6G4SOCIETY

TOWARDS A SOCIALLY ACCEPTED AND SUSTAINABLE 6G

November 2025

Operational Brief on Securing Europe's Technological Sovereignty in 6G

Carmela Occhipinti
Lucas Pereira Carwile

CyberSocial Lab.

1. Highlights

Europe's technological sovereignty in sixth-generation (6G) mobile network faces increasing risks. Current analysis shows that Europe still produces only around 10% of the world's semiconductors 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 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:

- Strengthen supply chain resilience through diversification, transparency mechanisms such as Software Bills of Materials (SBOM), and investment in European capacity;
- Build internal expertise for independent 6G technical assessment, reducing dependence on vendor expertise for critical decisions;
- Lead in global standards bodies to embed European values in technical specifications through active participation in 3rd Generation Partnership Project (3GPP), O-RAN Alliance, and European Telecommunications Standards Institute (ETSI);
- Harden systems against foreign government access and interference through zero-trust architectures and supply chain attestation;
- Align with harmonised European approaches to security, certification, and deployment requirements;
- Contribute to sovereignty-focused research, certification frameworks, and governance capacity building.

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.

The technical architecture of 6G introduces specific sovereignty challenges that industry must address. Cloud-native, software-defined network functions mean that critical operations depend on software supply chains spanning multiple jurisdictions, making Software Bill of Materials (SBOM) tracking essential for transparency. AI-native optimisation implies the need for large-scale data processing that may traverse non-European infrastructure, demanding clear data localisation and sovereignty-aware orchestration. Open RAN disaggregation, while offering vendor diversity and reducing lock-in, also distributes trust across more component interfaces, requiring robust multi-vendor accountability frameworks. Integrated sensing and communication (ISAC) capabilities generate sensitive geolocation and environmental data that becomes a strategic asset requiring protection. Each of these architectural shifts demands corresponding operational responses that go beyond current practice. 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 in areas directly relevant to industry practice: comprehensive supply chain mapping for 6G components, sufficient regulatory expertise to govern AI-native networks, coordinated European participation in global standards bodies, frameworks addressing foreign interference in cloud-based architectures, harmonised security approaches across Member States, 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. For industry, this operates across three dimensions: **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 closed, nationalist strategies that risk fragmentation and isolation [5].

TECHNOLOGICAL SOVEREIGNTY

3.Operational Recommendations

Aligning 6G deployment with Europe's vision of technological sovereignty implies the need for industry action across six interconnected areas. The following recommendations translate strategic sovereignty objectives into concrete operational practices for network operators, equipment vendors, and infrastructure developers.

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. Operational options are:

1. **Implement supply chain transparency through Software Bill of Materials (SBOM):** Generate and maintain SBOMs for all critical software components using standardised formats (SPDX, CycloneDX) [14] [15] as anticipated under NIS2 and the Cyber Resilience Act. Integrate SBOM tracking into CI/CD pipelines to enable automated vulnerability scanning against databases such as the National Vulnerability Database (NVD). Require SBOM documentation from all software suppliers and maintain a centralised repository enabling rapid impact assessment when new vulnerabilities emerge.

2. **Adopt Open RAN architectures to reduce vendor lock-in:** Deploy Hardware Security Modules (HSMs) for cryptographic key management and secure boot processes. Require Trusted Platform Module (TPM) attestation for critical network elements to verify firmware integrity. Where feasible, evaluate open hardware architectures (e.g., RISC-V) and European chip designs emerging from EU Chips Act Investments to reduce dependency on proprietary instruction set architectures.

3. **Document accountability across multi-vendor deployments:** Create component-level responsibility matrices mapping each network function to its supplier, maintainer, and security contact. Establish incident response protocols that span vendor boundaries with pre-agreed escalation paths and communication channels. Maintain provenance documentation enabling rapid determination of which vendor is accountable for any given failure or vulnerability.

4. **Integrate supplier risk scoring into procurement:** Develop vendor risk assessment frameworks that evaluate geopolitical exposure, jurisdictional risks, supply chain depth, and historical security performance. Weight sovereignty considerations alongside price and technical performance in procurement decisions. Prioritise suppliers from democratic, rule-of-law jurisdictions and build relationships with emerging European suppliers, including SMEs supported through IPCEI and Horizon Europe programmes.

