European technological sovereignty and digital infrastructure

1. Definition and state of play of technological sovereignty

We understand technological sovereignty as:

- Having regard to the European Declaration on Digital Rights and Principles for the Digital Decade, which commits "to promote a European way for the digital transformation, putting people at the centre; Calls EU institutions to take concrete steps to uphold these ambitions both within the EU as in the Union's cooperation with third countries
- Building capacities, resilience and thus security for citizens and companies by reducing strategic dependencies.
- Preventing strategic dependencies on foreign actors. Reducing reliance on single provider. Building partnerships with trusted third countries and entities.
- Concept of openness and interoperability to ensure that Europe remains an attractive hub for investment, while safeguarding critical technologies.
- Technological sovereignty should be seen as the whole value chain from excellence in research to creating better competition and reaching a better European sovereignty.
- Enhancing industrial policy to boost domestic R&D and manufacturing capacities in strategic technologies, including semiconductors, AI and cybersecurity.
- Developing a comprehensive risk assessment framework for dependencies on hardware and software elements of digital infrastructure;
- To that regard, Europe needs a comprehensive technology model encompassing, in particular, hardware, AI systems, data and governance, ensuring secure digital future grounded in European values.
- Recognizing the increasing concentration of power in non-European companies, particularly in cloud infrastructure, semiconductors, and AI platforms, which constrains Europe's ability to innovate, compete, and maintain control over its digital economy, society, and democracy.
- Recognizing that European firms contribute a minor share to global R&D in software, internet technologies, and electronics, while the US and China lead in these sectors;
- Noticing the energy consumption challenges in AI, cloud and quantum computing, and data centres requiring integrating sustainability into digital infrastructure strategies;
- Recognizes the European Commission's Digital Compass, Digital Decade Policy Program, and Competitiveness Compass as essential frameworks for strengthening Europe's digital ecosystem, securing technological leadership, and ensuring long-term economic resilience;
- Recognizing that a comprehensive industrial policy for digital ecosystem is needed, integrating all relevant policy domains such as market access, standardization, research and development, , investment, trade and international cooperation Calls the European Commission to establish a European Digital Industrial Policy to promote a resilient and sustainable, trust-worthy and safe digital ecosystem that drives innovation and ensure that the development, deployment, and use of new and existing technologies adhere to European values.
- Points to the digital solutions created by the EU such as EU Digital identity that can offer innovative infrastructure to the EU's digital economy.

2. Digital infrastructure

We understand digital infrastructure as:

- composed of hardware elements related to connectivity, including fibre, 5G and 6G, submarine cables, satellites and spectrum, and computing, including semiconductors, data centres, HPCs, quantum technologies, and software elements including identity solutions, IoT, cloud and AI systems, as well as the intermediation layer including advertising, search, payments and communication systems;
- Recognises the strategic importance of critical digital infrastructure; sees the need to enhance security and resilience for them; critical digital infrastructure include, but not limited to, cables (terrestrial and submarine), cellular network towers, satellite communication systems, spectrum and radio equipment, cloud servers containing sensitive information and data centres processing sensitive information; some software elements include security software protecting critical networks and data centres.
- The EU's competitiveness will increasingly depend on the digitalisation of all sectors, supported by resilient, safe and trustworthy digital infrastructure. In this context, the Digital Single Market is a vital asset since it can enable companies to grow and scale up.
- Recognizes the full potential of the Digital Single Market remains untapped, with intra-EU trade in digital services represents just 8% of GDP, significantly lower than the 25% for trade in digital goods;
- Calls on the European Commission, while preparing future legislative proposals, to concentrate on the single market dimension, in line with the recommendation made in Enrico Letta's report "Much more than a market" and in Mario Draghi's report "The future of European competitiveness", with an aim to un-tap the potential of the Digital Single Market;
- Takes note of the recommendations set in the two (Draghi's and Letta's) reports that the EU needs a paradigm shift from promoting connectivity in the EU towards establishing a single market in electronic communications and connectivity;
- Welcomes the Commission's White Paper on How to master Europe's digital infrastructure needs which outlines 3 pillars: Creating the "3C Network" - "Connected Collaborative Computing"; Completing the Digital Single Market; and Secure and resilient digital infrastructures for Europe.
- Sees the White Paper and subsequent consultation process as part of the preparation of the legislative initiative planned for this term; Calls the Commission to take, in this process, a more holistic view on the digital infrastructure and acknowledge that the digital infrastructure encompasses numerous elements beyond pure connectivity; Underlines the need to accompany any new digital policy measure by an impact assessment.

