# TOWARDS A SOCIALLY ACCEPTED AND SUSTAINABLE 6G

*November 2025*

## Policy Brief on Securing Europe's Technological Sovereignty in 6G

Lucas Pereira Carwile
Carmela Occhipinti

6G4SOCIETY

CyberSocial Lab.

# 1. Highlights

Europe's technological sovereignty in sixth-generation (6G) mobile network is at risk. Current analysis shows that Europe still produces only around 10% of the world's semi-conductors and remains highly dependent on imports for many critical digital technologies [1], while leading-edge chips are manufactured entirely outside European borders [2], [3]. The global telecommunications equipment market is dominated by a small number of large suppliers – especially Huawei, Ericsson, and Nokia – creating oligopoly conditions that limit European strategic choices and increase vulnerability to supply-chain disruptions [4].

While citizen surveys revealed concerns about Europe's competitive position, network reliability, and dependence on external actors, expert consultations with Smart Networks and Services Joint Undertaking (SNS JU) projects confirmed six critical vulnerabilities requiring policy intervention: supply chain dependencies in critical components, fragmentation of global standards processes, risks of foreign government access to European infrastructure, integration with critical sectors creating cascading failure risks, regulatory fragmentation across Member States, and insufficient European capacity for independent technical assessment. These findings underscore that 6G's success depends not only on technological performance but on ensuring Europe can design, deploy, and govern networks in line with its democratic values while maintaining security and economic competitiveness.

Against this backdrop, this brief proposes examines the following question:

**HOW CAN EUROPE DEVELOP TECHNOLOGICAL SOVEREIGNTY FOR 6G THAT STRENGTHENS SECURITY, EMBEDS EUROPEAN VALUES, AND MAINTAINS GLOBAL INTEROPERABILITY WITHOUT RESORTING TO TECHNOLOGICAL ISOLATION?**

It proposes six priority recommendations:

- 1. **Strengthen supply chain resilience** through targeted investment in European capacity for semiconductors, software, and manufacturing equipment while maintaining cooperation with trusted partners;
- 2. **Build European governance capacity** for independent 6G technical assessment, reducing dependence on vendor expertise for critical security and sovereignty decisions;
- 3. **Coordinate European positions** in global standards bodies to embed privacy, transparency, and democratic governance principles in technical specifications from the outset;
- 4. **Enhance protections** against foreign government access and interference through strengthened security frameworks adapted for AI-native, cloud-based 6G architectures;
- 5. **Harmonise Member State approaches** to vendor security, spectrum allocation, and deployment requirements, eliminating vulnerabilities created by regulatory fragmentation;
- 6. **Develop specialised expertise** for 6G governance through training programs, research support, and capacity building enabling effective democratic oversight.

# 2.Context of the Issue

The debate on technological sovereignty has intensified following the COVID-19 pandemic, supply chain disruptions, and rising geopolitical tensions that exposed **Europe's deep dependencies on foreign technologies** for connectivity, cloud services, and semiconductors. In response, the European Union updated its Industrial Strategy and embraced the concept of "**open strategic autonomy**", seeking to reduce critical dependencies while remaining engaged in global cooperation, maintaining interoperability, and supporting standards-based development [5].

Unlike previous mobile generations that primarily served communications, 6G is being designed as **AI-native infrastructure deeply integrated with critical sectors** including energy, transportation, healthcare, and financial systems. This integration creates novel **vulnerabilities** where foreign control over components or data flows could enable economic coercion, espionage, or disruption of essential services.

Europe has established instruments [6] including the EU Chips Act, the 5G Security Toolbox [7], the NIS2 Directive [8], and STEP to address sovereignty concerns [9]. However, **significant gaps** remain: comprehensive supply chain mapping for 6G components, sufficient regulatory expertise to govern AI-native networks, coordinated European strategy in global standards bodies, frameworks addressing foreign interference in cloud-based architectures, harmonised Member State security approaches, and integrated critical infrastructure resilience mechanisms.

