

ANALYSIS

Jul 2026

AUTONOMY THROUGH PARTNERSHIPS

Charting the EU's global
digital engagement

By

Clotilde Bômont

Senior Policy Analyst, EUISS

Fee-Marie von der Brelie

Policy Officer, Cybersecurity and Technology at the
Independent Diplomat

euiiss
European Union
Institute for
Security Studies



The EUISS is an agency
of the European Union

© European Union Institute for Security Studies, 2026.
The views expressed in this publication are solely those of the author(s)
and do not necessarily reflect the views of the European Union.
CATALOGUE NUMBER QN-01-26-008-EN-N
ISBN 978-92-9462-529-8
DOI 10.2815/4875129
Cover image: EUISS composite based on photography
by NATO, EDA, Envato, Unsplash

SUMMARY

- > Europe's digital autonomy depends not only on strengthening its internal capabilities but also on building trusted international partnerships. As geopolitical competition intensifies, the EU needs a more coherent external digital strategy that complements its pursuit of digital sovereignty.
- > Drawing on 199 EU-led digital initiatives across all major regions and five domains, this Analysis shows that the Union's global engagement now extends well beyond regulation to include infrastructure, research, cybersecurity and security cooperation. Yet the EU's growing digital footprint remains fragmented, highlighting the need for greater prioritisation, coordination and delivery to translate engagement into strategic impact.
- > The EU should develop targeted partnerships to secure access to critical technologies, deepen trusted value chains and strengthen resilient digital infrastructure. By supporting partners' capacity-building, it can also reinforce its diplomatic influence while fostering long-term economic ties. A stronger external posture would ultimately reduce Europe's exposure to coercion in a technological landscape where structural dependencies are increasingly weaponised.

Europe's security and power increasingly depend on its influence in the digital domain, and its ability to develop international cooperation, shape standards and secure trusted infrastructures worldwide. Over the past decade, the EU's digital agenda has focused primarily on internal consolidation: developing European capabilities, deepening the internal market and protecting data. It now needs a stronger external dimension.

The current geopolitical instability has starkly exposed Europe's vulnerability to structural and asymmetric dependencies on external digital actors. This realisation has accelerated European efforts towards greater autonomy and given momentum to the concept of 'digital sovereignty', formally articulated in EU policy

documents for the first time in 2019–2020 under the first von der Leyen Commission¹. Since the late 2010s, European policymakers have increasingly recognised that data security requires greater control over the technologies through which data is generated, stored, transmitted and processed. Enhancing European 'digital sovereignty' thus entails strengthening the Union's industrial and technological base, fostering innovation and R&D, and asserting greater control over data governance. These objectives aim to reinforce the EU's and Member States' capacity to act autonomously and reduce exposure to external coercion. But addressing vulnerabilities also requires engaging with partners beyond Europe's borders, whether to diversify supply chains, consolidate support in international digital governance forums, or mobilise additional resources for regional initiatives². **The EU's digital autonomy therefore depends on its ability to build external partnerships.**

The EU may engage with partners whose strategic priorities and political systems differ from its own. Balancing cooperation with the protection of its interests and values is therefore central to its external digital policy. While the 2025 EU Digital International Strategy³ outlines an ambitious global agenda, it also illustrates the **EU's difficulty in clarifying its strategic ambitions in an increasingly competitive technological landscape.**

Driven by a political push for 'more strategic, coherent and effective EU action in global digital affairs⁴', the EU's digital external engagement has expanded rapidly, spanning multiple regions and policy domains – from regulatory dialogues and cyber cooperation to infrastructure financing, research exchanges and industrial initiatives. Yet this expansion has largely unfolded without a fully articulated strategic framework, reflecting a longstanding focus on the internal dimension of European digital policy⁵. While the breadth of EU external digital action demonstrates strong engagement, the proliferation of initiatives and instruments has weakened strategic oversight, resulting in a fragmented agenda and making the EU's external posture harder to discern. **Greater coherence, prioritisation and coordination are needed** to translate the EU's growing engagement into tangible strategic impact. Addressing this gap requires clear and systematic assessment of

EU digital external action to support **targeted, reliable and high-value partnerships**. While the following sections examine regional dynamics in detail, several cross-cutting patterns can already be identified, reflecting the growing strategic and security reframing of the EU's digital policy.

A STRATEGIC AND SECURITY RECALIBRATION

Over the past decade, EU digital external action has shifted **from a technical and largely siloed domain to a core instrument of the Union's foreign policy**⁶. This reflects intensifying geopolitical competition, technological fragmentation and heightened cybersecurity risks, alongside recognition that digital power is now inseparable from economic security, societal resilience and global influence.

In practice, this has led to **a more integrated approach to digital issues**, as digital trade, data flows, cybersecurity and regulatory cooperation are now systematically embedded in free trade agreements, dialogues and regional or bilateral strategies – from the Mediterranean to the Arctic – rather than addressed through stand-alone initiatives. Initially centred on like-minded countries, EU digital external action has also expanded to more diverse partners, through a growing portfolio of longer-term and more structured initiatives, including umbrella frameworks such as the EU-LAC Digital Alliance, the Digital for Development (D4D) Hub, and Global Gateway digital packages, which bundle governance, infrastructure financing and capacity-building.

The EU remains a regulatory power in the digital domain. The export of standards on data protection, artificial intelligence (AI), cybersecurity and digital trade – often framed as the 'Brussels effect' – continues to anchor its global influence, particularly with partners seeking access to the EU market. But regulation is no longer the sole pillar of EU digital engagement. Infrastructure, skills, innovation ecosystems and security cooperation (notably cyber resilience, cybercrime prevention and law-enforcement cooperation) increasingly complement the normative agenda, reflecting recognition that rules alone do not ensure

security and power in a context of technological rivalry. Institutional coordination has also strengthened, notably through 'Team Europe' initiatives, which have helped align the work of the Commission, the High Representative and Member States. Similarly, convergence between the Council and the Commission on the International Digital Strategy reflects more mature strategic framing. **EU digital engagement is thus moving from fragmented *ad hoc* initiatives towards a more comprehensive and structured geopolitical posture.**

Yet this strategic expansion is accompanied by **persistent implementation gaps**. The rapid extension of digital engagement to new regions – such as the Arctic or Central Asia – and capital-intensive sectors like infrastructure development has exposed capacity constraints, with ambition often outpacing execution. These limitations mirror domestic shortcomings, as slow progress in broadband rollout, AI adoption and cloud uptake undermine the EU's external credibility⁷. **Internal fragmentation and technological dependencies continue to weaken the EU's external digital posture.** The single digital market remains incomplete in key areas, while diverging national priorities hinder unified strategic projection and effective resource pooling. At the same time, reliance on foreign technologies, platforms and infrastructure constrains EU leverage in external negotiations and complicates efforts to advance strategic autonomy.

Overall, the EU's digital external action reflects a clear strategic and security recalibration, but remains constrained by gaps in delivery, alignment and strategic prioritisation. Addressing these limitations requires moving beyond expansion towards consolidation, through targeted strategic shifts prioritising impact, coherence and long-term positioning.

