



HIGH REPRESENTATIVE
OF THE UNION FOR
FOREIGN AFFAIRS AND
SECURITY POLICY

Brussels, 5.6.2025
JOIN(2025) 140 final

**JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE
COUNCIL**

An International Digital Strategy for the European Union

An International Digital Strategy for the European Union

The digital and Artificial Intelligence (AI) revolution is reshaping economies and societies in Europe and across the world. Economic players and countries that are able to master them do not only gain a decisive economic edge in terms of competitiveness and efficiency but can also use these technologies to strengthen their national defence and security, as well as ensure they are aligned with the core values of their society. Conversely, those who are late in embracing them risk lagging behind economically and undermining their sovereignty.

In such context, the EU is determined to boost its tech competitiveness and innovation capacity while working with partners and allies to support their own digital transition. No country or region can tackle the digital and AI revolution alone. The EU remains committed to the rules-based global order and to the defence of its fundamental values.

For the EU's competitiveness, economic security and defence capacity, it is crucial to closely cooperate with our partners and tech allies to enhance the ability of European tech companies to innovate and grow globally. Concerted EU efforts are necessary to ensure that global digital governance supports EU interests and fundamental values.

This strategy sets out the basis on which the EU will address these objectives, working in a joined-up way.

1. DIGITAL AS A CORE ELEMENT OF THE EU'S EXTERNAL ACTION

At the current geopolitical juncture, the EU remains a reliable and predictable partner, committed to strengthening its existing relations with allies globally, and forging new mutually beneficial partnerships with those willing to work towards shared objectives. The EU's support to the rules-based global order, aligned with the values of democracy, rule of law and fundamental rights, is steadfast.

The EU's growing network of bilateral and regional partnerships allows the EU to be stronger on the world stage, building coalitions in pursuit of shared objectives in key international fora and organisations. From shaping norms in multilateral fora to deepening bilateral partnerships, the EU aims to make progress on concrete and immediate priorities, protecting and promoting the EU's strategic interests.¹

As emphasised by the Draghi report², the increasing productivity gap between the EU and the United States since the mid-1990s is largely explained by the superior ability of the US to innovate, scale-up globally and succeed in the tech sector. The EU also faces the risk of weaponisation of its technological and economic dependencies and the risk of critical technology leakage. As outlined in the ProtectEU Strategy³, the lines between offline and online

¹ See the [Conclusions](#) of the European Council, 17th April 2024: "*The European Council also highlights the need to strengthen the EU's leadership in global digital affairs and invites the Commission and the High Representative to prepare a joint communication on the subject*" (p. 10)

² The future of European competitiveness: Report by Mario Draghi (2024)

³ Communication on ProtectEU: a [European Internal Security Strategy](#), COM(2025) 148

threats are increasingly blurred and the EU needs to cooperate better with its partners to combat the misuse of technologies.

In boosting its tech competitiveness and innovation capacity, as set out in the EU's Competitiveness Compass⁴, the EU can build on several strengths. The EU has a large and integrated digital single market and is the global leader in the import and export of digitally delivered services⁵. It hosts world-leading tech companies and has an increasing number of tech start-ups⁶. It can draw on world-class research and innovation and 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.

As part of its Digital Decade Policy Programme 2030⁷, the EU aims to boost investment in connectivity infrastructure, skills, and research⁸, and create more favourable conditions for EU disruptive start-ups to emerge and scale up. As technologies such as AI, semiconductors, cloud and quantum computing are fundamentally changing the industrial as well as defence and security landscape, Europe needs an industry capable of designing, developing, manufacturing and delivering these technologies and products faster and at scale.

An increasingly active **Digital Diplomacy** has built on these strong domestic foundations to advance our international priorities and to build partnerships⁹. Investments and initiatives launched under the **Global Gateway**, including in enlargement and neighbourhood countries, notably the EU Growth Plans, demonstrate the strategic importance of the digital sector from a geopolitical, security and economic point of view.

Building on the EU's strengths and internal policies and actions, the International Digital Strategy for the European Union will therefore focus on the following objectives:

- a) **Boost the EU's tech competitiveness through economic and business cooperation.** The EU will continue to cooperate with trusted partners to reinforce EU leadership in emerging tech, including through research and innovation and by attracting foreign investments and talents; use its international tools to develop and promote EU technology solutions worldwide; and expand its growing network of digital trade agreements
- b) **Promote a high level of security for the EU and its partners.** In line with existing commitments¹⁰, the EU will continue to strengthen its cybersecurity and cyber defence, particularly of key critical infrastructures; enhance the security of research while enhancing research in security-related fields; tackle hybrid threats and foreign information manipulation and interference; enhance the resilience, security, and stability of ICT supply chains, including beyond its borders; tackle cybercrime through joint operations¹¹, including through bilateral and multilateral cooperation; and promote trusted suppliers of digital technologies, including in dual-use technologies such as AI and quantum.
- c) **Shape global digital governance and standards with a network of partners.** The EU will continue to promote its values-based approach on digital governance and digital

