POLICY REPORT

The European Centre for Economic Security, Technology and Resilience - ECESTR

UNLOCKING 6G'S NEXT FRONTIER:

FROM 5G LESSONS TO A REDESIGNED STANDARDS PLAYBOOK.

Standardisation, Supply-Chain Trust, and Transatlantic Implementation

Francesco Cappelletti & Dr Raluca Csernatoni

BRUSSELS, MARCH 2026

This policy report is to be accompanied by a Technical Working Paper providing detailed methodology, data, models, and case studies.

CONTENTS:

EXECUTIVE SUMMARY

The 6G Window Is Open — But Closing

The sixth-generation network for mobile communications is not simply about achieving faster connectivity; it serves as the foundational infrastructure for artificial intelligence-driven systems that will operate autonomously and are expected to support essential functions across energy networks, transport systems, healthcare, and industrial automation. 6G is also a geopolitical issue. It should consequently come as no surprise that it will influence the geopolitical landscape, shaping who controls the future digital order.

Decisions made today—within forums such as the 3rd Generation Partnership Project (3GPP) working groups and the International Telecommunication Union (ITU), which are bodies that play a key role in the development and deployment of telecommunication standards, and supply-chain procurement processes—will determine whether European companies in 2032 oversee networks they played a part in designing, or instead manage standards and infrastructure whose security, vendor dependencies, and artificial intelligence governance frameworks are influenced by external forces.

The study items within 3GPP Release 20, which is the step where the global telecom community finishes improving 5G and starts formally designing 6G—addressing AI-native architecture, security-by-design, spectrum assumptions, and sensing integration—will form the foundation for the subsequent specifications in Release 21, expected between 2027 and 2029. 3GPP Release 21 is where 6G moves from ideas into actual, binding technical standards. Once these decisions are finalised, reversing them would not only pose substantial technical difficulties but also entail complex political, contractual, and financial challenges.

The experience with 5G—characterised by costly rip-and-replace operations, inconsistent security implementations across Member States, and delayed transitions to standalone architecture—demonstrates that retrofitting remains possible but is often prohibitively expensive. In the case of 6G, the window for correction narrows significantly, and the stakes are markedly higher. Because 6G embeds AI autonomy into network control functions, post-hoc correction becomes not only costly but also epistemically opaque—regulators may be unable to determine what requires correction.

This report is built on a distinction the European debate has consistently failed to make: leadership in standards development—specifically, the shaping of technical specifications negotiated within 3GPP—is categorically different from leadership in standards deployment. Confusing these roles has historically limited Europe's influence across successive generations of networks.

The report contends that the principal barriers to European leadership in standards are not fundamentally technical. Europe is well-equipped, with leading contributors to the development of standards for mobile communication, world-class research institutions, and a robust regulatory framework. What it lacks, however, is a sufficient recognition of the critical role that respect for intellectual property rights, both within the EU and internationally, plays in sustaining EU leadership in standards. This point should be clearly reflected in the EU's broader 6G strategy.

Three structural measures are vital: mandating security-by-design as a requirement within 3GPP, harmonising spectrum allocations ahead of WRC-27, and establishing a predictable policy environment during the critical period of 2025-2027, which includes stable intellectual property regimes.

While transatlantic cooperation can enhance Europe's influence, it cannot replace internal cohesion. Without it, the risk is a gradual strategic decline—networks built on standards Europe did not influence, governed by architectures it did not shape, and sustained by supply chains it has failed to diversify.
This trajectory, which the report terms 'technological museumification,' would see past achievements preserved while authority over future infrastructure is gradually ceded to actors whose priorities diverge from those of the European Union.

This report also highlights four architectural decisions where European influence remains possible but is constrained by time. These include spectrum-band harmonisation prior to WRC-27, the scope of Open RAN interoperability in Release 20, core-security conformance requirements before the Stage 2 freeze in September 2026, and the guiding principles for integrating AI/ML in Releases 20 and 21.

Key Concepts Used in This Report

Standards development leadership

pertains to active influence over the technical specifications negotiated within organisations such as 3GPP and ITU-R—proposing architectures, contributing to work items, and shaping the foundational assumptions that underpin subsequent compromises. True leadership is reflected in the depth, originality, and strategic importance of technical contributions, not in crude proxies such as participant counts or the sheer volume of Standard Essential Patent (SEP) portfolios.

If EU companies do not lead in the development of 6G, Europe will ultimately become dependent on standards built on non-EU technologies.

Standards deployment leadership

refers to the speed and extent to which standardised technologies are embraced within domestic networks, including coverage, densification, service maturity, and vertical integration. Delayed deployment prevents the EU and its industry from fully leveraging advanced connectivity, weakening their global competitiveness.

Success in deployment for one generation does not automatically translate into standards influence in the next; each requires different approaches and timelines.

Technological museumification

describes a governance failure in which a jurisdiction preserves its past technological achievements—vendor capabilities, regulatory frameworks, and research institutions—while gradually losing control over the architectural choices that will shape future infrastructure.
Signs include diminishing contributions to 3GPP, slower progress in expanding testbeds, and increasing dependence on non-European control-plane and AI infrastructure.

1 Why Standards Leadership Matters

Governments worldwide have recognised that leadership in setting telecommunications standards has implications that reach beyond mere economic growth. Technical standards, such as those guiding 5G and 6G networks, influence industrial competitiveness, shape supply chain dependencies, and impact national security and defence capabilities. As the global contest over sixth-generation networks becomes more intense, the question of who establishes the rules for future digital infrastructure has evolved into a matter of statecraft.