Five strategic shifts

 Implications	 Strategic rationale	 Regional illustration
 From normative power to market power		
Complement EU regulatory influence with a competitive external offer combining investment, industrial partnerships and technological deployment.	Regulatory alignment alone does not secure influence if it is not backed by capital, infrastructure and firms . Partnerships can also facilitate market access and enable European companies to scale internationally.	The EU Tech Business Offer, already launched with Kenya and through the Pact for the Mediterranean, strengthens European market presence by combining standards, financing, business support and deployable digital infrastructure, including projects such as the MEDUSA and Blue-Raman cables.
 From internal fragmentation to integration		
Align EU institutions, Member States and policy instruments across trade, development, industrial and diplomatic action.	Internal fragmentation reduces strategic clarity , weakens external credibility and complicates engagement for partners.	The absence of a coherent EU Arctic digital policy has resulted in fragmented national approaches to subsea cable and connectivity projects, limiting collective coordination. The upcoming EU Arctic strategy will provide a more integrated framework to strengthen EU alignment and its role in shaping resilient Arctic data routes.
 From profusion to clarity and prioritisation		
Simplify EU external digital architecture, clarify political ownership and decision-making, offer partners readable entry points, and define visible and high-impact priorities .	A high volume of initiatives can signal engagement but also dilute impact and obscure strategic intent .	In Latin America and the Caribbean, a high number of EU digital initiatives has resulted in a dense but diffuse footprint. The EU-LAC Digital Alliance was established to consolidate previously fragmented bilateral cooperation into a coherent bi-regional framework across connectivity, governance, innovation and skills.
 From dialogue to delivery		
Shift from frameworks and policy dialogues towards implementation, financing and measurable outcomes on the ground.	EU credibility increasingly depends on execution capacity, speed and tangible results rather than institutional density.	Armenia's association to Horizon Europe in October 2025 illustrates growing partner demand for access to EU programmes (DIHs, AI factories, Horizon Europe) and their funding, infrastructure and innovation ecosystems.
 From 'defensive' sovereignty to 'active' autonomy		
Build digital sovereignty through selective and long-term partnerships that expand European capabilities, reduce strategic dependencies and anchor the EU more deeply in global digital value chains.	Strategic autonomy is reinforced not only internally but also through partnerships in order to diversify dependencies, embed the EU in trusted value chains and gain political support and leverage .	Digital partnerships with Japan and South Korea focus on critical technologies such as semiconductors, 6G, HPC and AI, strengthening EU supply-chain resilience and capabilities in critical technology bottlenecks.

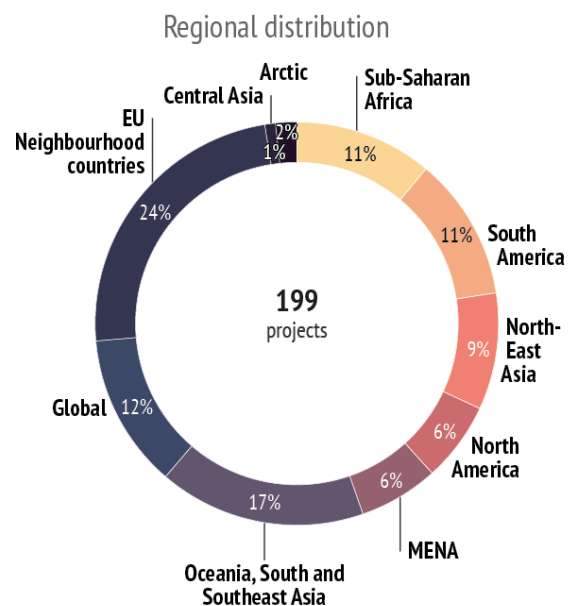
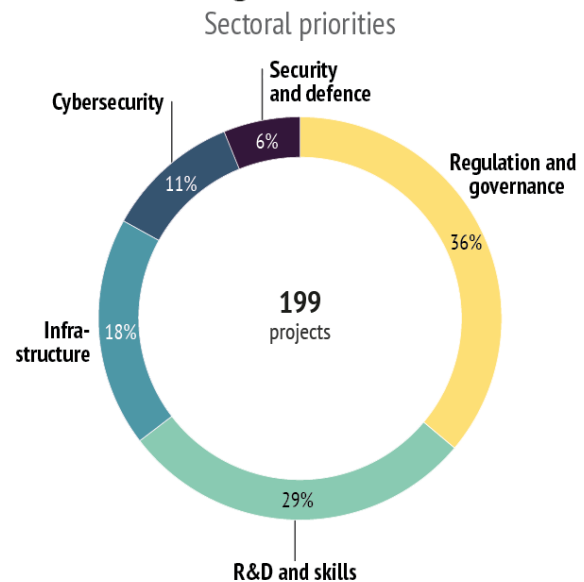
MAPPING THE EU'S GLOBAL DIGITAL ENGAGEMENT

To guide these strategic shifts, the following section assesses EU external digital engagement across regions and sectors. Through focused regional analyses, it identifies the EU's comparative strengths as well as areas of weaker or more fragmented involvement, providing a basis for a coherent global digital strategy.

The analysis draws on 199 EU-led, EU-funded or EU-coordinated digital initiatives – ranging from projects and programmes to agreements, partnerships and dialogues – covering ongoing activities up to May 2026. These initiatives span all major regions: the EU's northern and eastern neighbourhood, Oceania and South and Southeast Asia, Latin America and the Caribbean, sub-Saharan Africa, Northeast Asia, North America, the Middle East and North Africa, the Arctic and Central Asia (in descending order of activity), alongside global-level engagement. They are examined across five domains:

1. **Regulation and governance.** Legal and regulatory frameworks, standardisation dialogues, digital trade provisions, data governance, institutional capacity-building.
2. **R&D and skills.** Research cooperation, innovation ecosystems development, education and training, talent mobility.
3. **Infrastructure, connectivity and equipment.** Digital backbone and service infrastructure, including terrestrial and submarine fibre, broadband networks, satellite systems, data centres, cloud and edge infrastructure, telecommunications equipment, end-user devices.
4. **Cybersecurity.** Cyber resilience, preparedness and incident response, cybercrime prevention and investigation.
5. **Security and defence.** Defence-related digital cooperation, dual-use and military digital capabilities and technologies, cyber defence.

The EU's digital external action



Initiatives can span multiple domains and regions; categories are not mutually exclusive.

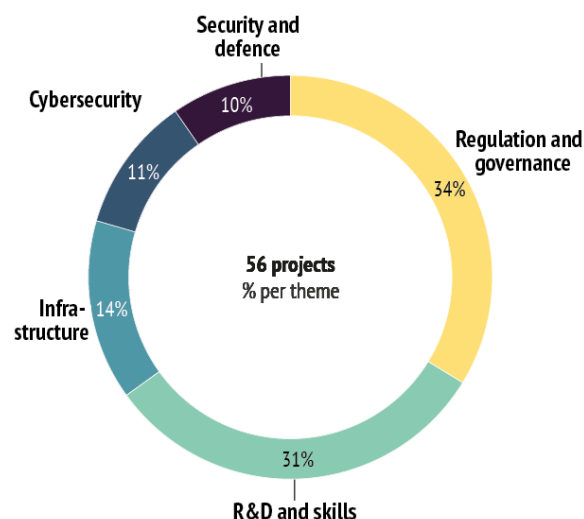
The northern and eastern neighbourhood: An integration-driven engagement

The northern and eastern neighbourhood is the most intensively engaged region in the EU's digital portfolio, reflecting its geographical proximity and political salience. It spans all sectors, combining market integration, security and resilience-building⁸, and ecosystem expansion.

