



HIGH REPRESENTATIVE
OF THE UNION FOR
FOREIGN AFFAIRS AND
SECURITY POLICY

Brussels, 5.6.2025
JOIN(2025) 140 final

ANNEX

ANNEX

to the

Joint Communication to the European Parliament and the Council

An International Digital Strategy for the European Union

ONGOING AND PLANNED ACTIONS

OBJECTIVE	DESCRIPTION	PARTNER COUNTRY / REGION / MULTILATERAL	INDICATIVE TIMELINE
1. Secure connectivity			
Support to Arctic connectivity	Arctic connectivity is of strategic importance for the EU. It will help reduce data latency and facilitate trusted data flows between the EU, Greenland, Canada, the US and Japan, providing an alternative cable route and enhancing cable security and resilience between the EU and its partners. The EU will work with its partners to boost support for projects that advance new submarine cable routes in the region, by making use of the Connecting Europe Facility to catalyse public and private investments.	Japan, US, Canada, Greenland	2025-2030
Promote secure connectivity in enlargement countries	Promote the alignment with the EU 5G Cybersecurity Toolbox and support to adopting a legislative framework that would allow for and lead to imposing exclusions and/or restrictions on high-risk suppliers.	Enlargement countries	Continuous
Promote secure connectivity in Global Gateway partner countries	Promote secure and trusted connectivity, including 5G, submarine cable and space connectivity, in line with the EU 5G Cybersecurity Toolbox and the 2025 EU Action Plan on Cable Security, through diplomatic outreach, technical assistance and financial support under the Global Gateway.	Global	Continuous
National and regional 5G implementation guidelines and development of the LAC Connectivity Toolbox	These guidelines will address security, infrastructure challenges, and priority use cases in various Latin America and Caribbean national contexts. Another key focus will be the development of the LAC Connectivity Toolbox, which shall provide practical tools, best practices, and guidance for addressing cross-border connectivity, secure and resilient infrastructure, and meaningful connectivity challenges. This includes co-developing actionable recommendations, providing technical support, and fostering bi-regional coordination for 5G deployment.	Latin America and Caribbean countries	Ongoing under the EU-LAC Digital Alliance – until Q4 2027

OBJECTIVE	DESCRIPTION	PARTNER COUNTRY / REGION / MULTILATERAL	INDICATIVE TIMELINE
Annual conference on secure connectivity	Possibly establish an annual conference on secure connectivity, hosted in Brussels, to deepen technical contacts and understanding on opportunities and security requirements for future routes, partnerships, and financing, feeding into the Global Gateway process.	Global	Annual
2. Emerging technologies			
<i>Artificial Intelligence</i>			
Cooperation on AI safety	<p>The EU AI Office has signed an administrative arrangement on cooperation on AI safety with Singapore, and bilateral exchanges have started with other AI Safety Institutes – Japan, Korea, the United Kingdom and Australia. Cooperation arrangements with partner countries, to be pursued further e.g. including topics such as boosting innovation and AI uptake and cooperation on AI for public good (Japan), AI safety (India and Canada) and governance and regulatory aspects (Australia).</p> <p>The EU AI Office will continue to deepen the cooperation on AI safety in the Network of AI Safety Institutes, in particular, addressing the safety of general-purpose AI models through information exchanges and best practices, joint testing and evaluations, development of tools and benchmarks, as well as research into AI safety.</p>	<p>Japan, the Republic of Korea, India, Australia, Canada, the US, the United Kingdom, Ukraine, Moldova</p> <p>Western Balkans, Africa, Latin America and the Caribbean</p>	Continuous
Global Partnership on AI and OECD	The EU is a founding member of the Global Partnership on AI and continues to engage in this initiative after it formed an integrated partnership with the OECD Working Party on Artificial Intelligence Governance (AIGO). The AI Office holds one of the Vice-Chair posts in the OECD AIGO. In addition, the AI Office is involved in all the AI-related working groups of the OECD and actively contributing to this work.	Multilateral	Continuous
G7 and G20	The EU will continue to engage actively in the AI discussions in G7 and G20. This includes the Hiroshima AI Process and its reporting framework as well as the Hiroshima Friends Group, a voluntary framework of countries supporting the spirit of the Hiroshima AI Process towards achieving safe, secure and trustworthy AI.	Multilateral	Continuous