The strategic importance of standards is now recognised at the highest levels of policy. The U.S. Department of Defense has identified leadership in cellular standards as vital to maintaining technological superiority, while NATO has identified advanced mobile communications as an emerging key technology. China's approach views standards as tools for strategic positioning and systematically expands its influence within international standards organisations. Similarly, the European Union's Standardisation Strategy frames standards as a means to enhance competitiveness, resilience, and technology development rooted in shared values (European Commission, 2022a). The U.S. National Standards Strategy for Critical and Emerging Technology considers international standards leadership a foundation of innovation, security, and prosperity, emphasising the need for allied coordination to sustain open and transparent standards ecosystems (White House, 2023). In December 2025, the U.S. administration reinforced this trajectory by signing a Presidential Memorandum directing immediate spectrum reallocation for 6G and by engaging diplomatically to advance American leadership in next-generation networks (White House, 2025). Yet, behind this apparent consensus on standards as a form of statecraft lies a critical difference in implementation: the US relies on private-sector scale, China on state-led coordination, and Europe on regulatory frameworks. It is this divergence, rather than differences in ambition, that reveals Europe's vulnerability.

These parallel strategies converge on a single insight: in a world where digital infrastructure underpins vital sectors such as energy grids and autonomous transportation, the actors who establish technical standards wield a form of structural power that endures for decades. This influence extends beyond mere economics; it is epistemic in nature—those responsible for developing standards define what counts as "secure", what "interoperability" involves, and what "AI-native" truly signifies in practice.

Standards, once adopted, become embedded in procurement contracts, regulatory compliance frameworks, and interoperability requirements. Reversing or modifying them after deployment is technically possible but prohibitively costly, as the 5G rip-and-replace experience has demonstrated.

For the European Union, the ambition to lead in 6G is not merely a matter of industrial competitiveness. It is a prerequisite for strategic autonomy: the capacity to operate, secure, and govern critical infrastructure

without excessive dependence on external actors whose priorities may diverge from European interests. The EU's position is distinctive because it combines strong research capabilities, leading contributors to standard development such as Ericsson and Nokia, an extensive regulatory portfolio, and a commitment to open, interoperable standards. The challenge is not a deficit of assets but a deficit of coordination.

This policy report examines the decisions being made now—within 3GPP and the ITU-R—that will determine the foundational architecture of 6G before commercial deployment begins around 2030. 3GPP develops the detailed system specifications that define how networks operate, from radio interfaces to core architecture and security protocols. Its work is organised in 'releases'—multi-year cycles that progressively define each generation of mobile technology. The ITU-R, through its spectrum study groups and the World Radiocommunication Conference (WRC), allocates the radio frequencies on which these technologies operate. Together, these institutions set the technical and regulatory parameters within which commercial networks are built. The report is accompanied by a Technical Working Paper providing the full analytical detail, methodology, and case studies underpinning the findings presented here.

2 Four Lock-in Points That Cannot Wait

Lock-in points are architectural decisions made during standardisation that become prohibitively costly—whether technically, contractually, or politically—to reverse once commercial deployment is underway. This report identifies four such decisions where European influence remains possible but is constrained by time.

2.1 Spectrum Harmonisation

The decisions made at World Radiocommunication Conference scheduled for late 2027, convened by the ITU, will set harmonised bands for 6G. Fragmented national allocations—the default inherited from the 5G era—limit economies of scale for equipment and undermine the commercial viability of deployment of cellular networks in Europe. Member State alignment on candidate bands in the 7-15 GHz range before WRC-27 is essential. Preparations for WRC-27 include agenda items concerning potential new spectrum identifications for IMT (International Mobile Telecommunications, the ITU framework defining each generation of mobile networks), with debates influenced by incumbent users and competing visions of where 6G should operate (ITU-R, 2026). The distributional outcomes—who gains access to harmonised bands, where economies of scale for equipment develop, and which regions set the early deployment model—are profoundly strategic.

2.2 RAN Architecture

The 3GPP Release 20 work items, which, among other things, lay the technical foundations for 6G, will shape the scope of Open RAN (Open Radio Access Network, an approach that allows network components from different vendors to interoperate, rather than requiring operators to source all equipment from a single supplier) interoperability for 6G. Whether to adopt open, disaggregated architectures or integrated vendor solutions will significantly affect supply-chain diversity, security responsibilities, and the competitiveness of European vendors. The transition to cloud-native (i.e., network functions designed to run on shared cloud computing infrastructure rather than dedicated hardware) and Open RAN architectures presents genuine opportunities for diversifying supply chains, while also creating new security vulnerabilities that require careful engineering from the outset (Bauer & Bohlin, 2022). This decision is currently under discussion within the 3GPP SA and RAN working groups.

2.3 Core Security

The Stage 2 architecture freeze for Release 20 core security is scheduled for September 2026. Security requirements embedded at this stage become mandatory conformance standards: interoperable, testable, and vendor-neutral. Any requirements introduced after deployment function as supplementary toolboxes—useful but structurally weaker. The EU Cybersecurity Act certification framework must therefore influence 3GPP specifications before this freeze, not afterwards. This timeline makes coordinated European positions in 3GPP SA3 (the security working group) an immediate priority.