⁴ Communication on a Competitiveness Compass for the EU, COM(2025) 30 final

⁵ See source [WTO](#)

⁶ COM(2025) 217 of 28/05/2025 – 'EU startup and scale-up Strategy'

⁷ See the full [Digital Decade Policy Programme](#)

⁸ As outlined in the Communication on the Union of Skills COM(2025) 90 final

⁹ As outlined by the Foreign Affairs [Council Conclusions on Digital Diplomacy](#) in June 2023

¹⁰ The [Protect EU Strategy](#) ((COM)2025 148), [Joint White Paper for European Defence Readiness 2030](#), [Preparedness Union Strategy](#) (JOIN(2025) 130), [Strategic Compass](#) (7371/22)

¹¹ For example: [Europol](#)

standards to shape a global digital transformation that is human-centric, trustworthy, and respects human rights and fundamental freedoms. By acting decisively, the EU can be a driving force of responsibly guided technological advancement on the global stage.

2. SCALING THE EU'S GLOBAL NETWORK OF PARTNERS

The EU has developed strong **regional and bilateral digital cooperation with partners** through Ministerial-level Trade and Technology Councils¹² and Digital Partnerships¹³, as well as Digital Dialogues¹⁴. It maintains Cyber Dialogues with a wide range of partners¹⁵, and digital issues are an increasingly important feature of the tailor-made Comprehensive and Strategic Partnerships¹⁶.

In addition, digital cooperation also builds on the association of partner countries to key EU programmes, notably Horizon Europe¹⁷ and the Digital Europe Programme¹⁸ for advanced research and innovation cooperation and the deployment of digital technologies.

Advancing the harmonisation of key digital transformation policies, investing in secure digital connectivity and boosting innovation are also at the heart of the EU's cooperation with **enlargement and neighbourhood countries**, via instruments such as Deep and Comprehensive Free Trade Agreements or Stabilisation and Association Agreements. These trade agreements and other related instruments such as the Growth Plans for the Western Balkans¹⁹, the Reform and Growth Facility for Moldova²⁰ and the Ukraine Facility²¹ set a strategic basis for the gradual integration of candidate countries into the Digital Single Market²².

The EU is developing a **New Pact for the Mediterranean** with partners of the Southern Neighbourhood, building on the 2021 Agenda for the Mediterranean, to deepen our political engagement and strengthen cooperation in areas of mutual interest, notably in the digital domain.

The EU is continuously expanding its network of **free trade agreements**²³ and digital trade agreements²⁴. Among others, these set high-standard digital trade rules that ensure a secure and safe online environment for consumers, bring transparency, predictability and legal certainty for companies, and prevent or remove unjustified barriers to digital trade including for cross-

¹² With the U.S. and India

¹³ With Japan, the Republic of Korea, Singapore and Canada

¹⁴ With Brazil, Mexico, Argentina, Australia and the Western Balkans

¹⁵ India, Japan, the Republic of Korea, Brazil, United States, Ukraine and the United Kingdom

¹⁶ With partners such as Tunisia, Egypt or Jordan

¹⁷ Nineteen countries are currently associated to Horizon Europe – listed [here](#). In addition, Switzerland, the Republic of Korea and Egypt are expected to become associated in 2025, whereas association negotiations are progressing with Japan

¹⁸ Countries associated to DEP are listed [here](#)

¹⁹ Communication new Growth Plan for the Western Balkans, COM(2023) 691

²⁰ See more information on the [Growth Facility for Moldova](#)

²¹ [Ukraine Facility - European Commission](#)

²² For example, following the transposition of the relevant EU acquis, Ukraine and Moldova are on their path to be granted mutual internal market treatment for roaming

²³ Free Trade Agreements with comprehensive digital trade chapters have been concluded with the United Kingdom, New Zealand and Chile, and are ongoing with India, Indonesia, Thailand, Philippines and Malaysia

²⁴ Signature of the EU-Singapore Digital Trade Agreement took place on 7 May 2025. Negotiations for the Digital Trade Agreement with Korea were concluded March 2025. Rules on cross-border data flows with Japan, complementing the EU-Japan Free Trade Agreement, entered into force in July 2024.

border data flows. Furthermore, the Commission liaises with other leading regulators and enforcers, building new networks on digital services and AI.