2.1. We need high-speed connectivity

- The upcoming Digital Networks Act must support the objective to provide all EU consumers with high-quality connectivity by 2030, especially in remote and rural areas, as well as removing administrative barriers s for the rollout of 5G, 6G and secure, high-speed broadband;
- Calls for an introduction of EU Cloud and AI Development Act to strengthen European data infrastructure and the promotion of European cloud providers and ensure secure data sharing while adhering to GDPR.

- Fibre
  - Welcomes the introduction of the Gigabit Act, which responds to the growing needs for faster, reliable, data-intensive connectivity; sees the importance of sharing use of ducts and poles for deploying very high-capacity networks to optimise resources and reduce costs; Urges Member States to streamline permitting processes and harmonize regulations to lower financial and administrative barriers for expansion of fibre infrastructure.
  - Stresses the importance of accelerating the deployment of fiber-optic networks and modern wireless communications systems that can deliver fast, secure and reliable digital services; underlines that fiber-optic networks form one of the backbones of EU's digital infrastructure, enabling high-speed internet, 5G networks, and future technological improvements.
  - The EU is behind on the rollout of 5G to meet the 2030 targets, with still limited fibre coverage of only about 64% of European households being included. Prioritizing direct fiber connections for homes, businesses, and public institutions is crucial to ensure ultra-fast and reliable connectivity, in addition to network rollouts with public works such as roads, water, electricity to streamline fiber rollout
- 5G and 6G
  - Believes that private investments are essential for deployment of electronic communication networks, 5G and 6G that are advanced enough in terms of transmission, speed, storage capacity, edge computing power, and interoperability.
  - Enforcement and implementation of the Gigabit Infrastructure Act is further necessary in a creation of One-Stop-Shop for Permits, a centralized digital permitting process to reduce delays in infrastructure deployment and ensuring uniform rules for infrastructure access, pricing, and environmental impact assessments, therefore we call for strong efforts in this area.
  - European Union needs to have a strong cybersecurity protection in all critical infrastructure sectors, with stricter measures to de-risk high-risk vendors in 5G and 6G networks, ensuring dense deployment of small cells and macro towers, particularly in urban and rural areas with inconsistent coverage and ensuring the infrastructure is sustainable and energy-efficient to support Europe's global competitiveness in the digital economy
- Spectrum
  - Notes that investment needs in the state of the art connectivity in the EU are immense; Therefore, calls on Member States and the Commission to work on an enhanced coordination of spectrum allocations, in particular by earlier identification and harmonisation of the release of new frequencies, starting with 6G frequencies Calls for a radio spectrum policy that promotes investment in Europe. This includes harmonising spectrum assignment policies across Member States to accelerate 5G deployment based on best practices, promoting longer license durations, and access to new spectrum such as the upper 6GHz band to meet future demand and enable 6G.
- Satellites and satellite communications systems
  - Recognises the EU GOVSATCOM initiative, which aims at ensuring long-term availability of secure, reliable and cost-effective governmental satellite communication services for

EU and national public authorities managing security critical infrastructures and missions.

- Underlines the importance of satellite-based communications, to increase the resilience and develop capacities of EU's digital infrastructure and EU actors, and reduce dependencies on non-EU providers, specifically in defence., and provide alternative connectivity solutions for consumers in remote and rural areas
- Calls for increased progress on Ariane 6; stresses the importance of private sector involvement in launcher technologies to further accelerate the deployment of IRIS2;
- Notes that there are several issues with latency in satellite networks today and recognizes that the integration of satellite networks with 5G and in future 6G technologies is pivotal in extending the reach and reliability of terrestrial networks;