5. **Communicate supply chain practices transparently:** Publish annual supply chain transparency reports documenting diversification efforts, SBOM coverage, and vendor risk assessments. Engage with regulators and stakeholders on sovereignty practices. Contribute supply chain data to European coordination mechanisms where appropriate.

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: The European Union Agency for Cybersecurity (ENISA) offers extensive technical guidance through the EU 5G Toolbox [16], 5G Threat Landscape [17] [18], 3GPP security guidance for regulators [19], and 5G Security Controls Matrix [20] while the Body of European Regulators for Electronic Communications (BEREC) facilitates regulatory coordination and knowledge exchange through its 5G Radar [21] and associated reports [22]. The NIS Cooperation Group has established strategic cybersecurity coordination for 5G networks through the EU coordinated Risk Assessment and 5G Toolbox [23].

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 have limited specialised training in these areas, a gap confirmed by ENISA's cybersecurity skills reports and European Cybersecurity Skills framework [24][25]. This emerging capacity deficit risks undermining democratic oversight and increasing reliance on the very entities being regulated as 6G deployment approaches.

Operational options are:

Implement AI transparency and documentation practices: Maintain comprehensive documentation for all AI systems used in network management and optimization, including model cards specifying training data provenance, performance characteristics, known limitations, and intended use cases. Adopt explainable AI (XAI) techniques where feasible to enable meaningful human oversight of automated network decisions. Document AI model versioning, update procedures, and rollback capabilities to support external review.

Build internal expertise on 6G architectural transformations: Develop staff competencies in the specific technologies that differentiate 6G from previous generations: software-defined networking (SDN) and network function virtualization (NFV), RAN Intelligent Controllers (RIC) and O-RAN architectures, AI/ML model lifecycle management, and post-quantum cryptography (PQC) migration paths. Create dedicated roles responsible for sovereignty and governance considerations in technical decisions. Ensure engineering teams understand how architectural choices affect auditability, accountability, and democratic oversight.

Prepare for post-quantum cryptography transitions: Monitor National Institute of Standards and Technology (NIST) Post-Quantum Cryptography (PQC) standardisation and begin inventory of cryptographic dependencies across network infrastructure. Develop migration roadmaps for transitioning to quantum-resistant algorithms (e.g., ML-KEM, ML-DSA, SLH-DSA) [26] [27] [28] in key management, authentication, and secure communications. Engage with ETSI Quantum-Safe Cryptography working group and relevant 3GPP study items.

Enable independent verification and audit: Design network architectures with auditability as a first-class requirement. Provide comprehensive technical documentation enabling regulator review, including architecture diagrams, data flow mappings, and security control implementations. Support external audits and third-party security assessments. Implement logging and monitoring systems that create verifiable audit trails for critical network operations and AI-driven decisions.

Contribute to regulatory capacity building: Participate actively in regulator training initiatives and knowledge exchange programmes. Share technical expertise with national regulatory authorities, data protection authorities, and ENISA. Contribute to developing sector-specific guidance that bridges the gap between 5G-focused frameworks and 6G architectural realities. Offer secondment opportunities or technical briefings to build regulator understanding.

Experiment with participatory oversight mechanisms: Pilot new approaches to stakeholder engagement in technical decisions affecting communities. Test mechanisms for incorporating public input on deployment choices, particularly for sensitive applications such as sensing and positioning. Document and share learnings on democratic oversight models with industry peers and regulators.

3. Operational Recommendations

R3 Lead in global 6G standards development to embed European values

While European companies are key participants in 3GPP, ITU, and ETSI standards processes [29], 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 its measures remain general and not tailored to 6G technical specifications [30]. 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 [31]. Civil-society organisations also note that the current system provides limited venues for public-interest oversight, calling for more democratic governance of standardisation [32]. 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 [29]. Operational options are:

Commit sustained resources to strategic standards and participation: Dedicate expert staff to key standards bodies shaping 6G architecture: 3GPP RAN and SA working groups (particularly SA1 for service requirements, SA2 for architecture, SA3 for security, SA5 for management), ITU-T Study Group 13 (Future Networks) and Focus Group on Network 2030, and ETSI groups on NFV, MEC (Multi-access Edge Computing), and Reconfigurable Intelligent Surfaces. Support European candidates for leadership positions (working group chairs, rapporteurs) in these bodies. Coordinate positions with European industry peers through 6G-IA and SNS JU mechanisms to present unified European perspectives.