The Global Gateway strategy offers the opportunity to advance partnerships, policy dialogues, and investments with countries around the world, including through the EU-Latin America and Caribbean Digital Alliance²⁵, the administrative arrangement with Smart Africa²⁶, the Team Europe Central Asia initiative²⁷, and Digital Economy Packages with partners in Africa, Asia and Latin America²⁸, including with Least Developed Countries. The Clean Trade and Investment Partnerships²⁹ allow the EU to address the links between digital issues, trade and clean tech.

There is a growing appetite across the world for digital cooperation with the EU, and the current global landscape calls for new, deeper, and more flexible forms of cooperation to nurture mutually beneficial partnerships, which recognise the advances made by many of our partners across the digital arena, from digitising government services to facilitating electronic payments, from supporting citizens' rights to developing local resilience. The EU will keep seeking cooperation – not only with long-time like-minded partners, but with any country with which we share common objectives.

Faced with the need to accelerate its digital transformation in a more challenging geopolitical context, the EU will therefore scale its global network of partners in four directions:

- 1) **Deepening** its existing Digital Partnerships and Dialogues, to **advance cooperation in key areas**, such as research and innovation, industrial and policy cooperation on emerging tech, transparency and resilience of global supply chains, security and sustainability of digital infrastructure, AI deployment and innovation, with a focus on mutual economic benefits and enhancing economic security. The EU will propose a more significant integration of additional priorities into these partnerships, such as cybersecurity, research security, sensitive technology protection, and aspects related to dual-use technologies. It will continue engaging in advanced regulatory cooperation. Deepening the Digital Partnerships and Dialogues will also involve providing an enhanced role for businesses from the EU and partner countries, stimulating business-to-business and business-to-government cooperation and focusing on investment opportunities.
- 2) **Broadening** the existing cooperation network, with the establishment of **new Digital Partnerships and Dialogues** and expanding the network of **digital trade agreements**. Priority partners will be determined building on the EU's priorities and existing bilateral and regional cooperation at EU and Member State level. Under the Global Gateway, the EU will work to increase European investments in partner countries, linking the EU with centres of digital growth and contributing to the EU's economic security.
- 3) **Connecting** these partnerships to **operate as a network**. As the network of partnerships expands, so does the opportunity to work together in pursuit of shared interests. Likewise, cooperation is increasingly necessary as we face common challenges.

²⁵ https://international-partnerships.ec.europa.eu/policies/global-gateway/eu-latin-america-and-caribbean-digital-alliance_en

²⁶ <https://digital-strategy.ec.europa.eu/en/news/eu-and-africa-strengthen-cooperation-digital-transformation>

²⁷ https://ec.europa.eu/commission/presscorner/detail/pl/ip_22_6963

²⁸ Since 2022 the EU has launched Digital Economy Packages in Nigeria, Colombia, the Democratic Republic of Congo, Kenya and the Philippines.

²⁹ https://commission.europa.eu/topics/eu-competitiveness/clean-industrial-deal_en

Cooperation could take the form of regular technical exchanges on common issues (e.g. emerging tech, secure and trusted connectivity, standardisation or regulatory cooperation), the preparation of joint projects (e.g. research and innovation cooperation, interoperability pilots, joint projects in third countries), and the organisation of a network, involving high-level representatives from EU partners, the EU and EU Member States.

- 4) **Strengthening Security & Defence Partnerships**³⁰ as regards digital issues, given the increasing importance of advanced digital infrastructure and technologies. Leveraging investment into dual use advanced technological capabilities and promoting the EU security and defence tech industry as a central partner and driver of innovation in AI, quantum and other emerging technologies are among the priorities in this area.

The EU sees the development of AI as fundamental for the future of humanity. It cannot be reduced to the quest for supremacy among advanced AI powers. In response, the EU will continue to promote its open and collaborative model of developing trustworthy AI, which is based on participation of researchers and the private sector in ‘AI Factories’. In this regard, cooperation with like-minded partners and allies which share our respect for the rule of law and fundamental and democratic values, will be crucial.

Examples of forthcoming actions:

- Preparation of potential **new Digital Partnerships and Dialogues**, in a Team Europe approach, ensuring close cooperation with Member States, industry, stakeholders and partner countries, including in the context of the EU cooperation with neighbourhood countries.
- Establishment of a **Digital Partnership Network**, involving the EU’s partners, the EU and its Member States.
- Close cooperation to promote **synergies between Digital Partnerships** and the technology-related issues of the EU’s **Security and Defence Partnerships**.
- Expansion of the network of **Digital Trade Agreements** and continuation of negotiations of **Free Trade Agreements including on digital trade**.