2.4 AI/ML Integration

This is arguably the most significant qualitative shift from 5G to 6G: the evolution of networks from mere transport infrastructure into autonomous decision-making systems. As 6G networks develop, they will fundamentally integrate AI into their control and optimisation systems. The way AI components are incorporated—whether as interoperable, auditable functions or as proprietary black boxes—will influence the effectiveness of regulatory oversight, the scope of the AI Act's dual-compliance obligations for critical infrastructure, and the vulnerability to model poisoning and adversarial attacks. 6G's AI-native architecture shifts networks from passive transport layers to intelligent orchestrators that make autonomous decisions about routing, slicing, and resource allocation. For critical infrastructure, security must now also cover AI model integrity, training data provenance, and autonomous decision failure modes. These design considerations span Releases 20 and 21.

3 From 5G to 6G: Lessons and Structural Challenges

The transition from 5G to 6G represents a geostrategic inflection point whose architectural foundations are being set now. While Europe is deploying 5G infrastructure, with approximately 81% of the population covered by 2023 (EPRS, 2024), significant gaps in performance, investment, and industrial capacity remain compared with competitors. The 5G legacy reveals a recurring pattern: Europe consistently converts early-mover advantage in research and regulation into late-mover disadvantage in deployment and governance. The systemic vulnerabilities are by now familiar—fragmented markets across 34 mobile network operator groups, regulatory complexity involving over 270 agencies overseeing digital networks across EU Member States (Draghi, 2024b), limited capital flows restricting infrastructure densification, and delayed security upgrades exposing critical vendor dependencies.

A crucial analytical distinction shapes this section: the challenges affecting 6G deployment and those affecting standards development are related but distinct. Many of the structural weaknesses identified below—market fragmentation, investment constraints, regulatory complexity—primarily affect deployment. In the area of standards development, Europe's position is considerably stronger, with Ericsson and Nokia consistently listed among the leading contributors to 3GPP. However, deployment economics and standards engagement are not independent: operators' ability to fund vendors' participation in pre-standardisation R&D depends on their investment capacity, which is itself constrained by market conditions. As Letta has highlighted, achieving scale is 'not just an economic imperative but also a strategic one' (Letta, 2024). Understanding this linkage is essential for designing effective policy responses.

3.1 Supply-Chain Security: Strategic Lessons

The 5G supply-chain debate clarified how telecommunications infrastructure has become a central issue in economic security and geopolitical strategy, most notably through the controversy surrounding Huawei and ZTE. In Europe, the main policy tool has been the EU 5G Cybersecurity Toolbox, which combines technical measures with strategic ones to address supplier risk profiles and non-technical vulnerabilities (European Commission, 2020; NIS Cooperation Group, 2020).

Four lessons from the 5G experience are directly relevant to 6G. The first is the master lesson from which the others follow, namely, supply-chain security relies more on governance than purely on technology; for 6G, where software-defined networks, cloudification, and AI-native functions extend supply-chain surfaces beyond traditional radio hardware to include chip supply chains, virtualisation layers, data pipelines, and model supply chains, this insight is critical. Second, voluntary or inconsistent implementation leads to ongoing externalities within the internal market; one Member State's lenient stance can produce

security spillovers for others. Third, timing and lock-in shape cost curves: once equipment is deployed, rip-and-replace becomes prohibitively costly and politically contentious. Fourth, credible risk assessment requires shared baselines; Europe cannot depend on post-hoc corrections.

The Commission's January 2026 cybersecurity package proposals represent an effort to shift from recommendations to more harmonised EU-level frameworks for trusted ICT supply chains and phase-out mechanisms in critical sectors (European Commission, 2026a; European Commission, 2026b). For 6G, these lessons translate into specific standardisation imperatives: security requirements must be embedded before the architecture freeze, not retrofitted afterwards.

3.2 Regulatory Fragmentation and Investment Constraints

Europe's regulatory landscape for telecommunications remains highly fragmented. Market fragmentation limits the ability of operators and vendors to achieve economies of scale, while regulatory complexity involving over 270 agencies slows coordinated responses to rapidly evolving standardisation timelines. The investment gap is equally significant. European operators have consistently underspent relative to US and Asian counterparts on network densification and technology deployment, a structural deficit documented in both the Draghi and Letta reports.

A critical policy challenge concerns the intellectual property frameworks governing standards participation. Key European companies, including Ericsson and Nokia, have historically relied on licensing to sustain the R&D investments that underpin their contributions to standards. A stable and predictable patent framework is therefore essential for European standards leadership. The EU's SEP regulatory trajectory has introduced uncertainty: the Commission's proposed SEP regulation (COM/2023/232) was formally withdrawn in 2025, but the European Parliament has pursued legal action contesting the withdrawal (European Parliament, 2026). Externally, the Commission initiated WTO proceedings challenging Chinese practices related to global licensing terms for SEPs (DS632) and, in February 2026, announced it would request a WTO panel after consultations failed to resolve the dispute (European Commission, 2025a; European Commission, 2026c; WTO, 2025). This IP uncertainty not only discourages individual firms but also weakens the entire ecosystem's motivation to engage in pre-standardisation R&D, which is exactly where architectural influence is gained or lost.

The risk is not that Europe has already lost its standards-development position—Ericsson and Nokia remain among the top contributors to 3GPP—but that regulatory instability, investment uncertainty, and fragmented coordination could erode it during the critical 2025-2027 window when 6G's foundational architecture is being defined. Unless these challenges are translated into clear policy actions by the end of 2026, this period represents a critical inflection point after which European influence over foundational 6G architecture becomes substantially more difficult and costly.