Analysis within 6G4Society reveals that while citizens rarely used "technological sovereignty" terminology, they expressed **concerns about Europe's competitive position, dependence on external actors, network reliability, and regulatory lag**. Expert consultations with SNS JU projects confirmed these concerns operationally: **geopolitical competition** risks fragmenting 6G into incompatible regional standards, with governance models embedded in technical specifications shaping how rights and security are distributed [10].

Experts emphasised that sovereignty means retaining **capacity to embed European values** (e.g., transparency, privacy, democratic governance) in 6G design while balancing innovation needs with regulatory safeguards [10].

Within this context, technological sovereignty for 6G encompasses Europe's capacity to make **autonomous, democratically accountable decisions** about 6G development and governance while remaining interoperable and globally engaged. It operates across **industrial capacity** (semiconductors, software, equipment, security autonomy (preventing foreign control, maintaining verification capability), and **value integration** (embedding European commitments to rights, privacy, transparency in technical design). This aligns with the EU's "open strategic autonomy" approach, distinguishing European sovereignty from close, nationalist strategies that risk fragmentation and isolation [5].

# 3. Policy Recommendations

Aligning 6G with Europe's vision of technological sovereignty requires coordinated action across six interconnected areas, from supply chain resilience to specialised governance expertise.

## R1 Strengthen 6G supply chain resilience and critical industrial capacity

Europe's reliance on non-European suppliers for advanced semiconductors, manufacturing equipment, and key software components creates vulnerabilities to supply disruptions, geopolitical tensions, and strategic dependencies that could compromise autonomous decision-making. While the EU Chips Act [11] and IPCEI mechanisms [12] address strategic dependencies in semiconductors and microelectronics generally, and mapping exercises have identified 137 products in sensitive ecosystems with high external dependencies [13], these efforts have not yet been extended to the specific requirements of 6G networks. The telecommunications sector requires **dedicated supply chain resilience frameworks** that address 6G-specific components including RF equipment, AI accelerators for network intelligence, and software-defined networking infrastructure. Building European capabilities while maintaining cooperation with **trusted partners** enables strategic autonomy without technological isolation. Recommended policy options:

- To mitigate the risk of heavy dependence on external suppliers, adopt **a coordinated 6G governance framework**, aligning Member State policies and fostering a diverse industrial ecosystem that **links innovation with sovereignty.**
- Regulation should clarify accountability and liability across complex, multi-vendor systems, supported by **independent certification and transparent reporting.**
- Foster public trust enforcing clear responsibility, openness, and citizen engagement, to ensure that connectivity remains a public good, not a private monopoly.
- Embed **cooperation with democratic partners and empower communities** through transparency and inclusion, so that Europe can turn technological autonomy into a form of shared governance, achieving resilience not through isolation, but through fairness, openness, and collective trust in its digital future.

R2

## Build independent European governance capacity for 6G oversight

The complexity of AI-native, software-defined 6G networks will significantly exceed current regulatory expertise in most Member States. Existing EU bodies do provide important foundations: ENISA offers extensive technical guidance through the EU 5G Toolbox [14], 5G Threat Landscape [15] [16], 3GPP security guidance for regulators [17], and 5G Security Controls Matrix [18] while BEREC facilitates regulatory coordination and knowledge exchange through its 5G Radar [19] and associated reports [20]. The NIS Cooperation Group has established strategic cybersecurity coordination for 5G networks through the EU coordinated Risk Assessment and 5G Toolbox [21].

However, all these frameworks remain focused primarily on 5G, not the architectural transformations introduced by 6G, including native AI integration, distributed network intelligence, quantum-resistant cryptography, and software defined 6G architectures. European institutions – regulators, data protection authorities, and security agencies – currently lack specialised training in these areas, a gap confirmed by ENISA's cybersecurity skills reports and European Cybersecurity Skills framework [22][23]. This emerging capacity deficit risks undermining democratic oversight and increasing reliance on the very entities being regulated as 6G deployment approaches.