3. THE EU TECH BUSINESS OFFER

To engage with a broader set of trusted partners, the EU will develop an integrated **Tech Business Offer**. Such a comprehensive Offer will support the deployment of secure and trusted connectivity, Digital Public Infrastructure, AI and software solutions, and beyond. The objective will be to tailor and combine technology components in a modular approach – balancing the interests of partner countries and the EU, in order to create **a package of mutual benefits**. This will be complemented with capacity-building and measures to bridge the global talent gap, coordinating training efforts on digital skills with international partners. The EU will actively promote digital solutions enabling more energy- and resource-efficient manufacturing, services and other applications.

The Tech Business Offer will be managed jointly by the EU and its Member States in a ‘**Tech Team Europe**’ approach, closely involving EU companies³¹, EU Development Finance

³⁰ The EU has secured such partnerships with the United Kingdom, Norway, Moldova, South Korea, Japan, Albania and North Macedonia.

³¹ Including through the [Global Gateway Business Advisory Group](#)

Institutions and Export Credit Agencies, with a strong facilitator role by the **D4D Hub**³² and the EU4Digital³³ umbrella initiative. The Offer will build on existing external financing tools and investments by the private sector. It will be essential to coordinate investments through the different programmes, between public and private sector and to continue improving the business environment. This will be done in close cooperation with EU Delegations and national Embassies, for example via the **Informal Digital Hubs**, which the EU has established in a number of partner countries³⁴ to promote Team Europe cooperation. In countries with which strategic partnerships have been concluded or are being negotiated, the Offer will be integrated in the existing or negotiated partnership framework.

4. PRIORITY AREAS OF COOPERATION WITH PARTNER COUNTRIES

Cooperation with partner countries will cover the following areas:

Secure and trusted digital infrastructure

The security and resilience of digital networks and infrastructures are essential to enable developments in critical sectors such as energy, transport, finance and health. While the EU has already demonstrated leadership in this area, work will continue, by drawing on instruments such as **the 5G Toolbox**³⁵, to assist partner countries who are equally concerned about the need to build their digital economy on secure foundations. In line with the recent Communication to strengthen the security and resilience of submarine cables³⁶, this approach could be extended to submarine cables and other critical digital infrastructure. This could be the subject of an annual conference to deepen technical contacts and understanding on opportunities and security requirements for future routes, partnerships, and financing, feeding into the Global Gateway process.

The EU will promote the deployment of secure digital connectivity and sustainable infrastructure worldwide – in particular secure and trusted 5G networks, submarine and terrestrial cables, satellite connectivity, Internet infrastructure, supercomputers and data centres. The EU will also work to support its partners' resilience through diversification and integration of networks, including through satellite connectivity and other forms of non-terrestrial networks. The EU will seek to develop a network of secure³⁷ submarine and terrestrial communication cables connecting the EU with partner countries, as well as sovereign and resilient space connectivity. This should support the EU's role as an international hub capable of hosting data and computing capacities in a resilient and reliable space, tapping the opportunities of the data economy, and attracting investments in sustainable data centres, computing and AI capacities. In cooperation with partner countries, the EU will actively seek to support digital solutions enabling more energy- and resource-efficient manufacturing,

³² The [Digital for Development \(D4D\) Hub](#) is a platform that aims to strengthen digital cooperation and coordination between the European Union and its Member States and partners in Africa, Asia-Pacific, Latin America and the Caribbean, and EU neighbouring countries.

³³ The EU4Digital umbrella initiative pools together EU funded programmes aimed at extending the benefits of the Digital Single Market to the [Eastern Partnership](#) countries and to the Western Balkans.

³⁴ Kenya, Tanzania, Nigeria, Colombia, Brazil.

³⁵ [Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures](#)

³⁶ [Joint Communication on EU Action Plan on Cable Security](#), JOIN(2025) 9 final

³⁷ In line with the [Commission Recommendation on Secure and Resilient Submarine Cable Infrastructures](#), C(2024) 1181, and the [Joint Communication to strengthen the security and resilience of submarine cables](#), JOIN(2025) 9.

services and other applications, reducing the carbon footprint as well as facilitating climate adaptation and resilience.