4 6G Technology and Architecture

Sixth-generation network architectures differ from 5G not only in spectrum utilisation but also in architectural philosophy. Where 5G added network slicing and edge computing to cellular infrastructure, 6G is expected to embed AI functions deeply into network control and optimisation, rather than treating them purely as application-layer add-ons.

4.1 AI-Native Networks

The 'AI-native' orientation enables more autonomous network functions—such as closed-loop traffic steering and beam management—that adapt in near-real-time. The network can re-optimise itself as conditions change, reducing the need for manual reconfiguration and shortening the time between detection and response. AI-driven programmability makes network behaviour more visible and auditable, a property with direct regulatory significance for NIS2 supervisory obligations and AI Act conformity requirements for high-risk network functions.

Whether 6G and AI prove mutually reinforcing depends entirely on architectural choices made during standardisation. This conditionality is paramount. Sixth-generation networks and artificial intelligence are expected to be mutually reinforcing if designed with this symbiosis in mind. On the demand side, generative and 'physical AI' applications increase the need for reliable low-latency connectivity and for distributed inference close to the edge. On the supply side, 6G architectures embed AI into network control loops, enabling more autonomous optimisation and more granular performance assurance. However, this symbiosis is not automatic; it depends on architectural choices made during the standardisation process. If Release 20 studies do not prioritise AI-network integration, the bidirectional benefits may not materialise.

4.2 Software-Defined Infrastructure and New Dependencies

Software-defined networking principles, only partially realised in 5G, become foundational in 6G. Network functions can be distributed across compute resources, with control-plane intelligence dynamically reconfiguring capacity to match application requirements. However, virtualisation creates new vectors of dependency. If control-plane software or orchestration layers rely on proprietary systems from single vendors, the promised flexibility becomes a new form of vendor lock-in. As control-plane intelligence moves to cloud computing infrastructure, dependencies on hyperscale providers introduce concentration risks that may exceed the vendor concerns of the 5G era. Standards must address interoperability at the software orchestration level, not merely at hardware interfaces, and cloud control-plane assurance must be resolved before architecture choices become fixed. The question this raises is whether 3GPP is the appropriate forum for managing hyperscaler dependence, or if a separate European instrument is necessary, given that current institutional structures do not provide for this.

4.3 Sensing as Infrastructure.

Beyond communication, 6G architectures are expected to integrate sensing capabilities—using radio signals for positioning, environmental monitoring, and object detection. The IMT-2030 framework includes 'Integrated Sensing and Communication' as a usage scenario, suggesting that future networks will blur the boundary between communication infrastructure and sensor networks. For policymakers, this raises governance questions about data collection, surveillance boundaries, and the public-value applications—transport safety, precision agriculture, disaster response—that sensing integration could enable if governed appropriately. Equally important, sensing and telemetry can expand the volume and diversity of real-world data available for model improvement. When designed with clear governance, these data streams can support legitimate innovation without collapsing into indiscriminate surveillance. As sensing capabilities become embedded in network infrastructure, they also become part of critical infrastructure themselves, subject to the same governance, resilience, and assurance requirements that apply to the communication functions they complement.

4.4 The Political Economy of Standardisation

3GPP Release 20 is a critical juncture because it will establish the fundamental architecture decisions that constrain all subsequent 6G development. While Release 20 focuses on 5G-Advanced enhancements and initial 6G studies, Release 21 will contain the normative 6G specifications. The architectural decisions and study directions established in Release 20 constrain Release 21's specification space, making 2025-2027 the critical window for shaping 6G's technical foundations.

The political economy of standardisation indicates that early participation often exerts a disproportionate influence on outcomes. Companies and coalitions proposing initial technical specifications establish fundamental assumptions that shape subsequent compromises. By the time a standard is formally adopted, the range of feasible architectures has typically already been considerably reduced. Those firms initiating early contributions do not usually wait until regulatory mandates are in place; rather, their participation is the result of strategic choices made years earlier, motivated by expectations concerning SEP monetisation, patent portfolio management, and competitive positioning. Although most substantive work in standards development is undertaken by industry rather than governments, effective institutional coordination can create conditions that encourage firm-level involvement. The primary policy goal should be to foster market conditions enabling European companies to invest in research and development and to develop advanced technologies that position them as leaders in standard development.

5 The Geopolitical Contest Over 6G

5.1 Standards as Statecraft

6G geopolitics will be determined by rules: spectrum allocations, technical requirements, security architectures, certification baselines, and IP/licensing governance. The ITU-R has established the high-level IMT-2030 framework via Recommendation M.2160 (November 2023), which includes expanded usage scenarios beyond IMT-2020 (5G) and overarching aspects such as security and resilience (ITU-R, 2023). This shifts security and resilience from optional compliance to fundamental design principles, making it more difficult for ecosystems to treat security as a late-stage national addition.

Policy initiatives increasingly treat standards as a tool of statecraft. A significant development was the February 2024 minilateral agreement, in which ten countries—including Finland, Sweden, Japan, the Republic of Korea, Canada, and Australia—issued a joint statement endorsing principles for 'secure, open, and resilient by design' 6G (U.S. Department of State, 2024). The geopolitically relevant aspect is not the statement's non-binding nature but the signalling: like-minded states are attempting to pre-coordinate norms before technical specifications become fixed.