3. Operational Recommendations

Translate European values into concrete technical contributions: Develop standards contributions that operationalise European requirements in technical specifications. Privacy-by-design principles should inform proposals on data minimisation in network signalling, consent mechanisms for sensing data, and anonymisation requirements for network analytics. Transparency requirements should shape proposals on AI model documentation, algorithm auditability hooks, and explainability interfaces. Security-by-design should drive contributions on zero-trust architecture patterns, supply chain attestation protocols, and quantum-resistant security frameworks. Document the values-to-specifications mapping to enable consistent advocacy across working groups.

Contribute to and leverage open-source reference implementations: Support open-source projects that demonstrate European standards contributions in working code: O-RAN Software Community (OSC) for RAN disaggregation, ONAP (Open Network Automation Platform) for network orchestration, OpenAirInterface for 5G/6G protocol stacks, and the Sylva project for European telco cloud infrastructure [33]. Contribute to engineering resources, code, and testing to these communities. Use open-source implementations to validate technical feasibility of European proposals before standardisation, strengthening negotiating positions with demonstrated implementations.

Engage actively with O-RAN Alliance technical development: Participate in O-RAN Alliance working groups, particularly WG1 (Use Cases), WG2 (Non-RT RIC), WG3 (Near-RT RIC), and WG4 (Open Fronthaul), to ensure open interfaces support European sovereignty and security requirements. Contribute to O-RAN security specifications and advocate for privacy preserving approaches in RAN Intelligent Controller (RIC) applications. Engage with O-RAN ALLIANCE's 6G Research Group to shape the evolution of open architectures toward next-generation networks.

Build coalitions for European positions: Coordinate with European industry peers, research institutions, and SNS JU projects to develop shared positions before major standards meetings. Engage with like-minded international partners (e.g., through EU-US Trade and Technology Council, EU-Japan, and EU-Korea digital partnerships) to build broader coalitions supporting interoperable, values-aligned standards. Participate in 6G-IA working groups and policy discussions to align industry positions with European strategic objectives.

Monitor and report on standards developments with sovereignty implications: Track standards proposals from all major contributors that could affect European sovereignty, security, or values integration. Assess implications of competing proposals for European interests and flag concerns through appropriate coordination channels. Report to European coordination mechanisms on standards developments requiring policy attention.

3. Operational Recommendations

3. Operational Recommendations

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 [34] [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 [35][36]. 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. Operational options are:

1. **Implement zero-trust architecture principles:** Design network architectures assuming breach, requiring continuous verification of all users, devices, and network functions regardless of location or prior authentication. Implement micro-segmentation to limit lateral movement within networks. Apply least-privilege access controls to all management interfaces, APIs, and inter-component communications. Deploy identity-aware proxies and software-defined perimeters for all remote access, eliminating implicit trust based on network location.

2. **Deploy confidential computing for sensitive workloads:** Utilise Trusted Execution Environments (TEEs) such as Intel SGX, AMD SEV, or Arm CCA [37] [38] [39] [40] to protect sensitive data and processes even from privileged systems administrators or compromised hypervisors. Implement confidential computing for subscriber data processing, key management, and AI model inference where network intelligence operates on sensitive inputs. Ensure that data remains encrypted during processing, not only at rest and in transit, to mitigate risks from foreign access to physical infrastructure or cloud platforms.

3. **Establish cryptographic supply chain attestation:** Implement code signing for all software components, firmware, and configuration updates using European-controlled certificate authorities where feasible. Deploy secure boot chains with hardware roots of trust (TPM, HSM) to verify integrity from power-on through application loading. Require cryptographic attestation from suppliers demonstrating software provenance, build environment integrity, and absence of tampering. Verify attestations automatically before deploying updates to production systems.

4. **Harden against covert exploitation and exfiltration:** Conduct security assessments specifically targeting supply chain risks, including analysis of third-party libraries and dependencies for hidden functionality. Implement mandatory code review and static/dynamic analysis for all critical software, with particular attention to network-facing components and management interfaces. Deploy network traffic analysis and AI-driven anomaly detection to identify covert data channels, beaconing behaviour, or unauthorised command-and-control communications. Test for steganographic exfiltration and protocol-level covert channels.

5. **Implement sovereignty-aware data routing and processing:** Design orchestration systems to enforce data localisation policies, ensuring sensitive data categories remain within European jurisdiction unless explicitly authorised. Implement policy engines that automatically route workloads to sovereignty-compliant infrastructure. Maintain real-time visibility into data flows across the network, enabling rapid identification and remediation of policy violations. Apply encryption with European-held keys for any data that must transit non-European infrastructure.