2.2 We need collaborative connectivity and computing ecosystems:

- <u>High-performance computing (HPC) systems:</u>
  - Recognizes the progress made in the recent years in enhancing high performance computing; calls on the European Commission for the continuous integration and enhancement of computing power at EU High-Performance Computing (HPC) centres to enhance the training of AI models and prepare for future advancements in supercomputing;
  - Calls on the European Commission to develop a coordinated strategy to bridge the gap between Europe's cutting-edge HPC technology and its practical, scalable deployment across industries;
  - Notes that these strategy shall foster collaboration between public institutions, private sector partners, including SMEs, to ensure that Europe's HPC capabilities become a key driver of economic competitiveness and technological sovereignty;
- <u>Hardware for computing: semiconductors, chips and quantum chips</u>
  - Recognizes that chips play a crucial role in increasing the technological competitiveness and resilience of Europe and sees the need to further enhance Europe's role in the supply chain of semiconductors.
  - Notes the current EU efforts, namely European Chips Act, in pushing for more EU self-reliance in semiconductor production, nevertheless recognizes that these efforts are not sufficient due to the increasing role of these chips in technological advancements, economic growth, and national security.
  - Urgent action is needed to boost EU domestic semiconductor manufacturing, improving supply chain resilience by forming strategic global partnerships, encouraging start-ups and innovation; fostering cross-border collaboration in advanced semiconductor development and by providing financial incentives, regulatory support, and market access.
  - Emphasizing the need for legal certainty to support semiconductor development, ensuring secure supply chains for critical raw materials and avoiding disruptions caused by investment uncertainties.
  - Urges to give utmost political importance to ensuring a sufficient supply of AI chips in European Union and to make it a focal point of EU digital industry policies. Notes the increase of for AI chips driven by expanding applications in cloud computing, edge devices, autonomous systems, and generative AI;

- Calls on the Commission to find a negotiated solution to the US ban on export of AI chips to 16 EU Member States.
- Calls on the Commission to put advanced AI chips, including their design and production, at the core of the revision of the Chips Act. Renew new: Calls on the Commission to come with this revision during this year, which is earlier than envisaged in the Chips Act, as there is a need for EU to react and move faster than expected.
- Recognizing that processors, memory technologies, GPUs, and quantum chips are critical to Europe's digital infrastructure and supply chain security;
- Believes that EU should enhance its efforts on quantum chips development if the EU is to accelerate the time-to-market for EU industrial innovation in quantum technology;

- Importance of Cloud
  - Recognizes that cloud services are fundamental to a wide range of computational activities;
  - Calls for a strategy for reducing reliance on foreign cloud providers while fostering European alternatives; Notes the need to secure data storage and computational power, and distributed computing infrastructures;
  - Calls on the European Commission to leverage initiatives like 8ra and the IPCEI CIS to advance decentralized cloud and edge infrastructure, reducing reliance on foreign providers and ensuring resilience while enhancing operational flexibility within Europe;
- AI systems
  - Welcomes the InvestAI initiative, including the AI gig factories; emphasises that this large-scale AI infrastructure is essential for enabling open, collaborative development of the most complex AI models;
  - Emphasises the need for Europe to position itself as a global leader in AI model training, scientific research and quantum computing advancements; Is committed to further supporting AI development by launching initiatives such as AI Factories to provide computing power for start-ups, scale-ups and researchers.
- Quantum technologies/quantum computing
  - Recognizes the urgency of defining a clear roadmap for quantum technology development, including quantum computing and quantum encryption, ensuring that public and private investments lead to tangible commercial applications
  - Calls on the Commission to do an assessment of existing national quantum sandbox frameworks and how existing legislation applies to them. to prevent market fragmentation; welcomes the announcement of the Quantum Strategy and Quantum Act in the European Commission's Competitiveness Compass.
  - Urges the European Commission to ensure the Quantum Act, accompanied by an impact assessment, delivers tangible technological applications by fostering policies that accelerate technological maturity and facilitate the transition from research to commercial success;
  - Calls for targeted investments, industry collaboration, and regulatory frameworks that support the development, scaling, and market adoption of quantum technologies across key sectors;

- Calls for a coordinated EU strategy for post-quantum cryptography to protect data from future cyber threats.

- Data centres:
  - Notes that data centers are an essential part of an advanced digital society, enablers of distributed processing and effective data storage; trusted capacity and availability of data storage is essential for European resilience and development. Notes that building and operating large-scale data centers requires substantial investment;
  - Reminds of Commission's plan to make data centers climate-neutral and highly energy efficient by 2030, bearing in mind that around 9 % of electricity global consumption is produced by data centers, cloud services and connectivity;
  - There is a need to improve integration of data centers with the energy system, focusing on heat reuse and providing flexibility services to the electricity grid needs; Recognizes a need to incentivize research for cooling and energy-efficient processors, while special attention should be given to supporting EU data centers
  - Calls the European Commission to support ecosystems for sharing industry-specific data within industrial sectors, fostering collaboration and driving innovation, while maintaining data sovereignty and ensuring compliance with European regulations, as outlined in the Data Act. Urges the Commission for strong enforcement to ensure that dominant market players to not impose unfair terms on SMEs and mid-sized enterprises when accessing and sharing data;
  - Believes that there is a need to ensure interconnected infrastructure that would allow data centers to work together efficiently under common standards with high-speed connectivity while flexibility, security, and scalability would be maintained. This interconnected system would help in ensuring distributed redundancy so that data and services remain available even in the event of a data center failure.'
  - Calls the European Commission to prioritize interoperability across platforms, allowing seamless integration of data across businesses and sectors, in alignment with the requirements of the Data Act, which mandate data portability and interoperability obligations for cloud and edge services. Stresses the need for robust enforcement of these provisions to prevent vendor lock-in and ensure that European industrial ecosystems can leverage data-driven innovation without technical or contractual barriers;