5.2 EU, US, and Chinese Approaches

The EU's approach to 6G combines three goals that are individually coherent and collectively in tension: sovereignty and resilience, openness and interoperability, and competitiveness at scale. Where exactly do these tensions have an impact? Sovereignty requires trusted-vendor standards that limit supply chains, and openness calls for interoperability that expands them. Competitiveness depends on scale, which points towards consolidation, and values-based regulation incurs compliance costs that penalise it. The EU has established a structured 6G R&I initiative through the Smart Networks and Services Joint Undertaking, with a budget of at least €1.8 billion (2021-2027), which is strategically significant because upstream contributions to standards are strongly linked to sustained R&D capacity and coordinated pre-standardisation work (European Commission, 2021).

Europe cannot credibly pursue leadership in geopolitical standards while tolerating internal fragmentation that hinders rapid learning, industrial scaling, and the establishment of uniform security standards. The EU is updating its connectivity governance accordingly: in January 2026, the Commission proposed a Digital Networks Act to modernise and harmonise rules for connectivity networks, explicitly linking regulatory modernisation to the need for resilient infrastructure and investment (European Commission, 2026d). On security governance, the January 2026 cybersecurity package and the February 2026 ICT Supply Chain Security Toolbox under the NIS2 Cooperation Group signal a shift towards more harmonised EU-level frameworks for trusted supply chains and phase-out mechanisms in critical sectors (European

Commission 2026a; European Commission, 2026b; European Commission, 2026e). Regarding IPR and standards competitiveness, the EU's WTO actions on SEPs show that Europe increasingly regards IP enforcement conditions abroad as a key economic security interest (European Commission, 2026c; WTO, 2025).

The U.S. approach is industry-led, emphasising private-sector innovation and strategic investment in pre-standardisation R&D at a scale that European public instruments cannot directly match. Chinese companies continue to participate actively in 3GPP and accumulate SEPs, benefiting from state-directed funding that creates a structural advantage in 3GPP participation—not only through spending levels but also through the systematic alignment of state direction and firm-level standards contributions, which market-economy actors cannot replicate through equivalent investment. Governments should focus on ensuring that patent rights are respected, both domestically and internationally, and that the standardisation process remains fair, industry-led, and grounded in technical merit.

5.3 International Cooperation

Transatlantic cooperation and alignment with like-minded partners bolster Europe's diplomatic influence. Nevertheless, they cannot substitute for internal unity. Europe cannot fully capitalise on partnerships with the United States, Japan, or South Korea while facing internal divisions. Two immediate actions are readily achievable: first, advancing standards diplomacy through coordinated stances in the ITU-R and 3GPP, with shared research and development priorities; second, enhancing assurance and certification interoperability. This involves aligning EU cybersecurity certification frameworks with US secure-by-design approaches and establishing mutual criteria for trusted supply chains. The European Union Agency for Cybersecurity (ENISA) and the National Institute of Standards and Technology (NIST) naturally serve as counterparts in this endeavour.

A note of realism is warranted. Given the prevailing transatlantic political climate, frameworks for cooperation should be judged primarily on their operational effectiveness rather than their institutional ambitions. The focus should be on areas where practical coordination is achievable and can contribute to strategic stability, rather than on institutional structures whose political foundations may have shifted. In practical terms, this entails prioritising domains such as spectrum management, mutual recognition of security certifications, and joint research and development prior to standardisation. These activities should yield tangible outcomes regardless of political headwinds, unlike ambitious institutional arrangements that may currently lack political support.

6 Security Architecture for Critical Infrastructure

This section offers a security governance perspective, recognising that technical security architectures are only as reliable as the policy tools, assurance frameworks, and coordination mechanisms that implement them across complex supply chains and cross-border infrastructures. The conceptual importance is high: 6G security governance requires a shift from "securing the network" to "governing autonomous behaviour within the network", a fundamentally different challenge that existing frameworks, including NIS2 and CER, were not originally designed to address.

6.1 Critical Infrastructure Dependencies

The EU's legal scope for critical sectors is extensive and expanding. The NIS2 Directive creates a unified cybersecurity framework across 18 critical sectors, while the Critical Entities Resilience (CER) Directive concentrates on the resilience of entities providing essential services against a wide range of hazards, including hybrid threats. The significance of 6G for critical infrastructure extends beyond bandwidth. Future networks will support AI and communication integration, integrated sensing and communication, and expansions of massive communication and low-latency reliability categories (ITU-R, 2023).

Critical infrastructure dependency pathways fall into four categories: operational control and automation (energy grids, transport, healthcare relying on low-latency communications); edge intelligence and robotics (autonomous systems requiring reliable connectivity for sensor fusion and coordination); data and model pipelines for AI (continuous data collection, distributed training, and model lifecycle management); and resilience through multi-layer connectivity (integrating terrestrial and non-terrestrial networks as fallback systems). Notably, as sensing capabilities become integral to network infrastructure, they themselves become critical infrastructure — expanding the governance perimeter that NIS2 and CER frameworks must address.

6.2 The Challenge of Agentic AI in Networks

The advent of agentic AI—systems capable of autonomous, goal-oriented action—introduces a new dimension to network security. As AI components gain increased autonomy within 6G control loops, the distinction between human-supervised and machine-autonomous decision-making becomes increasingly blurred. One of the principal challenges involves dual compliance obligations: AI-enabled network functions in critical infrastructure must adhere to both telecommunications cybersecurity standards (such as NIS2 and CER) and horizontal AI safety requirements mandated by the AI Act. This necessitates the development of coordinated governance mechanisms spanning both regulatory spheres. More fundamentally, NIS2 presumes a human-in-the-loop supervisory model; however, the integration of agentic AI into network control loops may effectively diminish this framework.

Consequently, the challenge extends beyond regulatory overlap to include the potential erosion of the supervisory premise itself.