6

Engage actively with European security coordination: Participate in ENISA-led security initiatives, including threat intelligence sharing through the EU Cybersecurity information and Intelligence Sharing Network: Contribute to NIS Cooperation Group activities and national CSIRT coordination. Support coordinated vulnerability disclosure and incident response across European operators. Engage with the European Cybersecurity Competence Centre (ECCC) and national coordination centres on emerging threats specific to 6G architectures.

R5 Harmonise 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 [41] [42]. 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 [41]. Industry can play a constructive role in driving harmonisation by implementing consistent practices that exceed minimum requirements and demonstrating the feasibility of unified approaches.
Operational options are:

1

Align security implementations with EU Cybersecurity Certification Framework: Prepare for and pursue certification under emerging European cybersecurity certification schemes, including EUCC (Common Criteria-based), EUCS (cloud services), and anticipated 6G-specific schemes. Implement security controls aligned with ENISA's 5G Security Controls Matrix as a baseline, extending coverage to 6G-specific architectural elements as guidance evolves. Where operating across multiple Member States, pursue certifications recognised Union-wide to reduce duplication and demonstrate consistent security posture. Engage with ENISA and national certification authorities during scheme development to ensure practical implementability.

2

Implement uniform security standards across all EU operations: Apply the highest applicable security standards across all Member State operations rather than calibrating to minimum local requirements. Develop internal security baselines that meet or exceed the most stringent national implementation of EU frameworks. Document security architectures, controls, and processes in standardised formats enabling cross-border consistency verification by regulators. Maintain centralised security governance with local compliance validation to ensure uniform implementation.

3

Ensure network slicing isolation meets cross-border requirements: Implement cryptographic isolation between network slices to guarantee that security properties are maintained as slices traverse national boundaries. Apply consistent slice security policies regardless of which Member State's infrastructure hosts specific slice components. Deploy slice-aware security monitoring that maintains visibility across distributed slice deployments. Document slice isolation mechanisms and security guarantees to enable regulatory verification in all jurisdictions where slices operate.

4

Harmonise spectrum usage and interference management: Coordinate spectrum utilisation practices with operators in adjacent Member States to prevent cross-border interference, particularly for new 6G spectrum bands. Implement dynamic spectrum sharing mechanisms that respect harmonised European spectrum assignments. Participate in CEPT and RSPG processes to support coordinated European spectrum policy. Deploy spectrum monitoring and interference detection capabilities that support cross-border coordination.

5

Contribute actively to harmonisation processes: Engage constructively with national regulators, sharing technical expertise to support consistent implementation of EU frameworks. Participate in NIS Cooperation Group consultations, ENISA working groups, and BEREC initiatives developing harmonised approaches. Provide implementation experience and practical feedback to European bodies developing 6G security guidance. Support peer learning among regulators by facilitating cross-border regulatory dialogues and technical exchanges.

6

Report transparently on sovereignty and harmonisation metrics: Provide data supporting Digital Decade monitoring and European sovereignty assessments. Document and publish key sovereignty-relevant metrics: supply chain European content, certification status, cross-border security consistency, and standards participation. Contribute to industry-wide benchmarking initiatives that demonstrate collective progress on harmonisation. Track and report on implementation of 5G Security Toolbox measures and readiness for 6G-specific requirements.

SECURING EUROPE'S TECHNOLOGICAL SOVEREIGNTY

R6 Reinforce targeted research and coordinated policy support

Addressing technological sovereignty challenges requires both dedicated research to develop evidence-based frameworks and systematic capacity building to enable implementation. Without coordinated support, European regulators and technology providers risk approaches that fail to achieve collective sovereignty objectives. Industry engagement with research initiatives, governance development, and European digital infrastructure projects is essential to translate sovereignty principles into operational reality. Active participation in these ecosystems also positions European industry to shape emerging frameworks rather than merely comply with them. Operational options are:

1

Engage with European cloud and infrastructure sovereignty initiatives: Participate actively in Gaia-X federation services development, contributing to specifications for sovereign cloud interoperability and data exchange [43]. Engage with IPCEI-CIS (Important Project of Common European Interest on Cloud Infrastructure and Services) projects to support development of European cloud capabilities. Adopt and contribute to the Sylva project, the European open-source telco cloud stack, to reduce dependence on non-European cloud platforms for network function hosting. Evaluate European cloud providers aligned with sovereignty requirements for non-critical workloads as a pathway to broader adoption.