Examples of forthcoming actions in the field of **secure connectivity**:

- **Arctic connectivity** is a strategic priority for the EU. The EU will work with 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.
- A key element of **Global Gateway** investment in the digital sector is a network of strategic submarine communication cable infrastructure projects to provide secure and resilient links between the EU and partner countries. Investments include:
 - 1) **BELLA**, the first transatlantic optical fibre cable between the EU and Latin America and the Caribbean, which connects Latin-American research institutes, provides fast access to Earth Observation data from the Copernicus component of the EU's Space Programme. It will be further extended across Central America and the Caribbean and will support the growth of High-Performance Computing in the region.
 - 2) The **MEDUSA** submarine cable, supported by the European Commission and EIB Global, will provide high-speed connectivity between the northern and southern shores of the Mediterranean and will be extended to West Africa.
 - 3) **Blue-Raman** consists of a planned 11,700km secure submarine cable system connecting Europe to India, with landings in the Middle East and Eastern Africa, along the India-Middle East-Europe Economic Corridor (IMEC). With its strong connectivity dimension linking Europe and India via the Gulf region, it will facilitate the exchange of data and increase cooperation with partner countries.
- The EU's Black Sea strategy recognises the **Black Sea** as a key gateway linking Europe to the South Caucasus, Central Asia, and beyond. To increase connectivity and trade with the **Eastern Partnership** region, the EU will support targeted investments in digital infrastructure, with the development of Black Sea digital links aiming at creating secure, high-capacity internet connection, when conditions allow.
- The **Central Asia Team Europe Initiative** will provide enhanced secure connectivity, primarily to unserved and underserved areas in Central Asia, via satellite provided by the EU private sector.
- **IRIS²**, the new secure satellite-based connectivity component of the EU's Space programme, will provide global coverage when the entire constellation will have been deployed. At an early stage, it will set up pilot projects in Sub-Saharan Africa.
- The **EU-ASEAN Sustainable Connectivity Team Europe Initiative** under the Global Gateway includes a digital component promoting the expansion of the Copernicus mirror site in the Philippines to further countries in ASEAN, including Indonesia and Thailand.

Emerging technologies

- **Artificial Intelligence:** As outlined in the AI Continent Action Plan³⁸, the EU will continue to engage bilaterally, regionally and multilaterally with trusted partners to attract

³⁸ [Communication on an AI Action Plan](#), COM(2025)165

investments in the EU, support the establishment of a global level playing field for trustworthy AI, and to promote the good governance of AI globally. The EU will also act decisively to establish itself as a frontrunner in applying AI to science for its own competitiveness and to attract top scientists to Choose Europe³⁹. The EU will further seek cooperation with trusted partners, notably on innovation-related aspects of AI, such as the deployment of AI Factories outside the EU and their connection to the network of EU AI Factories. Such cooperation will also include providing access to AI models and algorithms, in particular on projects relating to AI for the Public Good (e.g. tackling climate change and supporting clean transition, improving healthcare or agriculture). This cooperation will also leverage EU public and commercial satellite data and services to enhance AI-driven solutions for global challenges, such as environmental monitoring and disaster response. Given the dual-use nature of some AI applications, the EU will continue to work on the role of Artificial Intelligence in the Common Foreign & Security Policy (CFSP) and Common Security and Defence Policy (CSDP), working with Member States to ensure that the EU's CFSP and CSDP are able to profit from the technological advances of AI.

- **5G/6G:** The EU is the global innovation leader in advanced connectivity, such as 5G and fixed network solutions. The objective to reach common standards for the next generation sustainable by design (6G) requires cooperation with like-minded countries, starting with research and innovation cooperation and standardization. The main challenge is the development and choice of 6G technologies, notably Radio Access Network technologies, including integration of terrestrial and non-terrestrial networks. EU industry can lead 6G development in line with EU standards notably on cybersecurity, interoperability and compliance with legal access standards and will benefit from cooperation with countries having complementary strengths in the value chain, including microelectronics, devices, cloud or AI.
- **Semiconductors:** Geopolitical uncertainty and the growing complexity of semiconductor supply chains demand a tailored, country-specific approach, ensuring that the EU partners with global leaders of the semiconductor ecosystem while safeguarding its own technological, economic and security interests. The EU will continue engaging with countries where collaboration in areas like pre-competitive research and development and supply chain resilience is mutually beneficial. In line with the Economic Security strategy⁴⁰, the EU will also defend its economic security interests, including through bilateral, regional and multilateral engagement, encouraging information sharing to prevent supply chain disruptions, mitigating risks, and attracting global talents to address the skills gap in the European semiconductor ecosystem.
- **Quantum technologies:** Advancing common standards and applications in quantum technologies demands robust international collaboration, particularly in research and innovation. The EU will strengthen ties with countries that offer complementary strengths in the quantum technology value chain, including computing, sensing, communication, post-quantum safe encryption, and related fields on a reciprocal basis. The EU remains attentive to the role of quantum technologies in the future security landscape and maintains regular contact with NATO and other relevant partners in the field. The EU will join forces with partner countries on concrete applications of quantum technologies in sectoral policies, for example to develop new materials.