OBJECTIVE	DESCRIPTION	PARTNER COUNTRY / REGION / MULTILATERAL	INDICATIVE TIMELINE
	<p>Moreover, the EU will continue to explore the possibility of G7 guidelines on AI in Science.</p> <p>One of the G20 South African Presidency priorities is Artificial Intelligence and Innovation for Sustainable Development, which is a priority in Africa, Asia and LAC countries.</p>		
Clean Energy Ministerial	The Republic of Korea, host of the 16th Clean Energy Ministerial meeting 2025, made “AI & Energy” one of its priority themes. The EC will actively engage with the ministerial programme and explore international collaboration in the field of digitalisation and AI in the energy sector.	Multilateral	Continuous
Research cooperation under Horizon Europe	The association of a number of non-EU partner countries to Horizon Europe will support research cooperation in AI and AI-based applied research.	Associated Countries to Horizon Europe	Continuous
AI for Public Good	As part of the AI for the Public Good initiative, the EU supports the deployment of AI solutions for the public good, including Generative AI, technology transfer and capacity building, with partner countries in Africa and Latin America and the Caribbean (building on EU-LAC Alliance). The EU also supports scientific cooperation and development of AI-based Local Digital Twins underpinning urban reconstruction in Ukraine.	Africa, Latin-America and Caribbean, Asia-Pacific Ukraine	Continuous
AI Hub for Sustainable Development and AI collaboration with Smart Africa	<p>The AI Hub for Sustainable Development is co-designed by the Ministry of Enterprises and Made in Italy (MIMIT) and the UNDP, aiming at strengthening local AI ecosystems in partnership with African countries.</p> <p>Smart Africa has launched the Africa AI Council and the EU is structuring its collaboration with Smart Africa under the Global Gateway strategy, building on the administrative arrangement between the European Commission and Smart Africa and following a Team Europe approach.</p>	Africa	Continuous
GovTech4all	Development and piloting of AI solutions in the public sector for enhancing decision making, service delivery and internal administrative tasks. The goal is to support and	EU and EU candidate and potential candidate countries	Q4 2025/2026

OBJECTIVE	DESCRIPTION	PARTNER COUNTRY / REGION / MULTILATERAL	INDICATIVE TIMELINE
	accompany the goals of the Interoperable Europe Act, as well as wider policy goals of public sector innovation and start-up growth in Europe.		
5G/6G			
6G research and innovation aligned 2026 call	Research and innovation cooperation on 6G AI powered RAN. One project from Smart Networks and Services Joint Undertaking mirroring one project from Japan and the Republic of Korea.	Japan and the Republic of Korea	Project running 2027-2030
6G research and innovation aligned call	6G research and innovation cooperation focused on physical layers, advanced antennas and AI RAN.	Taiwan	Potential aligned call in 2026 or cooperation between existing projects
5G testbed	To support the development of 5G use cases, the EU is partnering with Costa Rica on a 5G testbed, with Nokia and Ericsson expected to provide the equipment.	Costa Rica	Continuous
Semiconductors			
Joint research and innovation projects in the field of semiconductors	Research and innovation projects in semiconductors, jointly funded by the European Commission and Japan and the Republic of Korea. With the Republic of Korea, projects aim at advancing heterogeneous integration of chips as well as neuromorphic computing technologies. With Japan calls are planned for 2026 on per- and polyfluoroalkyl substances (PFAS) replacement, heterogeneous integration and chiplets, and devices and processes beyond 2 nanometres.	Japan, Republic of Korea	Continuous
Early warning mechanism on supply chain & public subsidies	Joint early warning mechanism, between the European Commission and the US and Japan respectively, aimed at identifying supply chain disruptions, and transparency mechanism on public subsidies provided to the semiconductor sector.	US, Japan	Continuous