EU action seeks to integrate neighbouring countries into the Union's digital regulatory and market frameworks. Eastern Partnership (EaP) countries – particularly Ukraine, Moldova and Georgia – are the core focus, notably through flagship programmes such as EU4Digital, launched in 2019. These initiatives harmonise telecommunications rules, digital trust services and cross-border e-services, reduce roaming costs, expand broadband and support innovation ecosystems. They also promote eHealth, eTrade and digital skills building, extending the Digital Single Market eastwards. In the Western Balkans, regulatory dialogues and programmes such as Wi-Fi4WB support national alignment with EU legislation and accelerate broadband and digital identity deployment, notably under the EU Growth Plan, which boosts pre-accession funding to advance integration into the EU single market.

The EU's digital engagement in the region is increasingly shaped by security and resilience considerations, in response to Russia's hybrid and cyber threats. The EU-Ukraine Cyber Dialogue and the authorisation to use the EU Cybersecurity Reserve for Moldova underscore a growing emphasis on collective cybersecurity and solidarity. These efforts focus on protecting critical infrastructure, countering disinformation and aligning partners' frameworks with EU standards such as the 5G Cybersecurity Toolbox and the NIS2 Directive.

The EU is also extending its digital infrastructure and innovation ecosystem into the neighbourhood. Projects such as the Black Sea Digital Connectivity Submarine Cable strengthen resilient links between Ukraine and EU networks, while the Western Balkans Investment Framework (WBIF) supports broadband and smart infrastructure deployment. At the same time, Digital Innovation Hubs (DIHs) and AI

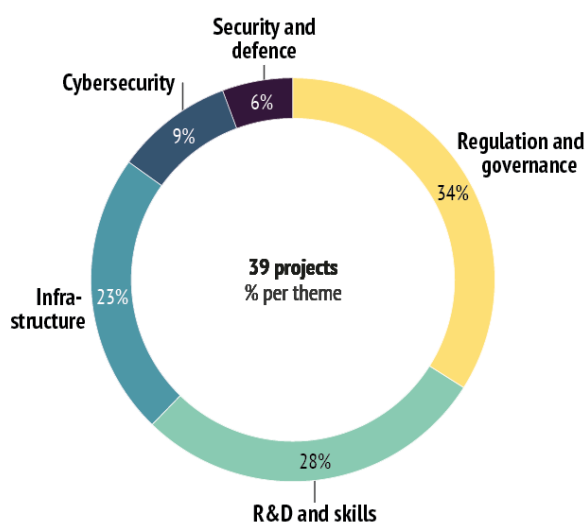


Factory antennas – 43 across neighbouring countries – embed partners within Europe's research, industrial and talent networks. This dense footprint positions the neighbourhood not merely as a partner region but increasingly as an extension of Europe's digital value chains.

Therefore, EU digital engagement in the neighbourhood aims not only to reduce digital divides but to embed EU standards, institutions and capabilities across a strategically critical region. Its effectiveness will depend on combining regulatory alignment, development support and security cooperation while adapting to partners' capacities and geopolitical pressures.

Oceania, South and Southeast Asia: Advancing connectivity, multilateralism and sustainability

Oceania, South and Southeast Asia comprise countries with highly diverse political systems, levels of digitalisation, technological capabilities and degrees of geopolitical alignment with Europe – from technological hubs like Singapore, to large developing digital markets such as Indonesia and advanced innovation-driven economies like Australia. This diversity and the region's central role in global trade and technological competition explain the EU's strong engagement. It seeks to position itself as a comprehensive partner, supporting trusted connectivity, advancing R&D&I on emerging technologies, and promoting governance frameworks.



The significant share of infrastructure and equipment-related projects reflects a priority to enhance secure connectivity and reduce reliance on single-vendor solutions in a region where backbone infrastructure is largely supplied by Chinese companies. Through investments in subsea cables⁹, satellite systems¹⁰ and telecommunications networks¹¹, the EU aims to strengthen resilient links across dispersed Pacific territories and expand local digital capabilities.

Regional actors and the EU also converge on maintaining multilateralism amid geopolitical tensions, addressing climate change and mitigating the weaponisation of trade and technological dependencies. This is visible in discussions on governance frameworks – particularly on AI safety – although concrete regulatory cooperation remains limited, largely confined to like-minded partners such as Australia or embedded in global initiatives¹². In parallel, a strong footprint in education and research demonstrates an investment in scientific diplomacy, with several infrastructure projects specifically targeting R&D networks and academic exchanges.

The comparatively modest number of cybersecurity and defence-related initiatives nonetheless highlights structural constraints. The regional security architecture is shaped primarily by US-led partnerships such as the Quad and AUKUS, which increasingly link defence cooperation with industrial interests, notably in semiconductors and advanced technologies. The region is the frontline of US-China technological rivalry. While this could strengthen cooperation with the EU to counterbalance the two tech powers' influence, security and industrial

commitments remain anchored in US-centred coalitions where the EU plays a complementary role only¹³.

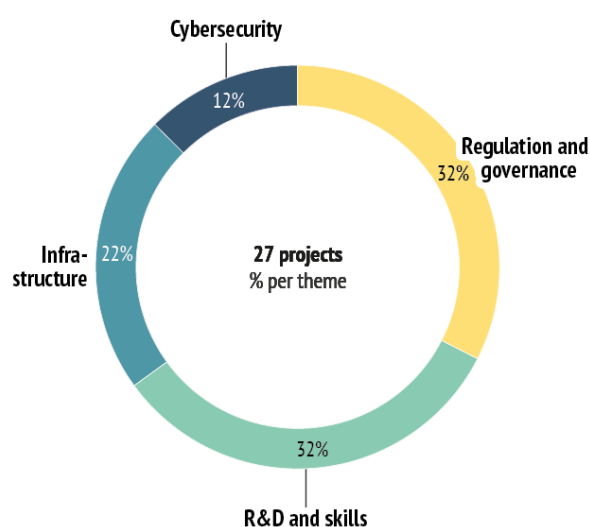
To reinforce economic security and supply-chain resilience, the EU is thus deepening industrial ties through trade agreements with Singapore, Indonesia, New Zealand and India, ongoing FTA negotiations with Thailand, Philippines and Malaysia, and cooperation under the EU-India Trade and Technology Council (TTC) on semiconductors, HPC and 6G. These initiatives also connect to EU green-digital priorities, including renewable-digital integration, energy-efficient data centres and climate monitoring technologies.

Yet local partners sometimes perceive European engagement as fragmented and difficult to navigate. Without greater strategic clarity, prioritisation and visibility, the EU risks weakening its credibility as a long-term strategic partner.