**Recommended policy options:**

- Develop a coordinated governance ecosystem for 6G that **combines expertise, oversight, and innovation.**
- Establish a governance hub to **train regulators and policymakers** in the technical, security, and sovereignty dimensions of next-generation networks.
- Create an **independent assessment capability** to analyse system vulnerabilities through research and public-private partnerships.
- Launch a governance innovation programme to **design democratic oversight models** suited to AI-driven, software-defined infrastructures.
- Support these efforts through **a knowledge-sharing and expertise-exchange platform** linking national authorities and European institutions, ensuring consistent understanding, accountability, and resilience across the 6G policy landscape.

## R3

## Lead in global 6G standards development to embed European values

While European companies are key participants in 3GPP, ITU, and ETSI standards processes [24], the EU still lacks a 6G-specific strategy for systematically translating its legal and ethical requirements into coordinated positions in these fora. The 2022 EU Strategy on Standardisation outlines a values-based approach and calls for stronger coordination, but it measures remain general and not tailored to 6G technical specifications [25]. Existing initiatives such as the EU Standardisation Booster provide project-level support, yet there is no dedicated long-term mechanism to sustain European expert leadership in 6G standardisation [26]. Civil-society organisations also note that current system provides limited venues for public-interest oversight, calling for more democratic governance of standardisation [27]. As major global actors explore separate 6G standards pathways, this lack of sustained support and oversight increases the risk that European legal and ethical requirements will not be fully reflected in future technical architectures [24]

- Establish a **standards leadership initiative with dedicated support for regional experts** to take leading roles in global 6G standards development.
- Create a **values-based standards framework** requiring that positions in international technical negotiations include human rights, privacy, and ethical impact assessments to ensure technology aligns with democratic principles.
- Implement a **reference implementation programme offering open-source** versions of proposed standards to demonstrate technical feasibility, encourage global uptake, and provide non-proprietary alternatives that foster openness and interoperability.

R4

## Enhance protections against foreign government access and interference

Existing frameworks including the 5G Security Toolbox and NIS2 Directive already provide common approaches to vendor risk assessment and cybersecurity obligations for 5G networks and other essential services [28] [8]. However, they were conceived for current generations of networks and do not yet systematically address the specific threat model of AI-native, cloud based 6G architectures – including large-scale virtualisation, pervasive remote-management functions and more complex software supply chains. The EU's coordinated 5G risk assessment and subsequent toolbox already highlight non-technical vulnerabilities, such as dependencies on suppliers subject to third-country laws and possible foreign interference through those suppliers.

In parallel, European case law and guidance on international data transfers, notably Schrems II and the EDPB's Guidelines on Article 48 GDPR, emphasise the systemic risk of foreign government access to data via extra-territorial legal orders [29], [30]. As 6G would become tightly integrated with critical infrastructures in sectors such as energy, transport, healthcare and finance, these combined technical and legal exposure points could enable not only surveillance, but also disruption of essential services if not proactively mitigated.

**Recommend policy options:**

- Reinforce the 5G Security Toolbox and NIS2 Directive implementation by explicitly **addressing foreign technical exploitation risks, including** supply chain vulnerabilities, covert data channels, or software backdoors, within a coordinated 6G security framework. Building on existing provisions on supplier risk Toolbox and third-country influence, these measures should be translated into clear, verifiable safeguards and certification schemes applicable across Member States.
- To guarantee coherence and oversight, the EU should strengthen ENISA's mandate under **the Cybersecurity Act,** or establish a joint coordination mechanism with **BEREC** and national authorities to manage certification, intelligence-sharing, and audits related to cybersecurity, foreign interference, and technological sovereignty in 6G networks.