OBJECTIVE	DESCRIPTION	PARTNER COUNTRY / REGION / MULTILATERAL	INDICATIVE TIMELINE
Attracting talent and skilled workforce	As part of the EU-India Trade and Technology Council, EU and India committed to developing a dedicated programme that will facilitate talent exchanges and foster semiconductor skills among students and young professionals.	India	Continuous
G7 semiconductor Point of Contact group	The G7 Point of Contact (PoC) group on semiconductors is dedicated to facilitating information exchange and sharing best practises among G7 members, on issues impacting the semiconductor industry, including pre-competitive industrial research & development priorities, sustainable manufacturing, the effect of non-market policies and practices, and crisis coordination channels.	Multilateral	Continuous
World Semiconductor Council – Government / Authorities Meeting on Semiconductors (GAMS)	The Government/Authorities Meeting on Semiconductor (GAMS) has a unique setting where Governments and Industry Associations representing together 95% of world's semiconductors production (EU, US, South Korea, Japan, Taiwan, and China), meet to respond to common challenges facing the industry. The European Commission is representing the EU.	Multilateral	Continuous
<i>Quantum and High-Performance Computing</i>			
EU-Japan Quantum Computing Collaboration	Joint research and innovation projects focusing on hybrid Quantum-HPC algorithms and optimizing applications in areas of mutual interest such as biomedical and environmental sciences. It aligns with the EuroHPC Joint Undertaking's objectives to support the EU-Japan Digital Partnership.	Japan	Continuous (2026-2029)
EU-Canada Quantum Research Initiatives	Establish collaborative projects in quantum computing, sensing, and communication, leveraging Canada's National Quantum Strategy and existing research hubs.	Canada	Continuous (2023-2026)
EU-Republic of Korea Quantum Technology Calls	Coordinate calls for joint projects in quantum computing, sensing and communication, enhancing research and innovation collaboration and aligning with the strategic priorities of Republic of Korea in quantum technology development.	Republic of Korea	2027-2030
G7 Quantum Technology Working Group	Under Canada's G7 presidency, establish a working group to enhance information sharing on quantum developments and promote common standards.	Multilateral	Ongoing

OBJECTIVE	DESCRIPTION	PARTNER COUNTRY / REGION / MULTILATERAL	INDICATIVE TIMELINE
EU-LAC Supercomputing Network	Establish a robust partnership to federate High Performance Computing resources in Latin America and the Caribbean and to enhance their interoperability and integration with the European HPC ecosystem.	Latin America and the Caribbean	Possible kick-off at the CELAC-EU Summit 2025
3. Cybersecurity			
Advance cyber dialogues with partner countries	The EU has Cyber Dialogues with the US, Ukraine, the United Kingdom, Japan, India, the Republic of Korea and Brazil. Cybersecurity is also discussed in the Digital Partnerships with Japan, the Republic of Korea, Singapore and Canada and the Digital Dialogues with Brazil, Mexico, Argentina, Australia and the Western Balkans.	US, Ukraine, United Kingdom, Japan, India, Republic of Korea, Brazil, Singapore, Canada, Mexico, Argentina, Australia, Moldova, Western Balkans	Continuous
Mutual recognition agreements (MRA) regarding product cybersecurity	The Cyber Resilience Act (CRA) sets out requirements for the cybersecurity of products with digital elements in the internal market. The EU will work with relevant partners to explore the potential for mutual recognition agreements regarding the CRA and respective frameworks of the partners to facilitate compliance with product cybersecurity requirements.	Bilateral discussions	By the time of CRA application (end 2027)
Extension of the EU's Cyber-Reserve to Ukraine and the Republic of Moldova	Amendments to the Association Agreements related to the participation of Ukraine and the Republic of Moldova in the Digital Europe programme will pave the way for extending the EU's Cyber-Reserve to both countries.	Enlargement countries	Continuous
Engagement in the G7 Cybersecurity Working Group	The Commission represents the EU in the G7 Cybersecurity Working Group. Among other topics, the Commission will pursue cooperation on healthcare cybersecurity, in line with the European action plan on the cybersecurity of hospitals and healthcare providers (COM(2025) 10 final).	Multilateral	Continuous
Advancing the UN Framework of Responsible	At the UN and within regional security bodies, the EU will continue to promote responsible state behaviour in cyberspace, based on the UN General Assembly-endorsed framework. This includes upholding international law, adhering to globally	Multilateral	Continuous