Examples of forthcoming actions in the field of **emerging technologies**:

³⁹ [Choose Europe: advance your research career in the EU](#)

⁴⁰ Communication on a European Economic Security Strategy, COM(2023) 20 final

- The EU will implement joint research and innovation projects in Quantum technologies with **Japan, the Republic of Korea and Canada**.
- As part of the **EU-India Trade and Technology Council**, the EU and India are working on developing a dedicated programme that will facilitate talent exchanges and foster semiconductor skills among students and young professionals.
- In the context of the EU-LAC Digital Alliance, the EU will 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.
- The EU will follow up on the commitments of the **EU-African Union Ministerial Meeting** (May 2025), to work together to develop regional innovation ecosystems, establishment of AI strategies and digital governance frameworks.
- The EU will support the deployment of **AI Factories** in trusted partner countries, supporting them with developing their compute infrastructure while also securely connecting them to the EU and its AI Factories ecosystem.
- The EU will work with Member States to outline areas where **Artificial Intelligence** can support the implementation of the Common Foreign & Security Policy and Common Security and Defence Policy.
- The EU will continue to support **defence innovation** through the **EU Defence Innovation Scheme (EUDIS)** and will explore ways to enhance collaboration with Ukraine in this domain.
- The EU will, in close dialogue with trusted partners such as Norway and Ukraine, explore new ways for supporting synergies with the Hub for European Defence Innovation (HEDI).

Cybersecurity

In today's hyper-connected world and evolving geopolitical landscape, cyber threats from state and non-state actors do not stop at the borders. A cyber-attack or incident in one country can cripple businesses and infrastructure worldwide, and our citizens and businesses rely on digital products and solutions from third countries. Strengthening cybersecurity and cyber defence, including the capacity to detect, prepare for and response to cybersecurity threats and incidents, and enhancing information sharing on cyber threats with international partners to improve response time and resilience, is a direct investment in the EU's own security. Nowhere is this truer than in the EU's neighbourhood, where the EU is fully committed to supporting enlargement countries to ramp up their cybersecurity and cyber defence capabilities.

The EU also has the tools to lead at a global scale on cybersecurity. With the Cyber Resilience Act⁴¹, the EU is setting a new standard for secure-by-design products. As countries worldwide seek to secure their supply chains, the EU's expertise in product security offers a powerful foundation for international partnerships. In a similar vein, as the EU's global partners are investing into securing their critical infrastructures, market opportunities arise in areas where the EU has strong European industrial leadership such as cryptography and highly secure digital products.

With its strong impact on businesses and hospitals, ransomware remains a global scourge, one that no single country can combat alone. In line with the ProtectEU Strategy, the EU will push for stronger international cooperation to take down the infrastructure that ransom groups rely

⁴¹ Regulation (EU)2024 2847

on, break their financial lifelines, ensure more efficient sanctions against perpetrators and facilitators, and bring the cybercriminals to justice.

As part of these efforts, the EU will also promote enhanced cyber resilience in sectors increasingly reliant on digital technologies, such as transport and smart mobility, where secure infrastructure, data and services are essential to ensure operational continuity and public trust.

Recent efforts have ensured that candidate countries that are associated to the Digital Europe Programme would be able to access the EU-level Cybersecurity Reserve established by the Cyber Solidarity Act⁴². In addition, the European Union Agency for Cybersecurity, ENISA, will continue cybersecurity cooperation with relevant third countries, including capacity building in candidate and Neighbourhood countries.

Examples of forthcoming actions in the field of **cybersecurity**:

- The EU will work with relevant partners to explore the potential for **mutual recognition agreements** regarding the Cyber Resilience Act and respective frameworks of the partners to facilitate compliance with product cybersecurity requirements.
- The EU will continue cooperating with partner countries to enhance global cyber resilience and contribute to a free, open, safe and secure cyberspace. Firmly anchored in the Global Gateway strategy, cybersecurity and **cyber capacity-building** support will focus on securing critical infrastructures, and strengthening cyber ecosystems, including through the development and implementation of relevant regulatory and policy frameworks, as well as cyber hygiene and literacy.
- 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 accepted norms of state conduct in peacetime, developing confidence-building measures, and supporting states in building the capacity to implement these framework elements.
- The EU will reinforce its attribution of **cyber-attacks** to malicious actors, including state-based actors, and continue to develop the associated **sanctions mechanisms**.

Foreign Information Manipulation and Interference (FIMI)

Together with its partners, the EU will also better protect citizens from Foreign Information Manipulation and Interference (FIMI) campaigns or other societal risks stemming from online platforms. To do so, ensuring algorithmic transparency in how content is recommended and moderated is essential to enhance accountability and public trust.

This is also relevant for candidate, potential candidate and neighbourhood countries, in view of their specific vulnerabilities to disinformation and foreign interference and will in turn allow to strengthen our mutual resilience, including democratic resilience.