## R5 Harmonize Member State approaches to 6G security and deployment

Despite common EU objectives, Member State implementation of the 5G Security Toolbox remains uneven. While a majority of countries are applying or preparing restrictions on high-risk vendors, others have not yet taken equivalent steps, and security aspects are still not addressed in a fully concerted manner across the Union [31], [32]. This fragmentation may create vulnerabilities that malicious actors can exploit, increases compliance costs for operators working across borders, and weakens overall European security. Differences in national approaches to spectrum assignment, vendor restrictions, and security obligations similarly undermine the coherence required for effective technological sovereignty in 6G [31].

- Strengthen technological sovereignty in 6G by transforming existing coordination into a **binding, coherent framework.** Building on current EU programmes, Member States should align decisions on security, vendors, and spectrum through a **formal consultation mechanism.**
- Evolve the 5G Security Toolbox into a **unified 6G security and resilience framework** with common vendor assessments and restrictions. Regulatory capacity should be reinforced, ensuring all authorities can **enforce standards.**
- Clear **accountability rules and a shared monitoring system** under the Digital Decade framework would prevent fragmentation and safeguard collective European resilience

## R6 Reinforce targeted research and coordinated policy support

Addressing technological sovereignty challenges requires both dedicated researches to develop evidence-based frameworks and systematic capacity building to enable implementation. Without coordinated support, European regulators and policymakers risk dependence on external expertise for critical decisions. The next EU research framework should include a dedicated CSA call equipping policymakers, regulators, and standards bodies with the evidence and operational capacity needed to act on these recommendations.

- Conduct **interdisciplinary research** on supply chain resilience, standards governance, security frameworks, and accountability in AI-native 6G architectures.
- Develop **EU guidance for telecommunications-specific** security certification, vendor assessment methodologies, and standards participation strategies.
- Produce **policy blueprints for sector-specific rules,** including codes of conduct and certification schemes for 6G service providers.
- Establish a European **6G governance hub** providing specialised training for regulators, policymakers, and data protection authorities.
- Strengthen EU's ability to independently **assess 6G technologies,** develop **governance expertise** and facilitate **structured knowledge exchange** with regulatory authorities.

# 4. Evidence and analysis

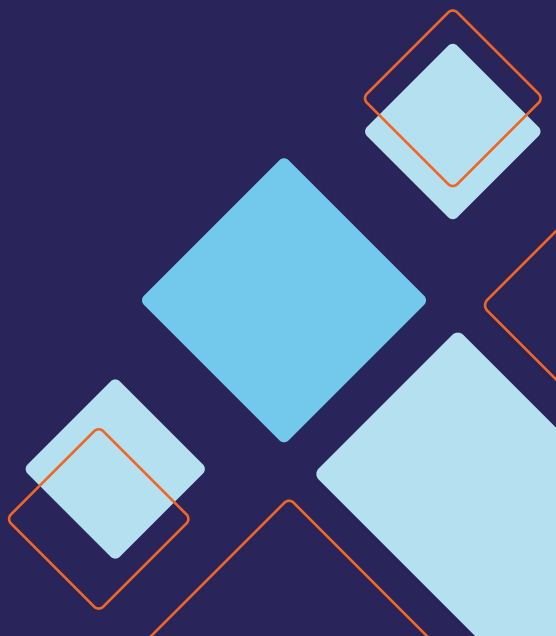
The project's findings are based on a triangulation of quantitative (surveys), qualitative (interviews and workshops), and desk-research methods, ensuring robustness and alignment between citizen, expert, and institutional viewpoints. Survey responses reflect the perceptions of participants rather than the full EU population, while evidence from SNS JU projects represents early-stage research rather than deployed infrastructures. Nevertheless, the extensive combination of scientific literature, citizen surveys, participatory workshops, interviews with industry practitioners and experts in acceptance, 6G, green ICT, smart cities and sustainability, as well as consultations with policymakers and engagement within the SNS JU community, provides complementary academic, civic, and institutional perspectives demonstrating where current frameworks require strengthening to align 6G development with European sovereignty objectives.