Latin America and the Caribbean: Dense engagement, normative leadership, limited economic footprint

Latin America and the Caribbean (LAC) ranks among the regions where the EU is most active in quantitative terms. The volume of initiatives, however, conceals an uneven engagement, weighted towards regulation and governance, and skills and R&D. The EU's digital action in LAC is therefore primarily normative and ecosystem-oriented.

Politically, the EU-LAC Digital Alliance constitutes the flagship framework of EU



engagement, designed to consolidate fragmented projects into a coherent bi-regional partnership on connectivity, governance, innovation and skills. This reflects the EU's ambition to act as a standard-setter in a region marked by relatively close alignment on data protection, digital rights and multilateralism, with several countries drawing on GDPR-inspired models – albeit with national variations.

In infrastructure, while EU investments remain modest compared to China or the United States, space-based and satellite connectivity stands out as a structured area of cooperation. Projects such as BELLA (and the EllaLink cable), CopernicusLAC, and satellite agreements¹⁴ embed LAC partners into European digital and space ecosystems, delivering operational services (connectivity, earth observation, disaster management) and durable institutional ties.

The prominence of education and skills initiatives is also strategic. Beyond academic exchange, EU programmes aim to support innovation ecosystems, connect universities with startups and SMEs, develop AI, data and cyber talent, and integrate LAC actors into European research networks¹⁵. In a region where the EU's industrial footprint is limited, investment in human capital and ecosystem-building provide the foundations for long-term partnerships.

Finally, the absence of defence-oriented cooperation reflects both regional preferences and the EU's civilian-oriented approach. Engagement centres on cybercrime and cybersecurity capacity-building initiatives such as LAC4 and bi-regional dialogues.

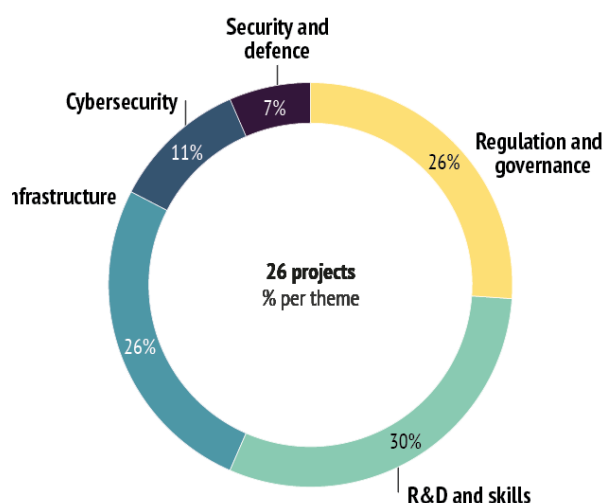
Overall, EU digital engagement in LAC is dense but diffuse: politically ambitious, institutionally rich, yet financially constrained. Converting volume into influence will require tighter prioritisation around high-impact domains, such as connectivity, cybersecurity, and trusted data governance and digital public goods, where European standards and capabilities are in demand. Regulatory cooperation also needs to be more systematically paired with concrete financing, including Global Gateway projects, to embed these standards in deployed networks, platforms, and services. Incentivising the uptake of EU-compatible norms could in return offer investment predictability and clearer access to both regional markets, strengthening the durability of the partnership.

Sub-Saharan Africa: A capacity-building and governance-driven approach

EU digital engagement in sub-Saharan Africa is driven by a dual imperative: narrowing the digital divide¹⁶ and positioning Europe as a credible partner. Africa's digital economy is among the most dynamic globally, yet its digital transformation is unfolding amid acute connectivity gaps, uneven infrastructure deployment, rapid mobile expansion, growing demand for data centres¹⁷, and rising exposure to cybercrime and disinformation.

This transformation is also taking place in a context of intensifying geopolitical competition. China remains a central infrastructure provider in the region, supplying telecom equipment (especially mobile connectivity and 5G), terrestrial and submarine cables (including PEACE, 2Africa and SAIL), cloud services and bundled financing under the Digital Silk Road. The United States engages more selectively, leveraging private-sector dominance, expanding data-centre investments and competing in satellite connectivity. Gulf countries are also emerging as rising actors in the region, increasing investments in digital infrastructure and services. African governments, meanwhile, seek to diversify their partnerships, strengthen digital sovereignty and support industrial upgrading, while advancing continental frameworks through the African Union's Digital Transformation Strategy and the African Continental Free Trade Area (AfCFTA).

Against this backdrop, the EU has positioned itself as a partner in regulatory cooperation and capacity building. Its engagement combines



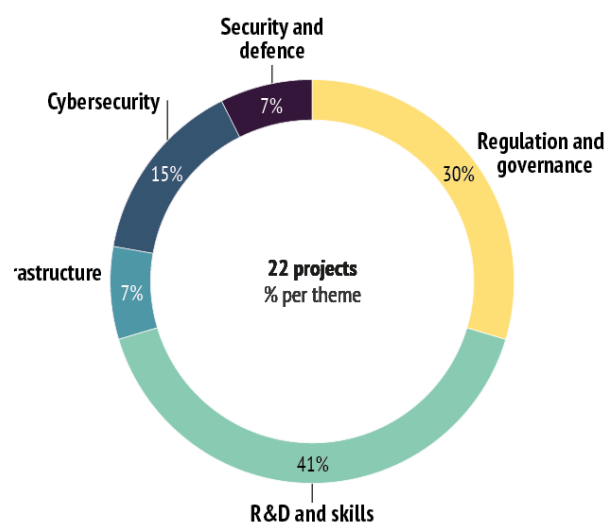
investments in digital infrastructure – including the deployment of fibre-optic networks¹⁸, the extension of the Blue Raman and Medusa submarine cables, and data-centre projects¹⁹ – with institutional cooperation²⁰, especially on data protection and regulatory harmonisation. In parallel, emphasis on research, AI cooperation and knowledge platforms signals a strategy centred on long-term normative influence, standard-setting and technical community-building rather than rapid market capture. Security engagement focuses on resilience, cybercrime prevention and justice cooperation, reflecting competence constraints and political sensitivities, while favouring a development-oriented approach to digital cooperation.

The EU's leverage in sub-Saharan Africa therefore lies not in matching the scale of Chinese financing or US corporate reach, but in delivering an integrated offer combining connectivity, governance and skills in support of African digital sovereignty. To consolidate this position, the EU should treat digitalisation as a cross-sector enabler – supporting public administration, industry, finance, health, etc. – while deepening cooperation with the African Union on emerging priorities such as AI ²¹. At the same time, engagement in the region advances European interests in resilient supply chains, open digital norms and access to a fast-growing market, particularly in satellite connectivity and data infrastructure. The priority now is strategic consolidation, turning multiple initiatives into a coherent, visible and geopolitically credible partnership.

Northeast Asia: Curated and high-end partnerships

Northeast Asia ranks mid-range in the EU's global digital engagement in terms of the number of initiatives, but this understates the strategic importance of EU action in the region. Engagement is concentrated on a limited set of technologically advanced partners and high-end domains, focusing on co-shaping standards and supply chains.