2

Contribute to sovereignty-focused research programmes: Partner with universities and research institutions on sovereignty-relevant research, including supply chain resilience, AI governance for networks, and post-quantum cryptography migration. Participate in SNS JU research projects addressing sovereignty dimensions of 6G architecture. Enable research access to relevant operational data (appropriately anonymised) and infrastructure for academic investigations. Contribute practical industry expertise to Horizon Europe projects examining technological sovereignty, ensuring research outputs are operationally relevant.

3

Develop and implement Key Value Indicators (KVIs) for sovereignty: Integrate sovereignty-related KVIs into internal performance measurement alongside traditional technical KPIs. Track metrics such as European supply chain content, data localisation compliance, certification coverage, standards body participation, and open-source contribution. Use KVI frameworks emerging from SNS JU projects (including 6G4Society) to benchmark sovereignty performance and identify improvement priorities. Report on KVIs transparently to demonstrate industry commitment to European sovereignty objectives.

4

Utilise European testbeds for sovereignty-compliant validation: Leverage SNS JU experimental facilities and national 6G testbeds to validate sovereignty-compliant architectures before production deployment. Test supply chain transparency mechanisms, data localisation enforcement, and cross-border security consistency in controlled environments. Use digital twin technologies to model sovereignty implications of architectural choices. Share testbed learnings with European research community and standard bodies to inform specification development.

5

Prepare proactively for emerging certification requirements: Align internal security and sovereignty practices with anticipated EU cybersecurity certification criteria (EUCC, EUCS, potential 6G-specific schemes). Participate in certification framework development through ENISA consultations and stakeholder processes. Conduct gap assessments against draft certification requirements and develop remediation roadmaps. Support standardised approaches to security and sovereignty verification that enable mutual recognition across Member States.

6

Contribute to European governance capacity building: Participate in training and knowledge-exchange initiatives organised by ENISA, 6G-IA, and national competent authorities. Contribute industry perspective to governance development, ensuring operational feasibility of proposed requirements. Support secondment programmes and technical briefings that build regulator understanding of 6G technologies. Engage with the European Cybersecurity Competence Centre (ECCC) and national coordination centres on sovereignty-related research and training priorities.

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 combination of methods provides complementary academic, civic, and institutional perspectives demonstrating where current frameworks require strengthening and where industry action can address sovereignty gaps. **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, particularly the absence of 6G-specific guidance on supply chain transparency, AI-native network governance, and sovereignty-aware architecture design.

Citizen surveys revealed that **concerns related to technological sovereignty,** while not always expressed in those terms, rank among public priorities for future connectivity. Participants expressed concerns about Europe's competitive position in digital infrastructure, dependence on external actors, network reliability, and regulatory capacity to keep pace with technological change. Citizens highlighted Europe lagging behind China and the US in global competition, the dominance of a small number of large telecommunications providers, and slower legislative response than technology requires. These concerns highlight public expectations that European industry will take proactive steps to strengthen sovereignty, not merely await regulatory mandates.

Expert consultations within SNS JU projects achieved approximately 80% coverage of the ecosystem, through 63 survey responses and targeted interviews with project members and technical leads. These consultations confirmed citizen concerns operationally, highlighting: vulnerability from reliance on foreign semiconductor and equipment suppliers; concentration of critical software and cloud services in non-European hands; accountability gaps in multi-vendor networks; and geopolitical dimensions of standards development, where diverging regional strategies risk non-interoperable systems embedding different governance models. Experts emphasised that sovereignty requires not only policy frameworks but concrete industry practices, supply chain transparency, European cloud adoption, active standards participation, and architectural choices that preserve auditability and democratic oversight. 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 evidence yields 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, and industry action is essential to achieving it.**

5. Sources

This operational brief synthesises findings from 6G4Society project's deliverables D1.1 [44], D1.2 [45], 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 Cyber Resilience Act, the NIS2 Directive, the Cybersecurity Act.

Technical and operational guidance draws on: the ENISA 5G Security Toolbox and 5G Security Controls Matrix; EU Cybersecurity Certification Framework (EUCC, EUCS); 3GPP security specifications; O-RAN Alliance security and architecture specifications [46]; NIST Post-Quantum Cryptography standards; and Gaia-X federation services documentation. Industry initiatives referenced include the O-RAN Software Community (OSC), ONAP, OpenAirInterface, and the Sylva European telco cloud project. European coordination mechanisms include IPCEI-CIS, the European Cybersecurity Competence Centre (ECCC), 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] NTIA, “The Minimum Elements For a Software Bill of Materials (SBOM),” 2021.
[15] CISA , “Software Bill of Materials,” 2024.