OBJECTIVE	DESCRIPTION	PARTNER COUNTRY / REGION / MULTILATERAL	INDICATIVE TIMELINE
State Behaviour in Cyberspace	accepted norms of state conduct in peacetime, developing confidence-building measures, and supporting states in building the capacity to implement these framework elements.		
Engagement in the Counter Ransomware Initiative	The Commission represents the EU in the International Counter Ransomware Initiative (CRI). The EU will continue its active participation in CRI. Moreover, the European action plan on the cybersecurity of hospitals and healthcare providers commits to advancing cooperation in the CRI.	Multilateral	Continuous
Cyber capacity-building	The EU is carrying out external cyber capacity-building projects with partner countries across the world. The EU will continue these initiatives, by prioritising activities addressing cybercrime and building cyber resilience, including support for building strategic frameworks, developing incident management capabilities and enhancing expertise through trainings.	Global	Continuous
LAC4	LAC4 is the regional hub for cybersecurity education and training in Latin America and the Caribbean. LAC4's objective is to provide cybersecurity and cybercrime expertise to support digital transformation and collaboration in Latin American and Caribbean to counter cyber threats.	Latin America and the Caribbean	Continuous
EU-LAC Cybersecurity Community of Practice (CoP)	Under the EU-LAC Digital Alliance, a Community of Practice (CoP) of cybersecurity experts and practitioners will be established to encourage the exchange of best practices on cybersecurity between both regions. Future activities may include institutionalising mechanisms to swiftly mobilise cybersecurity experts in case of cyber-attacks and emergencies and capacity-building.	Latin America and the Caribbean	Continuous (until Q4 2027)
4. Digital identities and Digital Public Infrastructure			
Mutual recognition of electronic signatures and other trust services	Advance towards mutual recognition of electronic signatures and other trust services with third countries in order to create a global trust framework. This includes developing a set of tools and services implementing trust anchors for the global recognition of trust services and digital identities, and dropping digital barriers by reusing and replicating the European Trust Services infrastructure in their territory.	Ukraine, Moldova, Western Balkans, Egypt, India, Brazil, Japan, Uruguay, members of the Central America Integration System (SICA)	Continuous (2025-2027)

OBJECTIVE	DESCRIPTION	PARTNER COUNTRY / REGION / MULTILATERAL	INDICATIVE TIMELINE
		(Costa Rica, El Salvador, Guatemala, Honduras, Nicaragua and Panama)	
Promote cooperation on Digital Public Infrastructures on the basis of the EU eID wallet	Promote cooperation on Digital Public Infrastructures by supporting the creation of a scalable suite of open-source digital building blocks and solutions around EU wallets. In addition, demonstrate interoperability between the EU eID Wallet and similar initiatives in third countries on the basis of practical use-cases.	Japan, India, Singapore Multilateral	Continuous (2025-2027)
Prepare onboarding of digital public services in scope of the Single Digital Gateway	Cooperate with EU accession countries to prepare onboarding and development of interoperable solutions for online administrative procedures and the Once-Only Technical System in scope of the Single Digital Gateway. Those services facilitate access of business and citizens to do business, work and live in EU countries.	Western Balkans, Moldova, Ukraine	Continuous (2025-2030)
Standardisation of digital identity solutions	The Architecture and Reference Framework for the European Digital Identity Wallets aims to set a global example for trusted and secure identification at a high level of assurance. Cooperation between the EU and like-minded countries on the development of common identity standards on the basis of the EU model shall be pursued, including in international organisations.	Japan, India, Canada Multilateral	Continuous (2025-2030)
Global Digital Health Certification Network (GDHCN)	The Global Digital Health Certification Network is an initiative aimed at creating a standardized, interoperable framework for digital health credentials and certifications. This network, created by the European Commission to fight against COVID-19 and later on taken up by WHO is intended to facilitate the secure and efficient exchange of health-related information across borders (e.g. COVID-19 certificates, Digital International Certificate of Vaccination or Prophylaxis/Yellow Booklet, Vaccination Card, International Patient Summary), promoting global health security and improving healthcare delivery.	Global	Continuous (2025-2028)
5. Online platforms and integrity of the information ecosystem			