This selective approach should be understood in the context of China's central role in regional digital geopolitics as, although no formal EU-China digital cooperation framework exists, it remains the structuring variable shaping EU



choices. Beijing's weight across manufacturing, platforms, AI deployment and digital infrastructure makes full decoupling unrealistic, yet incentivises the EU to reduce critical dependencies. The postponement of the 2026 EU-China Digital Dialogue confirms that engagement with Beijing remains necessary but fragile, and centred on risk management rather than alignment.

In contrast, cooperation with Japan and South Korea is explicitly strategic and trust-based. The numerous initiatives in education, skills and research reflect deep integration of digital, industrial and security objectives. Collaboration on 6G, semiconductors, HPC, quantum technologies and AI governance²² positions the EU within a trusted circle of advanced democracies shaping innovation and next-generation standards. The limited infrastructure footprint is not a gap but a marker of maturity: cooperation targets architectures and supply-chain resilience rather than connectivity rollout.

Taiwan occupies a distinct and sensitive position. The anticipated 2026 EU-Taiwan Digital Economy Dialogue²³ reflects growing recognition of Taiwan's strategic importance in semiconductors, advanced manufacturing and digital trade. While framed as technical and economic, such cooperation is inherently geopolitical, as Taiwan is a critical node in EU efforts to secure trusted digital value chains across Northeast Asia and the wider Indo-Pacific region.

The limited but notable presence of security-related initiatives with Japan and the Republic of Korea (especially through Security and Defence Partnerships) also points to a gradual evolution of

the EU's posture. In a region defined by US–China competition and heightened cyber risks, the EU acts as a selective security partner, strengthening resilience and coordination with trusted actors.

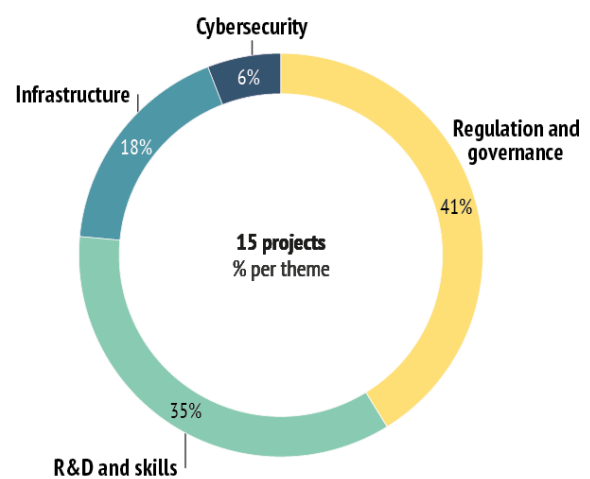
EU digital engagement in Northeast Asia therefore represents strategic positioning under constraint: deepening partnerships with Japan and the Republic of Korea (ROK), informally engaging Taiwan, and managing a competitive relationship with China. Fewer initiatives do not imply weaker engagement; they reflect a deliberate focus on technological sovereignty, alliance building and long-term influence in a region central to global technological power.

North America: Institutionalised cooperation under structural asymmetry and regulatory tension

EU cooperation with North American partners is structured through high-level institutional frameworks, notably the EU-US Trade and Technology Council (TTC), the EU-US Cyber Dialogue, and the EU-Canada Digital Partnership. Since the mid-2010s, these mechanisms anchor transatlantic digital engagement, translating shared democratic principles into coordination on standards, data governance, supply chains and emerging technologies, while managing persistent regulatory divergence.

A defining feature of this relationship is the structural dominance of US private technology firms in the global digital ecosystem. American platforms and cloud services are deeply embedded in EU economies. This market reality underpins much of the regulatory friction. The EU's Digital Services and Digital Markets Acts, in particular, have triggered sustained pushback in Washington, and recent political signals – including visa bans on EU policymakers and threats of trade retaliation – illustrate how digital governance has become a flashpoint in wider transatlantic tensions²⁴. The standstill in the EU-US Cyber Dialogue and TTC since the start of Donald Trump's second term in office underscores the broader deterioration in transatlantic cooperation.

Despite these strains, cooperation endures where interests converge. Joint initiatives on semiconductor supply-chain resilience, research projects such as MIRAQLS and HYPERSPACE, and



common guidance on protecting human rights defenders online demonstrate continued alignment on innovation, values and systemic risk management. Cybersecurity cooperation continues, for instance through the ENISA–CISA working arrangement which focuses on infrastructure resilience, incident response and information-sharing.

Infrastructure cooperation in strategic spaces further signals shared priorities. Projects linked to Arctic and polar connectivity²⁵, for instance, highlight mutual concern over the resilience of data routes amid geopolitical competition, climate change and the weaponisation of critical infrastructure.

Overall, EU digital engagement with North American partners combines institutionalised governance dialogue with targeted operational initiatives, even as regulatory disputes and political tensions complicate alignment. The central challenge is to manage structural asymmetries while preserving interoperability between the two regions. Refocusing dialogue on shared threats – such as online terrorism, large-scale fraud and child sexual abuse material – could help depoliticise regulatory tensions and rebuild practical cooperation. In parallel, sustaining research, innovation and mobility programmes under Horizon Europe is essential to anchor long-term ties with US and Canadian ecosystems despite periodic episodes of political friction.

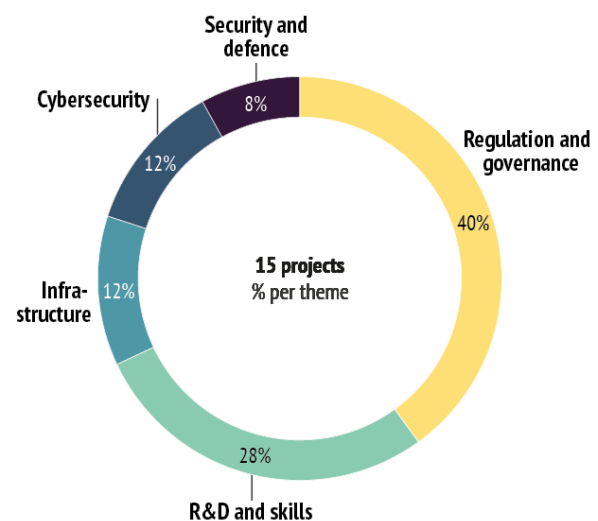
Middle East and North Africa: A security- and stability-focused digital engagement

The EU's modest footprint in the Middle East and North Africa (MENA) reflects a cautious posture in a highly dynamic yet deeply fragmented region, torn between authoritarian consolidation and reform efforts, and marked by intense intra-regional competition and rivalry. The predominance of cybersecurity and legal initiatives highlights the EU's priority to stabilise digital domains with immediate cross-border security implications, focusing on incident response and cooperation against cybercrime, while limiting exposure to politically sensitive infrastructure projects (data centres, 5G/6G projects, etc). The MEDUSA submarine cable linking North Africa and Europe, and the Blue Raman cable connecting India, Southeast Africa (via Djibouti) and Europe remain notable exceptions.