6.3 Governance Imperatives

For 6G, security governance must evolve beyond perimeter-based models. Software-defined architectures, AI-native control functions, and distributed cloud infrastructure require continuous assurance rather than point-in-time certification. The EU's cybersecurity certification framework under the EU Cybersecurity Act provides a foundation, but certification-ready profiles for AI-driven network functionalities must be developed before deployment begins. Member States should coordinate supervisory approaches to AI-native network functions under NIS2 to prevent fragmented national responses that would undermine the single market's security baseline.

The Commission's January 2026 cybersecurity package proposals, including the revised Cybersecurity Act, explicitly address ICT supply-chain risks and aim to shift from recommendations to more harmonised EU-level frameworks for trusted supply chains. The February 2026 ICT Supply Chain Security Toolbox adopted under the NIS2 Cooperation Group highlights multi-vendor strategies and dependency reduction. For 6G, these governance innovations must be operationalised before architecture choices are locked in, not afterwards. The 5G experience demonstrated that retroactive security interventions—however necessary—are prohibitively costly and politically contentious.

7 Roadmap and Recommendations

The analytical threads running through this report converge on a single institutional imperative: the window for shaping 6G is open now, and coordination failures that were tolerable in 5G will be structurally decisive in 6G. The following roadmap translates the analysis into phased, time-bound actions aligned with 3GPP Releases 20 (study phase 2025–2026; major freezes around 2027) and 21 (specification phase 2027–2029).

A foundational principle should guide European action: **do no harm to standards leadership**. The EU should avoid adopting policies that would undermine the ability of key European companies to compete for leadership in the development of 6G. This does not imply favouritism; rather, it means ensuring that patent rights are respected both domestically and internationally, that the standardisation process remains fair, industry-led, and grounded in technical merit, and that cooperation with like-minded nations reinforces these conditions.

7.1 Phase 1: Immediate Actions (2026)

European influence over Release 20 study items in AI-native architecture, security-by-design, spectrum assumptions, and sensing integration necessitates coordinated action across regulatory frameworks, funding instruments, and institutional mechanisms. Crucially, the Stage 2 architecture freeze for Release 20 core security is scheduled for September 2026. After this date, security requirements become mandatory conformance standards; the EU Cybersecurity Act certification framework must influence 3GPP specifications before the freeze.

European Commission. Issue a Recommendation under the Radio Spectrum Policy framework by Q3 2026, encouraging Member States to align pre-commercial testing allocations within the 7–15 GHz range ahead of WRC-27. Horizon Europe and SNS JU calls for 2026–2027 must explicitly prioritise Release 20 participation by SMEs and research institutes, AI-native security validation, and energy-efficiency modelling, with funding linked to measurable standards engagement. An EU 6G Standards Coordination Office should be established within DG CNECT by Q2 2026 to monitor European contributions, coordinate Member State positions, and align spectrum and security strategies with NIS2 and CER objectives.

Member States. Publish 6G spectrum roadmaps by December 2026, with at least 15 Member States harmonising technical conditions to enable equipment development and cross-border trials. By Q2 2027, three cross-border 6G test corridors—in Nordic, Central, and Southern Europe—should be operational, integrating AI-driven management and energy monitoring. A pooled pilot procurement framework (2026–2028) should support 6G-ready infrastructure trials and reduce vendor fragmentation.

Industry. Increase Release 20 contributions to reach a 20–25% European share of approved work items relative to 2024 baselines, and pursue leadership roles in key 3GPP working groups (RAN, SA, SA5). Deliver at least two multi-vendor Open RAN demonstrations by end-2026. Early alignment with the Cyber Resilience Act would reduce compliance risks and demonstrate responsible innovation.

7.2 Phase 2: Medium-Term Positioning (2027–2029)

As Release 21 moves from study items to normative specifications, Europe must embed its priorities into AI governance, security architecture, sensing integration, and energy efficiency. A key challenge in this phase is the dual compliance obligation: AI-driven network functions in critical infrastructure must meet both telecommunications cybersecurity requirements (NIS2, CER) and horizontal AI safety obligations under the AI Act. Moreover, as control-plane intelligence moves to cloud computing infrastructure, dependencies on hyperscale providers introduce concentration risks that may exceed the vendor concerns of the 5G era.

European Commission. Issue guidance by 2028 to clarify NIS2 supervision of AI-native network functions. Develop certification-ready profiles for AI-driven functionalities under EU cybersecurity schemes. Consider, within the bounds of competition law, whether merger-related remedies or commitments could include verifiable investment and deployment obligations. In collaboration with the European Investment Bank, design instruments to mitigate risks associated with densification in higher-frequency bands.

Member States. Harmonise licensing conditions for candidate 6G bands before WRC-27, ensuring consistent technical parameters and interference protections. At least five Member States should pilot integrated sensing applications—transport safety, precision agriculture, disaster response—by 2028.

I**ndustry.** Implement auditable model provenance and update integrity in commercial trials. Participate in EU-level red-team testing to expose vulnerabilities before deployment. Europe should aim for 25–30% participation in Release 21 security and AI normative specifications, with at least three European-held leadership positions in priority 3GPP working groups.

7.3 Phase 3: Long-Term Deployment and Governance (2030+)

By 2030, Europe must convert standards influence into deployment leadership. This is the stage at which the architectural decisions from Releases 20 and 21 are integrated into commercial systems. Europe's prospects will depend on its ability to deploy, secure, and govern AI-native 6G networks at scale, including managing new supply-chain surfaces that go beyond traditional radio hardware into chip supply chains, virtualisation layers, data pipelines, and AI model supply chains.