OBJECTIVE	DESCRIPTION	PARTNER COUNTRY / REGION / MULTILATERAL	INDICATIVE TIMELINE
DSA/DMA alignment support for EU accession countries	Support alignment of EU accession countries with EU DSA and DMA.	Moldova, Ukraine, Western Balkans	Continuous (2025-2027)
Marketplaces and e-commerce	Raise EU key concerns (closed market for digital services, illegal goods on Chinese marketplaces) and possible areas of closer cooperation (data sharing on illegal Chinese sellers), in line with the EU-China Administrative Arrangement on product safety cooperation and an Action Plan on Safety of Products Sold Online.	China	Continuous (2025-2027)
Global human rights-based implementation of online platform laws	Promote universal principles underpinning the DSA and DMA in global instruments (including OHCHR guidance on UN Cybercrime Convention).	UN, OHCHR, UNESCO, OECD	Continuous (2025-2027)
Regional human rights-based implementation of online platform laws	Prioritise regional engagement on human rights-based implementation of online platform laws, organised in cooperation with the UN (where possible), to bring together policymakers, regulators and civil society.	ASEAN, LAC, countries under the CEFTA	Continuous (2025-2027)
EU election observation missions (EOM) social media observation	EU EOMs integrate observation and of social media behaviour during electoral processes in their overall assessment of electoral integrity.	Global	Continuous
Advance partnerships to bolster resilience against FIMI	Promote resilience and technological awareness on FIMI attacks; expose and increase costs to perpetrators.	Global	Continuous
6. Internet Governance			
Promote an inclusive multi-stakeholder governance model for the Future Internet	In the negotiations for the World Summit on the Information Society (WSIS+20) Review, the EU aims at enhancing inclusivity, notably from partner countries and youth communities. This includes upholding an open, human-centric Internet based on human rights, enhance multi-stakeholder Governance, and bridge the new digital divides by	Multilateral	Q4 2025

OBJECTIVE	DESCRIPTION	PARTNER COUNTRY / REGION / MULTILATERAL	INDICATIVE TIMELINE
	<p>establishing an operational connection with the Sustainable Development Goals (SDGs) and the Global Digital Compact (GDC).</p> <p>The EU will also engage youth in shaping the future of Internet Governance by integrating their perspective into the forthcoming annual Youth Policy Dialogue on digital, fostering informed participation, strengthening digital civic responsibility, and equipping young leaders with the tools to uphold an open, secure, and inclusive Internet.</p>		
Work towards an Open, Free and Sustainable Internet	The EU will support accountability, comprehensive monitoring and promotion of internet freedom worldwide while strengthening the openness and sustainability of the internet infrastructure and empowering civil society organisations (CSOs) to hold their own governments accountable. This includes addressing internet shutdowns via diplomatic channels and promote policies that maintain an open and interconnected internet.	Global	Continuous
Improving the security, resilience and openness of the Internet	<p>Implement a multi-stakeholder strategy for the comprehensive deployment of Internet standards across the EU Internet infrastructure.</p> <p>Charting the EU Influence in Web 4.0: Conduct an extensive mapping of potential EU contributions to improved or new networking protocols and solutions required and enabled by impacts of core technologies like AI, extended reality (XR) / virtual reality (VR), blockchain, and quantum computing that are currently shaping the Web 4.0.</p>	Global	2026-2030
Promote the Open Internet Stack	The EU will support an international extension and broadening of the Open Internet Stack, referring to the foundational structure of protocols that enable communication and information sharing on the internet, to address the needs of partner countries, including enhancing trust, reducing costs, avoiding vendor lock-in, supporting customizability and integration, and upholding values such as privacy, security, and data protection.	Global	Continuous