This stance is shaped by three interacting drivers. First, state control over information and digital infrastructure remains tight across the region, particularly in the Middle East, where Iran, Saudi Arabia, the United Arab Emirates (UAE), Egypt, Bahrain and Turkey rank among the countries with the lowest levels of internet freedom²⁶. Network shutdowns, surveillance and content restrictions²⁷ run counter to EU values on democracy and privacy, narrowing the scope for cooperation, particularly on projects involving civil society.

Second, competing external and regional actors – most prominently China through the Digital Silk Road and the Gulf states through large-scale investments in cloud services and data centres – have oriented the region toward infrastructure-intensive deals that European actors have not pursued with comparable intensity. Saudi Arabia and the UAE, in particular, are positioning themselves as regional AI hubs, while simultaneously investing in the US AI ecosystem²⁸ and maintaining access to Chinese technologies, leaving limited strategic space for the EU in this triangle.

Third, a security environment dominated by migration, counterterrorism and protracted conflicts in Yemen, Syria and the Palestinian territories highlights the relevance of law-



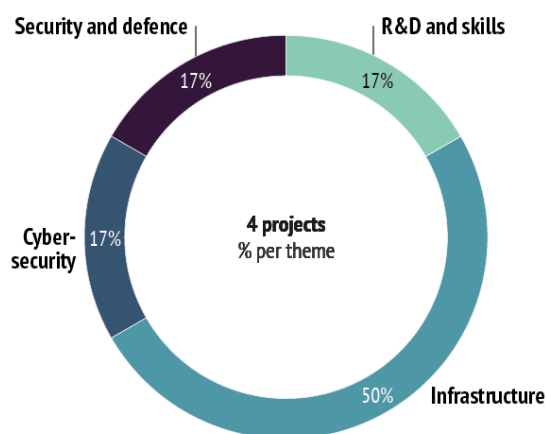
enforcement cooperation. Several EU initiatives focus exclusively on cyber and organised crime, with long-standing programmes such as EUROMED Police, which was launched in 2004 and is now in its sixth iteration.

The EU's digital engagement thus remains largely shaped by broader security and stability priorities. Its influence over MENA's digital backbone is limited, and support for digital transformation has yet to match the scale of regional change. To gain geopolitical traction and secure strategic partnerships, the EU needs to scale up investment in infrastructure and R&D under the Global Gateway and through the Tech Business Offer²⁹ – included in the Pact for the Mediterranean – and strengthen diplomatic engagement with key regional actors.

The Arctic: Securing strategic data routes

The Arctic occupies a paradoxical place in EU digital external action: it accounts for only four – mainly infrastructure-focused – initiatives yet carries considerable strategic weight amid intensifying geopolitical competition and growing vulnerabilities in global connectivity. This number reflects the region's narrow institutional landscape, sparse population, extreme operating conditions, and the inherently capital-intensive and long-term nature of Arctic digital infrastructure deployment.

The EU's focus on subsea and terrestrial fibre connectivity through projects such as Polar Connect, Far North Fiber Europe and Tusass Connect responds to a clear strategic rationale. Arctic data routes offer shorter, lower-latency



and potentially more resilient links between Europe, North America and Asia as conventional routes face mounting risks. Disruptions around southern maritime chokepoints and congestion in existing cable corridors (notably in the Red Sea) have exposed the fragility of current global data flows. Arctic connectivity therefore serves not only regional development, but also European priorities of economic security, strategic autonomy and network resilience.

As accelerating ice melt is opening new maritime routes and access to natural resources, the Arctic has become the theatre of geopolitical competition in the Northern hemisphere. This is driving major investments in critical infrastructure – by the EU, but also by Russia, China and the United States. Russia's military posture and digitalisation of the High North³⁰, China's 'Polar Silk Road' ambitions³¹, and intensified US-NATO efforts to secure subsea infrastructure – especially following sabotage incidents in the Baltic Sea and High North³² – have all raised the strategic value of Arctic data corridors. In this context, EU-backed connectivity projects perform an implicit de-risking and diversification function, even when framed in civilian or commercial terms. The absence of EU initiatives on cybersecurity or defence is consistent with regional realities, as security dynamics are managed primarily through NATO or bilateral defence arrangements.

Yet, while the EU's International Digital Strategy identifies Arctic connectivity as a priority, the EU's regional policies have not kept pace with these developments. Although revisions are underway, the EU's Arctic Policy has not been updated since 2021, and in the absence of a common strategic framework, Member States

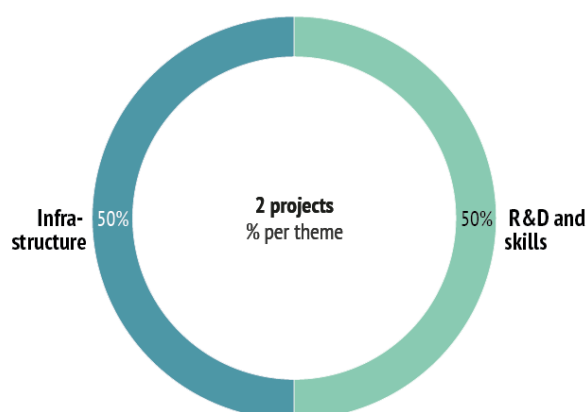
have pursued divergent national approaches, resulting in fragmented governance on digital infrastructure deployment. This could hinder coordinated funding and connectivity resilience. Weak indigenous participation also raises concerns over environmental impact, community livelihoods and the EU's normative credibility.

Governance fragmentation therefore remains the main challenge in the region. Strengthening coordination with local and Nordic partners, notably Canada and the United States, while integrating security-by-design principles, trusted-supplier frameworks, and climate resilience into connectivity projects, is also essential to secure strategic data routes and support regional stability.

Central Asia: Limited and connectivity-focused cooperation

EU digital engagement in Central Asia is very limited and centred on connectivity and infrastructure, notably through the Connectivity for Central Asia (C4CA) initiative. This programme supports the development of satellite ground stations, cybersecurity capacity-building and regulatory reforms, reflecting the EU's dual ambition: to accelerate digitalisation and bridge persistent divides, while offering trusted alternatives to dominant external suppliers.

The regional digital ecosystem remains largely shaped by Chinese and Russian influence, creating deep hardware-to-software dependencies. China expands its footprint through the Digital Silk Road (DSR)³³, bundling telecom equipment, cloud services and AI-enabled systems – especially smart industrial systems – with rapid deployment and concessional financing. Kazakhstan's and



Pakistan's DSR-related agreements and projects such as the China-Pakistan Economic Corridor show how Beijing embeds digital infrastructure in broader Belt and Road investments. Huawei's role in 5G and fibre-optic networks, Pakistan's use of BeiDou satellite systems, and the strong market presence of Chinese device manufacturers (smartphones, smart city technologies, etc.) such as Xiaomi and Honor in Uzbekistan and Kyrgyzstan further reinforce these dependencies.