Bibliography

[16] ENISA, “The EU toolbox for 5G security,” 29 January 2020. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/eu-toolbox-5g-security.
[17] ENISA, “ENISA Threat Landscape for 5G Networks,” ENISA, Heraklion, 2019.
[18] ENISA, “ENISA Threat Landscape for 5G Networks – Updated Report,” ENISA, Heraklion, 2020.
[19] ENISA, “Security in 5G Specifications: Controls in 3GPP,” ENISA, Heraklion, 2021.
[20] ENISA, “5G Security Controls Matrix,” ENISA, Heraklion, 2023.
[21] BEREC, “Guide to the BEREC 5G Radar and 5G Radar,” BEREC, Riga, 2020.
[22] “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.
[23] NIS Cooperation Group, “EU coordinated risk assessment of the cybersecurity of 5G networks,” European Commission, Brussels, 2019.
[24] ENISA, “Cybersecurity Skills Framework (ECSF) – Role Profiles,” ENISA, Heraklion, 2022.
[25] ENISA, “European Cybersecurity Skills Framework (ECSF) – User Manual,” ENISA, Heraklion, 2022.
[26] NIST, FIPS 203 "Module-Lattice-Based Key-Encapsulation Mechanism Standard", https://csrc.nist.gov/pubs/fips/203/final, 2024.
[27] NIST, FIPS 204 "Module-Lattice-Based Digital Signature Standard", https://csrc.nist.gov/pubs/fips/204/final, 2024.
[28] NIST, FIPS 205 "Stateless Hash-Based Digital Signature Standard", https://csrc.nist.gov/pubs/fips/205/final, 2024.
[29] 6G-IA, “European Vision for the 6G Network Ecosystem,” 6G Smart Networks and Services Industry Association, Nov.2024, 2024.
[30] 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.
[31] HSBooster.eu, “Horizon Standardisation Booster – Supporting Research Projects in Pre-Normative Activities,” European Commission, 2023.
[32] BEUC – The European Consumer Organisation, “For a Standardisation Governance Act: Making standardisation more democratic, inclusive and aligned with policy goals,” 2024.

Bibliography

[33] Linux Foundation Europe, Sylva: A European Telco Cloud Stack, 2024.
[34] NIS Cooperation Group, "Cybersecurity of 5G networks – EU Toolbox of risk mitigating measures," European Commission, Brussels, 2020.
[35] Court of Justice of the European Union, "Data Protection Commissioner v Facebook Ireland and Maximillian Schrems (Schrems II), Case C-311/18," 2020.
[36] European Data Protection Board (EDPB), "Guidelines 02/2024 on Article 48 GDPR," 2024.
[37] Confidential Computing Consortium, A Technical Analysis of Confidential Computing, 2021.
[38] Intel Corporation , Intel® Software Guard Extensions Developer Reference for Linux* OS, https://www.intel.com/content/www/us/en/developer/tools/software-guard-extensions/library.html, 2020.
[39] AMD, AMD Secure Encrypted Virtualization (SEV)-SNP API Specification v1.58, https://www.amd.com/en/developer/sev.html , 2025.
[40] Arm Limited , Arm Confidential Compute Architecture (CCA) Security Model., Available at: arm.com/architecture/security, 2024.
[41] European Court of Auditors, "5G roll-out in the EU: Delays in deployment of networks with security issues remaining unresolved," Luxembourg.
[42] European Commission, "Communication on the implementation of the EU Toolbox on 5G Cybersecurity," 2023.
[43] Gaia-X European Association for Data and Cloud, "Gaia-X Architecture Document – 24.04 Release," 2024. [Online]. Available: https://docs.gaia-x.eu/technical-committee/architecture-document/24.04/.
[44] 6G4Society, "D1.1: Societal aspects in 6G technology: concerns, acceptance models and sustainability indicators," 2024.
[45] 6G4Society, "D1.2 Towards a Socially Accepted and Sustainable 6G – Policy Brief.," 2025.
[46] O-RAN Alliance, O-RAN Architecture Description, O-RAN.WG1.OAD-R003-v10.00, 2024.
[47] 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.