At least ten Member States should operate commercial 6G pilots, demonstrating reduced reliance on non-European providers for critical components. Harmonised spectrum across 25 Member States should enable pan-European roaming and economies of scale. AI-native oversight must be integrated into NIS2 supervisory practices, with EU-level incident coordination mechanisms for autonomous network functions. A harmonised capital-expenditure tracking methodology should be established by 2027 to address Europe's structural investment deficit and achieve parity with US and Japanese telecom capex by 2030. At least two European vendors should remain among the top three contributors to 3GPP, ensuring sustained influence over future generations beyond 6G.

Table 1. European 6G Roadmap: Actors, Instruments, Timelines, and Metrics

Phase & Timeline	European Commission	Member States	Industry	Success Metrics
2025–2026 Release 20 Study Phase Goal: Shape AI-native architecture, security, spectrum, sensing	Radio Spectrum Rec Q3 2026 €500M earmarked Standards Office Q2 2026	Roadmaps Dec 2026 15 MS aligned 3 corridors Q2 2027 €1B procurement	+20% contributions 2 Open RAN demos Q4 2026 Early CRA alignment	20–25% work items 15 MS spectrum 3 corridors 2 AI demos
2027–2029 Release 21 Normative Goal: Embed priorities in specifications	NIS2 guidance 2028 AI certification EIB de-risk Explore consolidation	WRC-27 licensing 20 MS aligned 5 MS sensing pilots	Model provenance Red-team testing ~30% participation 3+ leadership roles	25–30% normative 20 MS bands Energy-per-bit (transparent methods)
2030+ Deployment & Governance Goal: Market leadership, resilience	Capex parity NIS2 integration EU coordination	10 MS pilots 25 MS spectrum Pan-EU roaming	2 vendors top 3GPP R&D for 7G	Standards parity Deployment scale Security integration Energy efficiency

Note: All percentage targets are indicative ranges relative to recent baselines. Timeline adjustments may be necessary based on the evolution of the 3GPP work plan.

7.4 Measuring Success

Progress should be evaluated through operational indicators linked to specific milestones that serve as early-warning signals rather than post-hoc assessments. If European-originated proposals do not meet the indicative 20-25% threshold in Release 20 work items by 2027, this should prompt a reassessment of funding and coordination before Release 21 specifications are finalised. Spectrum misalignment among fewer than 15 Member States by late 2026 would indicate fragmented preparation for WRC-27 and higher long-term deployment costs.

By 2027, Release 20 outcomes should reflect identifiable European propositions in AI-native control, security-by-design, and sensing integration. By 2029, European actors ought to influence core Release 21 specifications with at least 20 Member States aligned on key spectrum parameters. By 2030, Europe should demonstrate parity in standards participation, deployment readiness, security certification integration, and energy efficiency. Failure would not manifest as an outright collapse but as a gradual decline: decreasing contributions to 3GPP, diminished leadership roles, persistent spectrum fragmentation, and non-interoperable deployments—signals of growing dependence on external architectures.

7.5 Summary of Recommendations

European institutions: ensure policy coherence across digital, industrial, trade, and security portfolios. Establish a 6G Standards Coordination Office within DG CNECT, operational by end-2026, tasked with aligning Member State positions in 3GPP before each release cycle. Avoid policy instability in IP governance that could undermine R&D investment incentives during the critical pre-standardisation period.

Member States: align national spectrum strategies and pool resources for cross-border testing corridors by publishing national 6G spectrum roadmaps no later than December 2026, with at least fifteen Member States harmonising technical conditions to enable cross-border equipment development ahead of WRC-27.

Industry: intensify participation in international standards bodies and invest in open, modular architectures that enhance interoperability. AI-native security validation and model provenance frameworks must be tested in corridor environments before normative Release 21 specifications are finalised in 2027-2029.

Research institutions: prioritise applied experimentation linked to real-world deployment scenarios, ensuring that neither NIS2 nor the AI Act currently provides supervisory guidance calibrated to autonomous network functions—this gap must be addressed through empirical testing before regulations are operationalised.

Financial institutions: expand patient capital instruments suited to long innovation cycles, recognising that the 2025-2027 pre-standardisation period imposes the greatest marginal cost of investment uncertainty on European participation in 3GPP.

International partners: institutionalise joint technology governance forums capable of coordinating export controls, investment screening, and research collaboration. The February 2024 minilateral statement on secure, open, and resilient 6G demonstrates that coalition-building opportunities exist; the challenge is turning declarations into operational coordination before technical specifications are finalised.

The alternative—fragmented action across these domains—does not merely slow progress; it cedes the architectural decisions that will influence critical infrastructure for decades to come to actors whose priorities differ from those of the European Union.

CONCLUSIONS

Shaping the Rules or Accepting Them

The 5G experience provides Europe with a clear assessment of its institutional shortcomings. The Union entered the 5G era with ambitious coverage goals, a sophisticated regulatory framework, and top-tier vendors. Yet it concluded with fragmented operator groups, hundreds of separate regulatory bodies, a persistent investment shortfall, and security issues that necessitated costly interventions after vendor relationships had already been established. None of these failures was unavoidable.

The risk for 6G is not that Europe merely repeats past patterns, but that it does so with higher stakes and a more limited timeframe for correction. 6G represents the foundational infrastructure on which AI-driven systems will operate autonomously. The architectural decisions currently being made in 3GPP Release 20 will shape whether, in 2032, European operators govern networks they helped design or manage infrastructure whose security features, vendor dependencies, and AI governance frameworks are determined by others.