Russia, meanwhile, retains regulatory weight and significant network-level control, with much of the region's internet traffic still routed through Russian infrastructure. Cloud providers such as Yandex and 1C remain entrenched, and SORM-style surveillance systems create data-security and privacy risks. Yet, Russia's full-scale invasion of Ukraine in 2022 has weakened its digital influence: sanctions, disrupted supply chains and reputational costs have pushed Central Asian governments towards supplier diversification. The Trans-Caspian Fiber Optic Cable³⁴ and growing interest in diversified data-centre markets illustrate this strategic hedging, potentially reinforcing regional integration³⁵.

Domestic political dynamics further constrain EU engagement. Authoritarian consolidation, restrictive information laws and tighter state control over data flows increase operational risks for rights-based EU initiatives and favour vendors with fewer governance conditions. At the same time, post-Ukraine shifts in IT labour, data-processing hubs and illicit cyber operations heighten demand for cyber resilience and trusted infrastructure.

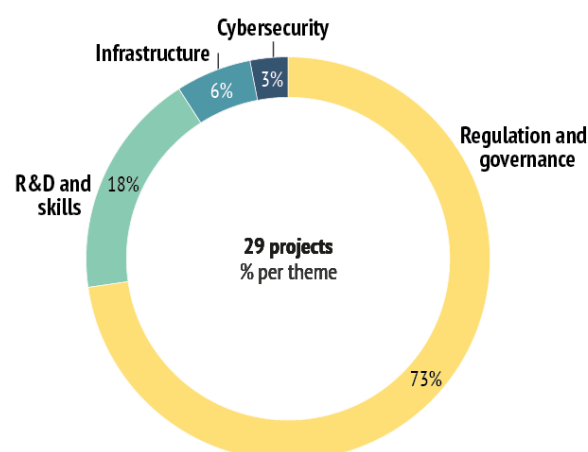
In this context, the Union's engagement remains opportunity-driven rather than structurally embedded. To strengthen its position, the EU should prioritise targeted connectivity projects with governance safeguards, support value-aligned digital public services, encourage European firms to expand into regional markets, and pursue coordinated diplomacy – recognising that durable influence requires sustained investment and calibrated expectations in a politically sensitive environment.

Global level: Shaping international digital governance

Alongside region-specific initiatives, the EU also pursues global action, aimed primarily at shaping international digital governance through multilateral forums, standard-setting and regulatory and institutional capacity-building in partner countries. Centred on regulation and political engagement, this approach reflects the Union's ambition to promote human rights, democratic principles, the rule of law and multistakeholder governance in a digital environment marked by intensifying technological competition, geopolitical fragmentation and norm contestation.

A second pillar of EU global engagement focuses on innovation cooperation and capability development. Initiatives in education, research and skills – notably Horizon Europe, Digital Europe, the Global Partnership on AI (with the OECD), and the International Network of AI Safety Institutes – demonstrate efforts to remain embedded in global innovation ecosystems. Countering technological autarky, the EU seeks to shape innovation pathways through cooperation, standard-setting and shared research agendas, while mitigating dependency risks in critical technologies such as AI, semiconductors and quantum computing.

Infrastructure initiatives form a third layer of EU global digital action. Projects such as IRIS² and Global Gateway initiatives support resilience and strategic autonomy by diversifying connectivity routes and securing trusted infrastructure. They nonetheless remain embedded in broader diplomatic and development frameworks.



The EU's global digital engagement is also unfolding amid intensifying US-China rivalry, increasing weaponisation of technological dependencies, and growing tensions around data governance, cyber stability and information integrity. EU engagement in UN discussions on digital governance and responsible state behaviour, together with its support for the implementation of the Global Digital Compact, reflects an attempt to stabilise the digital domain through rules and predictability while resisting both authoritarian governance models and techno-nationalism.

The EU's global digital action hence displays three structural trends: multilateralism as a force multiplier, regulation as a geopolitical instrument, and research cooperation as a hedge against fragmentation. In line with the work undertaken in recent years, strengthening impact will require closer alignment between global rule-shaping efforts and the EU's industrial and technological priorities, expanded research and talent partnerships in critical technologies, and the consolidation of coalitions across multilateral and informal platforms.

CONCLUSION - A PIVOTAL MOMENT FOR THE EU'S DIGITAL FUTURE

Europe's digital autonomy cannot be secured by internal policies alone. It also depends on the EU's ability to build external partnerships to diversify dependencies, strengthen trusted technological ecosystems and consolidate political support in a contested technological environment. This analysis shows that the EU's external digital engagement is substantial but uneven, combining regulatory influence, connectivity projects, innovation cooperation and selective security initiatives across diverse regional contexts. Mapping these engagements makes it possible to move beyond the proliferation of initiatives and identify the strategic priorities which should guide future action.

For instance, given their geographical proximity and direct exposure to cyber and hybrid threats, the EU should deepen enlargement partners' integration into its cybersecurity frameworks, while also extending resilience and cybercrime cooperation to other high-risk regions such as MENA and sub-Saharan Africa. At the same time, the EU neighbourhood, Africa and Latin America offer strong potential to expand digital markets and scale EU-compatible standards. Partnerships should also prioritise 'bottleneck' actors, particularly in Northeast Asia and with partners such as Taiwan and Singapore, to secure access to critical technologies, including semiconductors, AI, robotics, 6G and high-performance computing. In parallel, accelerating connectivity deployment in the Pacific, the Arctic and Central Asia would support resilient and trusted alternatives to Chinese, Russian and US infrastructure and equipment. Finally, in an increasingly fragmented digital landscape, sustaining multilateral engagement and strategic dialogue at the global level remains essential, and these efforts need to be matched by concrete capacity-building and institutional support to reinforce EU credibility.

In this perspective, strengthening the EU's external digital strategy requires adopting more flexible and operational criteria for engagement, based on trust, technological added value and complementarity, and geopolitical alignment. Such an approach enables pragmatic and incremental cooperation, focusing on areas of high impact, while allowing the EU to adapt to evolving political or technological conditions. Digital autonomy, in this sense, does not rest on uniform alignment but on the ability to develop targeted and robust partnerships, manage dependencies and expand the EU's strategic room for manoeuvre.