Examples of forthcoming actions in the field of **FIMI**:

- Following an expansion of its work on attributing cyber-attacks to defined actors, the EU will expand the **attribution of incidents** of FIMI.

⁴² Regulation (EU)2021 694

Digital identities and Digital Public Infrastructure (DPI)

The EU's experience in developing open-source digital identity wallets and secure and data protection compliant Digital Public Infrastructure offers significant value beyond EU borders. International cooperation and mutual recognition arrangements with key partners can simplify cross-border business for companies and facilitate citizens' mobility. The EU will notably continue to pursue cooperation with third countries (such as Ukraine, Moldova, the Western Balkans, Japan, India, Egypt) to achieve seamless cross-border usage of trust services. It will also promote the European Interoperability Framework⁴³ to help partner countries with fostering administrative modernisation and cross-border digital integration, including aligning with EU standards and practices. The EU will continue to promote the use of common specifications and open standards to ensure interoperability, transparency, and reuse.⁴⁴

Examples of forthcoming actions in the field of secure Digital Public Infrastructure:

- The EU will support the development of **trust services and digital identity solutions** (based on the EU Digital Identity Wallet specifications), putting them at the core of an interoperable and scalable suite of digital building blocks and solutions, including open-source ones, to support the digital transformation of public administrations and businesses of partner countries. The EU will also continue its work with Ukraine, Moldova and the Western Balkans, to prepare for their gradual integration with the EU Digital Identity Wallet.
- The EU will be cooperating with countries such as India, Egypt, Uruguay and Brazil in the area of **e-signatures and DPI interoperability**, with the view of creating benefits for businesses and citizens both in the EU and in partner countries.
- The EU will support an **interoperability-by-default** approach, based on the European Interoperability Framework, to facilitate seamless exchange of data across borders.
- The EU will continue to work with key international partners (Japan, India, Singapore, Australia, New Zealand, Malaysia) to promote the EU model for **eInvoicing**, based on the European eInvoicing standard and interoperable technical specifications.

Online platforms

The EU's Digital Services Act⁴⁵ protects democracy, free speech, privacy, the safety and security of children online, and provides a secure framework for the sale of legally compliant goods. The Digital Markets Act⁴⁶ and EU competition policy promote the contestability of digital markets, a level playing field and fair competition between digital players. These acts complement the protection provided in the digital environment by the GDPR⁴⁷ and consumer protection laws.

The protection and empowerment of minors online is a global priority. Under the Digital Services Act, all online platforms have to ensure a high level of privacy, safety, and security of

⁴³ Part of the Communication on a European Interoperability Framework – Implementation Strategy, COM(2017) 134

⁴⁴ A relevant example is the [Data Catalogue Vocabulary Application Profile](#), which has become a de facto standard, which facilitates harmonised metadata descriptions and seamless data sharing across borders.

⁴⁵ Regulation (EU)2022 2065 and amending Directive(2000) 31 EC (Digital Services Act) (OJ L 277, 27.10.2022).

⁴⁶ Regulation (EU)2020 1828

⁴⁷ Regulation (EU) 2016/679

minors, on their service. In addition, the largest online platforms must annually assess and mitigate any systemic risks that their services pose – including for the respect of the rights of the child and the protection of minors more generally. The Digital Services Act is supported and complemented by the Better Internet for Kids Strategy (BIK+). In particular, the EU co-funds the network of hotlines in Member States to tackle the dissemination of child sexual abuse material online. Global cooperation is ensured via the INHOPE network with 55 hotlines operating worldwide.

Strong and consistent consumer protection across online marketplaces is another priority the EU shares with many of its international partners and a key issue addressed by the Digital Services Act, as well as consumer protection and product safety frameworks. Under the Digital Services Act all online marketplaces are required to meet strong standards for safety, transparency and accountability to ensure that illegal and unsafe products cannot be sold to EU consumers through their services. The 2025 Communication on e-commerce⁴⁸ complements this by setting out new actions to address challenges linked to the surge of unsafe, counterfeit and otherwise illicit products sold through online platforms. The EU will prioritise cooperation with partner countries and in multilateral fora to find joint solutions to common risks to consumer safety stemming from online marketplaces.

Examples of forthcoming actions in the field of **online platforms**:

- The EU will continue to promote its regulatory approach and its underlying principles bilaterally and multilaterally and share its experience in implementing them.
- The EU will organise **regional events** with international organisations, third-country legislators, regulators and civil society to promote freedom of expression and safety online.