2.3. We need secure and resilient digital infrastructures in Europe:

- Submarine cables
  - Notes that submarine cables are critical infrastructure for global connectivity, economic stability and security; points out that submarine cables remain vulnerable to physical damage, cyber threats and geopolitical risks; stresses that submarine cables carry over 99% of international communications through them.
  - Calls on the Commission to take coordinated action to protect submarine cables reinforce cable security and repair capabilities; Stresses the need for continued investments in the construction of new submarine cables to ensure redundancy; welcomes the EU's role in co-financing such projects to enhance digital infrastructure and connectivity across Member States. Calls on the Commission to explore potential synergies between maintaining digital and energy undersea infrastructures

- Emphasises the importance of improving the EU's and Member States repair capabilities and response mechanisms for submarine cable disruptions is essential to maintain secure and interrupted communications.
- Calls on the Commission to promote R&I to enable advance technological innovations in cable security, including early warning systems and AI-driven threat assessments.
- Urges the Commission to review available instruments designed to better leverage private investments to support Cable Projects of European Interest (CPEIs); Calls on the Commission to include submarine cables projects in the Important Projects of Common European Interest (IPCEI); Recognizes the need to streamline and simplify the application and administrative process governing IPCEIs.
- Underlines the importance of international cooperation to repair cables that have been sabotaged and facilitating necessary investments.
- Calls on the Commission for an assessment of regulatory measures to ensure fair access and security, no matter if these infrastructures are privately or publicly owned;
- Welcomes the adoption of the Action Plan on cable security, that will be organised around 4 pillars: prevention, detection, response & repair and deterrence.

- Cybersecurity rules fit for current geopolitical situation
  - Underlines the importance of secure and resilient digital infrastructure, particularly considering the increasing number of cyberattacks against the European Union, its Member States and its industry and society;
  - Recalls the legislative work done over last term that would significantly improve cybersecurity in the EU, in particular welcomes the adoption of the Cyber Resilience Act, the Cyber Solidarity Act and the NIS2 Directive; stresses the need for harmonized and timely implementation and enforcement of these measures
  - Calls on the Commission to present an evaluation report on Cybersecurity Act, and to propose a legislative act to review this act with a particular focus on strengthening the mandate of the European Union Agency for Cybersecurity (ENISA) and accelerating the adoption process of European cybersecurity certification schemes.
  - Emphasizing the importance of the upcoming European Internal Security Strategy in strengthening cybersecurity and critical infrastructure protection.

- Application of Toolbox on 5G cybersecurity
  - Calls for the full implementation of the EU Toolbox on 5G Security to reduce reliance on high-risk vendors; notes that EU Toolbox on 5G Security is important to prevent cyber espionage and strengthen the resilience of supply chains in EU's digital infrastructure.
  - Notes with concern that, according to the Second report on Member States' Progress in implementing the EU Toolbox on 5G Cybersecurity, 14 Member States have yet to implement any restrictions on high-risk suppliers, posing significant security vulnerabilities.
  - Calls on the Commission to make the 5G toolbox binding, specifically with regards to high-risk vendors in critical infrastructure;

3. To achieve these we need:

- Active capacity building in critical areas
  - In order to strengthen digital infrastructure, it is essential to implement capacity-building initiatives at the EU level in critical areas. These initiatives should focus on developing a foundational layer of public infrastructure, such as a network of AI Gigafactories and European Web Indexation model. This layer will empower companies to develop their business models and ensure data sovereignty.

- Standardisation
  - Believes that the importance of standards is growing in view of increasing technological competition across the world, most notably from the US and China
  - Is of strong view that promoting interoperability and EU standards is paramount to foster competitiveness in technology sector as it ensures products can connect and work together, fostering innovation and open markets; recalls that both interoperability and common technological standards pave the way for the functioning of the Single Market.

- Research and Innovation
  - Fostering a supportive regulatory environment that encourages innovation, investment and the development of cutting-edge technologies in Europe.