-
- * The authors would like to express their thanks to Maria-Loredana Campione, EUISS trainee, for her valuable assistance with data collection and research.
- 1 Von der Leyen, U., 'A Union that strives for more', 2019 (https://commission.europa.eu/document/download/063d44e9-04ed-4033-acf9-639ecb187e87_en?filename=political-guidelines-next-commission_en.pdf).
 - 2 Bômout, C., 'Autonomy is not autarky: but is the EU's new Digital International Strategy's focus on partnerships enough?', Commentary, EUISS, 13 June 2025 (<https://www.iss.europa.eu/publications/commentary/autonomy-not-autarky-eus-new-digital-international-strategy-focus>).
 - 3 European Commission, 'An international digital strategy for the European Union', 5 June 2025 (<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025JC0140>).
 - 4 Council of the European Union, 'Council conclusions on EU digital diplomacy', 26 June 2023 (<https://data.consilium.europa.eu/doc/document/ST-11088-2023-INIT/en/pdf>).
 - 5 European Commission, 'Europe's Digital Decade' (<https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade>).
 - 6 European Commission, 'State of the Digital Decade 2025 report', 16 June 2025 (https://commission.europa.eu/news-and-media/news/state-digital-decade-2025-report-urgent-and-bold-action-needed-2025-06-16_en).
 - 7 Ibid.
 - 8 Bomont, C. and Zorić, B., 'Shared threats, shared resilience: Integrating enlargement partners in EU digital and cyber security', Brief no.8, EUISS, 26 May 2026 (<https://www.iss.europa.eu/publications/briefs/share-d-threats-shared-resilience-integrating-enlargement-partners-eu-digital>).
 - 9 European Commission, 'EU-Africa-India digital corridor' (https://international-partnerships.ec.europa.eu/policies/global-gateway/eu-africa-india-digital-corridor_en).
 - 10 European Commission, 'Digital transformation and connectivity: Philippines' (https://international-partnerships.ec.europa.eu/policies/global-gateway/digital-transformation-and-connectivity-philippines_en).
 - 11 European Commission, 'Nusantara, the new capital of Indonesia' (https://international-partnerships.ec.europa.eu/policies/global-gateway/nusantara-new-capital-indonesia-building-prosperity-connectivity-and-data_en).
 - 12 Council of the European Union, 'Implementation of the EU Strategy for Cooperation in the Indo-Pacific', 20 October 2025 (<https://data.consilium.europa.eu/doc/document/ST-14071-2025-INIT/en/pdf>).
 - 13 ESIWA+ (<https://www.eucybernet.eu/project/enhancing-security-cooperation-in-and-with-asia-and-the-indo-pacific-esiwa/>).
 - 14 Copernicus LAC (https://international-partnerships.ec.europa.eu/policies/global-gateway/copernicus-latin-america-and-caribbean_en); BELLA (https://international-partnerships.ec.europa.eu/policies/programming/programmes/bella-building-europe-link-latin-america_en); European Commission, 'EU and Costa Rica deepen digital partnership with satellite connectivity agreement', 24 March 2025 (https://international-partnerships.ec.europa.eu/news-and-events/news/eu-and-costa-rica-deepen-digital-partnership-satellite-connectivity-agreement-2025-03-24_en).
 - 15 EU-LAC Digital Accelerator (<https://eulacdigitalaccelerator.com/>).
 - 16 European Investment Bank, 'The rise of Africa's digital economy', 5 May 2021 (<https://www.eib.org/en/publications/the-rise-of-africa-s-digital-economy>).
 - 17 'Middle East & Africa: \$100B+ AI and data center buildout redefines the region', Global Data Center Hub, 24 November 2025 (<https://www.globaldatacenterhub.com/p/middle-east-and-africa-100b-ai-and>).
 - 18 In DRC, Zambia, Zimbabwe, Nigeria, Malawi and Mozambique.
 - 19 European Commission, 'Construction of a data center in Nouakchott and a submarine cable in Mauritania' (https://international-partnerships.ec.europa.eu/policies/global-gateway/construction-data-center-nouakchott-and-submarine-cable-mauritania_en).
 - 20 Africa-Europe Digital Regulators Partnership (<https://d4dhub.eu/initiatives/ipris-ict-policy-regulation-institutional-strengthening>); D4DHub, iPRIS (https://international-partnerships.ec.europa.eu/policies/global-gateway/africa-europe-digital-regulators-partnership-sub-saharan-africa_en).
 - 21 African Union, 'Continental artificial intelligence strategy', 9 August 2024 (<https://au.int/en/documents/20240809/continental-artificial-intelligence-strategy>).
 - 22 European Commission, 'EU and Japan reinforce tech and digital partnership', 12 May 2025 (<https://digital-strategy.ec.europa.eu/en/news/eu-and-japan-reinforce-tech-and-digital-partnership>); European Commission, 'EU and the Republic of Korea reinforce tech and digital cooperation at the third Digital Partnership Council', 28 November 2025 (<https://digital-strategy.ec.europa.eu/en/news/eu-and-republic-korea-reinforce-tech-and-digital-cooperation-third-digital-partnership-council>).
 - 23 Council of the European Union, 'Implementing the International Digital Strategy', 14 January 2026 (<https://data.consilium.europa.eu/doc/document/ST-5270-2026-INIT/en/pdf>).
 - 24 'Autonomy is not autarky', op.cit.
 - 25 Polar Connect (<https://nordu.net/polar-connect/>).
 - 26 Vesteinsson, K. and Baker, G., 'An uncertain future for the global internet', Freedom House, 2025 (<https://freedomhouse.org/report/freedom-net/2025/uncertain-future-global-internet>).

-
- ²⁷ Internet Society, 'Internet shutdowns', 28 October 2025 (<https://www.internetsociety.org/resources/policybriefs/2025/internet-shutdowns/>).
- ²⁸ The White House, 'President Donald J. Trump secures historic \$600 billion investment commitment in Saudi Arabia', 13 May 2025 (<https://www.whitehouse.gov/fact-sheets/2025/05/fact-sheet-president-donald-j-trump-secures-historic-600-billion-investment-commitment-in-saudi-arabia/>).
- ²⁹ EU Tech Business Offer (<https://digital-strategy.ec.europa.eu/en/factpages/eu-tech-business-offer>).
- ³⁰ 'Strategy for Development of the Arctic Zone of the Russian Federation and Provision of National Security for the Period up to 2035', Russia Maritime Studies Institute, US Naval War College, 26 October 2020 (https://usnwc.edu/_images/portals/0/NWCDepartments/Russia-Maritime-Studies-Institute/16MAR23_20201026_ENG_RUS_Arctic-Strategy2035_FINAL_16MAR238f95.pdf).
- ³¹ Designating itself as 'a near-Arctic state'. State Council of the PRC, 'China's Arctic Policy', 26 January 2018 (<https://www.uaf.edu/caps/resources/policy-documents/china-arctic-policy-2018.pdf>).
- ³² Conley, H. A., Arts, S., Berzina, K. and Rintakumpu, F., 'Protecting Undersea Infrastructure in the North American Arctic', GMFUS, May 2024 (<https://www.gmfus.org/sites/default/files/2024-10/Protecting%20Undersea%20Infrastructure%20in%20the%20North%20American%20Arctic.pdf>).
- ³³ Welch, D., 'Russia and China in Central Asia's Technology Stack', GMFUS, 5 June 2025 (<https://www.gmfus.org/news/russia-and-china-central-asias-technology-stack>).
- ³⁴ Involving Azerbaijan, Kazakhstan, Uzbekistan and Turkmenistan. Kassenova, N., 'Kazakhstan, Uzbekistan putting digital distance between themselves and Russia', Eurasianet, 13 February 2024 (<https://eurasianet.org/kazakhstan-uzbekistan-putting-digital-distance-between-themselves-and-russia>).
- ³⁵ Omirgazy, D., 'Kazakhstan, Pakistan sign 32 commercial agreements to deepen strategic economic cooperation', *The Astana Times*, 5 February 2026 (<https://astanatimes.com/2026/02/kazakhstan-pakistan-sign-32-commercial-agreements-to-deepen-strategic-economic-cooperation/>).