Desk research examined EU policy documents on industrial strategy, open strategic autonomy, cybersecurity, and digital regulation, tracing how European policy thinking evolved from viewing telecommunications primarily as market competition to treating digital infrastructure as strategic assets with direct implications for security, democracy, and economic resilience. Analysis of the EU Chips Act, 5G Security Toolbox, NIS2 Directive, and related frameworks revealed the gaps identified in this brief. Empirical engagement complemented this analysis. Citizen surveys revealed concerns about Europe's competitive position in digital infrastructure, dependence on external actors, network reliability, and regulatory capacity to keep pace with technological change. While citizens rarely used "technological sovereignty" terminology, their concerns about dependence, control, and lagging regulation reflect its underlying themes. Expert interviews with representatives from SNS JU projects confirmed these concerns operationally, highlighting vulnerability from reliance on foreign semiconductor and equipment suppliers, concentration of critical software and cloud services, accountability gaps in multi-vendor networks, and geopolitical dimensions of standards development where diverging regional strategies risk non-interoperable systems embedding different governance models.

These findings align with broader European analyses documenting high import dependence for critical digital technologies and uneven implementation of security frameworks across Member States Together, the desk research, citizen engagement, and expert consultations yield a consistent conclusion: technological sovereignty is not simply industrial policy but a practical prerequisite for ensuring 6G infrastructures can be governed in line with European law and values.

# 5. Sources

This policy brief synthetises findings from 6G4Society Deliverables D1.1 [33], D1.2 [34] and D1.3 [35], as well as WP2 and WP3 outputs on stakeholder engagement and liaison with the SNS JU community. It is framed within the wider EU policy context defined by the Updated Industrial Strategy (2021), the concept of open strategic autonomy, the EU Chips Act, the Digital Decade Policy Programme, the ENISA 5G Security Toolbox (ENISA, 2020), the NIS2 Directive, the Cybersecurity Act, Important Projects of Common European Interest (IPCEI), and the Strategic Technologies for Europe Platform (STEP).



# Bibliography


**[1]** European Comission, "Report on the state of the Digital Decade 2023," 2023.

**[2]** European Court of Auditors, SR-2025-12, "The EU's strategy for microchips," 2025.

**[3]** European Parliamentary Research Service (EPRS), "Strengthening EU chip capabilities. How will the chips act reinforce Europe's semiconductor sector by 2030.," 2022.

**[4]** "The Global RAN market stabilised in Q1 2025 thanks to North American sales.," telecoms.com, 05 2025. [Online]. Available: https://www.telecoms.com/telecoms-infrastructure/the-global-ran-market-stabilised-in-q1-2025-thanks-to-north-american-sales?. [Accessed 10 2025].

**[5]** European Commission, "Updated Industrial Strategy," 2021.

**[6]** European Court of Auditors, "The EU's strategy for microchips – reasonable progress in its implementation but the Chips Act is very unlikely to be sufficient to reach the overly ambitious Digital Decade target," European Court of Auditors, Luxembourg, 2025.

**[7]** European Commission, "Secure 5G deployment in the EU – Implementing the EU toolbox," European Commission, Brussels, 2020.

**[8]** "Directive (EU) 2022/2025 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972.," Official Journal of the European Union, vol. L333, pp. 80-152, 27 12 2022.

**[9]** "Regulation (EU) 2024/795 of the European Parliament and of the Council of 29 February 2024 establishing the Strategic Technologies for Europe Platform (STEP)," Offical Journal of Europe, vol. L229/1, 2024.

**[10]** 6G4Society, "D3.2 Position Paper. Social Acceptance of Technology," 2025.

**[11]** "Regulation (EU) 2023/1781 of the European Parliament and of the Council of 13 September 2023 establishing a framework of measures for strengthening Europe's semiconductor ecosystem and amending Regulation (EU) 2021/694 (Chips Act)," Official Journal of European Union, vol. L 229/1, 2023.

