strategy for the European Union. Brussels: Council of the EU.

Creemers, R., Webster, G. and Triolo, P. (2018). Translation: Cybersecurity Law of the People's Republic of China (effective June 1, 2017). DigiChina (Stanford University).

Creemers, R., Webster, G., Sacks, S., Tai, K., Neville, K. and Rafaelof, E. (2021). Translation: Data Security Law of the People's Republic of China (effective June 1, 2021). DigiChina (Stanford University).

Democraten 66 (D66), Volkspartij voor Vrijheid en Democratie (VVD) and Christen-Democratisch Appèl (CDA) (2026). Aan de slag – Coalitieakkoord 2026–2030.

Draghi, M. (2024). The Future of European Competitiveness. Brussels: European Commission.

Engelking, N. (2025). Chancellor Merz: "Will not allow components from China in 6G network". Hanover: Heise Online.

EuroStack Consortium (2025). Open Letter on the EuroStack Vision for European Digital Agency. Brussels: EuroStack.

European Commission (2019). EU-wide coordinated risk assessment of 5G networks security. Brussels: European Commission.

European Commission (2020). Cybersecurity of 5G networks: EU Toolbox of risk mitigating measures. Brussels: NIS Cooperation Group.

European Commission (2024a). White Paper - How to master Europe's digital infrastructure needs? Brussels: European Commission.

European Commission (2024b). Commission Recommendation (EU) 2024/779 on Secure and Resilient Submarine Cable Infrastructures. Brussels: European Commission.

European Commission (2025a). Proposal for a Regulation on establishing the European Competitiveness Fund (ECF), COM(2025) 555 final. Brussels: European Commission.

European Commission (2025b). The 2028-2034 EU budget for a stronger Europe. Brussels: European Commission.

European Commission (2026a). Industrial Accelerator Act. Brussels: European Commission.

European Commission (2026b). Submarine Cable Security Toolbox and Cable Projects of European Interest. Brussels: European Commission.

European Commission (EC), Directorate-General for Defence Industry and Space (DG DEFIS) (2026). IRIS² secure connectivity.

European Commission and High Representative of the Union for Foreign Affairs and Security Policy (2021). Joint Communication to the European Parliament, the Council, the European Economic and Social Committee, the Committee of the Regions and the European Investment Bank: The Global Gateway. (JOIN(2021) 30 final).

European Commission and High Representative of the Union for Foreign Affairs and Security Policy (2025a). Joint Communication to the European Parliament and the Council: An International Digital Strategy for the European Union (JOIN(2025) 140 final).

European Commission and High Representative of the Union for Foreign Affairs and Security Policy (2025b). Joint Communication to strengthen the security and resilience of submarine cables. Brussels.

Fiore, F. (2026). AfricaConnect receives a €40 million boost from the EU to expand digital infrastructure for research and education in Sub-Saharan Africa. GÉANT.

Fokuhl, J., Heide, D., Neuerer, D. and Scheuer, S. (2025) Infrastruktur: Koalition verschärft Sicherheitsanforderungen an 5G-Netz. Handelsblatt.

GÉANT (2025). Inside Medusa's Submarine Cable Project: A Bridge Between Africa and Europe. Amsterdam: GÉANT Association.

Harris, C. (2026) Should cloud be classed as critical infrastructure? Thales Group.

Jabbour, O. (2026). When data centres become critical infrastructure. World Economic Forum.

Jagtiani, S. (2025). 'Risky Configuration: China's Footprint in Germany's Technology Stack'. German Marshall Fund of the United States.

Letta, E. (2024). Enrico Letta's Report on the Future of the Single Market. Brussels: European Commission.

Murgia, M. and Gross, A. (2020) Inside China's controversial mission to reinvent the internet. Financial Times, 27 March.

Muscat, S. (2024). The EU needs a clear pitch for its human-centric approach to digital transformation. ECDPM Commentary. Maastricht: ECDPM.

Republic of Estonia (2021). The Tallinn Consensus on Trusted Connectivity.

Strand Consult (2025). The Market for 5G RAN in Europe: Share of Chinese and Non-Chinese Vendors. Copenhagen: Strand Consult.

Von der Leyen, U. (2025). State of the Union Address 2025: Europe's Independence Moment. Brussels: European Commission.

This document has been produced with the financial assistance of the European Union. The contents of this document are the sole responsibility of the authors and can under no circumstances be regarded as reflecting the position of the European Union.

This publication benefits from the structural support of ECDPM's institutional partners: The Netherlands, Austria, Belgium, Denmark, Estonia, Finland, Ireland, and Luxembourg.