5. GLOBAL DIGITAL GOVERNANCE

To advance its goals in the digital domain, the EU will continue to pursue a **multilateral and multi-stakeholder approach** and ensure meaningful participation of relevant stakeholders including civil society, academia and the private sector, building on the strong existing ties with partner countries.

The EU's Digital Partnerships and Dialogues allow for **coordination** ahead of discussion in multilateral and regional fora, building strong coalitions in pursuit of shared objectives in key international fora and organisations, such as the United Nations, G7, G20, OECD and the Council of Europe, as well as global Internet Governance institutions. In particular, with G7 partners, the EU will continue to promote the development and uptake of **Economic Security Standards** – including when relevant for digital technologies – taking into account various criteria such as transparency, diversification of supply, security, sustainability, trustworthiness and reliability.

The **Global Digital Compact** (GDC) of the United Nations was adopted by consensus as the first comprehensive framework for global digital governance. It sets out the objectives, principles, commitments and actions to develop an open, free and secure digital future for all. The EU will remain actively involved in the GDC implementation work to defend its

⁴⁸ A comprehensive EU toolbox for safe and sustainable e-commerce, COM(2025) 37 final

achievements, while ensuring non-duplication of efforts and maximizing synergies with the existing global digital architecture, including the Internet Governance framework.

In addition to these processes, the EU will focus on **standardisation** as a key tool to advance its goals. The EU has strengths to rely on, including a strong research and innovation base, world-leading tech companies and many innovative SMEs and start-ups that need to be encouraged to take part in international standards setting. By leveraging on the EU standardisation system to increase its influence in international standards setting for key digital technologies, the EU aims to strengthen the competitiveness of its industry, foster digital and tech sovereignty, and protect and promote its fundamental values and interests while pursuing international cooperation in standard setting. The EU acknowledges the important role of the ITU in the context of global standardisation.

The EU will also continue to defend a rules-based, equitable allocation of **radiofrequencies** under the global framework of the International Telecommunication Union (ITU), acknowledging that the radio spectrum is a scarce natural resource that underpins all wireless digital applications.

Multilateral cooperation is also crucial to address the digital aspects of other sectors, including the energy sector due to the rapidly increasing energy demand of AI. The EU is engaged in **international energy initiatives**, like the Clean Energy Ministerial, which develop collaborative approaches to meet these challenges.

As digital technologies continue to evolve rapidly, **global Internet Governance** must adapt to new geopolitical challenges, such as fragmentation risks, increased misuse of digital tools for practices such as Internet shutdowns and censorship and widening digital divides. Moreover, the transition towards **Web 4.0** – driven by core technologies like artificial intelligence, extended and virtual reality, blockchain, and quantum computing – introduces new governance complexities that require updated, effective, and inclusive multi-stakeholder frameworks. The EU will continue to shape the inclusive multi-stakeholder approach to Internet Governance and is committed continuously to improve its effectiveness, opposing initiatives for state-controlled Internet architectures that could fragment and undermine the openness and security that have characterised the Internet since the Tunis Agenda⁴⁹.

The EU will continue to proactively defend the general availability and integrity of the Internet as a global, interoperable network of networks, reflecting the importance of the multi-stakeholder model of internet governance, for example in the upcoming editions of the Internet Governance Forum (IGF) and World Summit on the Information Society 20-year review (**WSIS+20**) negotiations. The EU acknowledges the central role of ICANN in managing the foundations of the Internet architecture.

Examples of forthcoming actions in the field of **global digital governance**:

- The EU will work to ensure **proper** follow-up and review of the implementation of the **Global Digital Compact (GDC)** commitments.
- The EU will work as Team Europe to ensure a suitable outcome to the **World Summit on the Information Society (WSIS+20) Review** negotiations.

⁴⁹ [Tunis agenda for the Information Society](#), 18 November 2005

- 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 and security.

6. A COMPETITIVE AND SECURE EUROPE, OPEN FOR BUSINESS, CONNECTED TO THE WORLD

In a volatile world, the EU is a consistent, predictable and reliable partner. In the context of complex tech value chains, no country or region can advance on the digital and AI revolution alone. The EU's internal and external efforts on digital policy are closely intertwined and mutually-reinforcing. That is why the EU is not only boosting its own digital sector, from AI Factories to defence tech, but is also concluding substantial partnerships that bring visible benefits for the EU's citizens and businesses and for our partners.

As a champion of multilateral solutions to global challenges, the EU is a steadfast supporter of the UN, G7, G20, OECD and other bodies that enable us to tackle together the defining challenges of our time.

The EU is ready to join forces for new, deeper, and flexible forms of cooperation nurturing mutually beneficial partnerships, to reinforce Europe's competitiveness and security. The EU will continue to engage constructively based on respect for the international rules-based order.