**[12]** European Commission, "Communication from the Commission – Criteria for analysis of the compatibility with the internal market of State aid to promote the exclusion of important projects of common European interest," Official Journal of the European Union, Brussels, 2021.

**[13]** M. Szczepanski, "Resilience of global supply chains: Challenges and solutions," European Parliament, Brussels, 2021.

**[14]** ENISA, "The EU toolbox for 5G security," 29 January 2020. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/eu-toolbox-5g-security.

**[15]** ENISA, "ENISA Threat Landscape for 5G Networks," ENISA, Heraklion, 2019.

# Bibliography


**[16]** ENISA, "ENISA Threat Landscape for 5G Networks – Updated Report," ENISA, Heraklion, 2020.

**[17]** ENISA, "Security in 5G Specifications: Controls in 3GPP," ENISA, Heraklion, 2021.

**[18]** ENISA, "5G Security Controls Matrix," ENISA, Heraklion, 2023.

**[19]** BEREC, "Guide to the BEREC 5G Radar and 5G Radar," BEREC, Riga, 2020.

**[20]** "Regulation (EU) 2018/1971 of the European Parliament and of the Council of 11 December 2018 establishing the Body of European Regulators for Electronic Communications (BEREC) and the Agency for Support for BEREC (BEREC Office)," Official Journal of European Union, vol. L 321/1, 2018.

**[21]** NIS Cooperation Group, "EU coordinated risk assessment of the cybersecurity of 5G networks," European Commission, Brussels, 2019.

**[22]** ENISA, "Cybersecurity Skills Framework (ECSF) – Role Profiles," ENISA, Heraklion, 2022.

**[23]** ENISA, "European Cybersecurity Skills Framework (ECSF) – User Manual," ENISA, Heraklion, 2022.

**[24]** 6G-IA, "European Vision for the 6G Network Ecosystem," 6G Smart Networks and Services Industry Association, Nov.2024, 2024.

**[25]** C. C. a. R. Atkinson, "Mapping the International 5G Standards Landscape and How it Impacts U.S. Strategy and Policy," Information Technology & Innovation Foundation, 2021.

**[26]** HSBooster.eu, "Horizon Standardisation Booster – Supporting Research Projects in Pre-Normative Activities," European Commission, 2023.

**[27]** BEUC – The European Consumer Organisation, "For a Standardisation Governance Act: Making standardisation more democratic, inclusive and aligned with policy goals," 2024.

**[28]** NIS Cooperation Group, "Cybersecurity of 5G networks – EU Toolbox of risk mitigating measures," European Commission, Brussels, 2020.

**[29]** Court of Justice of the European Union, "Data Protection Commissioner v Facebook Ireland and Maximillian Schrems (Schrems II), Case C-311/18," 2020.

**[30]** European Data Protection Board (EDPB), "Guidelines 02/2024 on Article 48 GDPR," 2024.

**[31]** European Court of Auditors, "5G roll-out in the EU: Delays in deployment of networks with security issues remaining unresolved," Luxembourg.

**[32]** European Commission, "Communication on the implementation of the EU Toolbox on 5G Cybersecurity," 2023.

**[33]** 6G4Society, "D1.1: Societal aspects in 6G technology: concerns, acceptance models and sustainability indicators," 2024.

**[34]** 6G4Society, "D1.2 Towards a Socially Accepted and Sustainable 6G – Policy Brief.," 2025.

**[35]** 6G4Society, "D1.3 Towards a Socially Accepted and Sustainable 6G – Operational Brief.," 2025.

# Contact

For further information, contact


**https://cybersoclab.com**
eu-projects@cybersoclab.com


**6G4Society Website**
www.6g4society.eu

Project deliverables are publicly available through the **6G4Society Zenodo repository:**
https://zenodo.org/communities/6g4society


This work was supported by the 6G4SOCIETY project (Grant Agreement No. 101139070), which has received funding from the European Union's Horizon Europe research and innovation programme.


CyberSocialLab.