Europe's position in standards development remains strong: Ericsson and Nokia are among the top contributors to 3GPP globally, ETSI and SNS JU produce world-class pre-standardisation work, and the EU's regulatory portfolio—the AI Act, NIS2, the Cyber Resilience Act, the proposed Digital Networks Act—could, if coordinated effectively, establish the EU as a genuine global norm-setter. What Europe requires is the coordination infrastructure to deploy these assets simultaneously, before the window closes, rather than sequentially.

The window remains open. The architectural choices have not yet been finalised. The key question is whether European institutions, Member States, and industry will collaborate with the coherence and speed required by the standardisation timeline—or whether, by 2030, Europe will once again find itself deploying networks based on rules it did not establish. The more fundamental question is whether the EU's institutional architecture, designed for regulatory harmonisation over long periods, is structurally capable of the pace required by a 3GPP release cycle.

Bibliography:

Bauer, J. M., & Bohlin, E. (2022). Regulation and innovation in 5G markets. Telecommunications Policy, 46(4), 102260. https://doi.org/10.1016/j.telpol.2021.102260
Draghi, M. (2024a). The future of European competitiveness: A competitiveness strategy for Europe. European Commission. https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en
Draghi, M. (2024b). The future of European competitiveness: In-depth analysis and recommendations. European Commission. https://commission.europa.eu/document/download/ec1409c1-d4b4-4882-8bdd-3519f86bbb92_en
European Commission. (2020). Secure 5G networks: Implementing the EU toolbox (COM(2020) 50). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020DC0050
European Commission. (2021). Smart Networks and Services Joint Undertaking. https://digital-strategy.ec.europa.eu/en/policies/smart-networks-and-services-joint-undertaking
European Commission. (2022a). An EU strategy on standardisation: Setting global standards in support of a resilient, green and digital EU single market (COM(2022) 31 final). https://single-market-economy.ec.europa.eu/single-market/goods/european-standards/standardisation-policy/standardisation-strategy_en
European Commission. (2025a, January 19). WTO consultation on China's royalties for high-tech sector (SEPs) [Press release]. https://ec.europa.eu/commission/presscorner/detail/en/ip_25_293
European Commission. (2025b, December 3). Cyber Resilience Act: Policy page and compliance timeline. https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act
European Commission. (2026a, January 20). New measures to strengthen cybersecurity resilience and capabilities (Cybersecurity Package). https://commission.europa.eu/news-and-media/news/new-measures-strengthen-cybersecurity-resilience-and-capabilities-2026-01-20_en
European Commission. (2026b, January 20). Cybersecurity package: Questions & Answers. https://digital-strategy.ec.europa.eu/en/faqs/cybersecurity-package-questions-answers
European Commission. (2026c, February 12). EU requests WTO panel in dispute with China over royalties for EU high-tech sector (SEPs). https://policy.trade.ec.europa.eu/news/eu-requests-wto-panel-dispute-china-over-royalties-eu-high-tech-sector-2026-02-12_en
European Commission. (2026d). Proposal for a Regulation for the Digital Networks Act (DNA). https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-digital-networks-act-dna
European Commission. (2026e, February 13). EU launches new toolbox to strengthen ICT supply chain security. https://digital-strategy.ec.europa.eu/en/news/eu-launches-new-toolbox-strengthen-ict-supply-chain-security
European Parliament. (2026). Standard essential patents (SEP) regulation: Legislative train (status and withdrawal). https://www.europarl.europa.eu/legislative-train/spotlight-JD22/file-patent-licensing-package-1
European Parliament, European Parliamentary Research Service. (2024). A future-proof network for Europe: Full fibre and 5G. https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762298/EPRS_BRI(2024)762298_EN.pdf
International Telecommunication Union Radiocommunication Sector. (2023). Recommendation ITU-R M.2160-0: Framework and overall objectives of the future development of IMT for 2030 and beyond. https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2160-0-202311-I!!PDF-E.pdf
International Telecommunication Union. (2026). WRC-27 studies. https://www.itu.int/en/ITU-R/study-groups/rcpm/Pages/wrc-27-studies.aspx
Letta, E. (2024). Much more than a market: Speed, security, solidarity – Empowering the Single Market to deliver a sustainable future and prosperity for all EU citizens. European Commission. https://www.consilium.europa.eu/media/ny3j24sm/much-more-than-a-market-report-by-enrico-letta.pdf

NIS Cooperation Group. (2020). EU Toolbox of risk mitigating measures (CG Publication 01/2020). https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures

NIS Cooperation Group. (2023). Second progress report on the implementation of the EU Toolbox on 5G cybersecurity. https://portal5g.pt/wp-content/uploads/2023/06/Second_Progress_Report_on_the_Toolbox_implementation_Final.pdf

Serentschy, G., Timmers, P., & Matinmikko-Blue, M. (2023). Toward anticipatory regulation and beyond. In P. Ahokangas & A. Aagaard (Eds.), The changing world of mobile communications (pp. 221-251). Palgrave Macmillan. https://doi.org/10.1007/978-3-031-33191-6_9

U.S. Department of State. (2024, February 28). Joint statement endorsing principles for 6G: Secure, open, and resilient by design. https://2021-2025.state.gov/joint-statement-endorsing-principles-for-6g-secure-open-and-resilient-by-design/

White House. (2023). U.S. Government National Standards Strategy for Critical and Emerging Technology (USG NSSCET). https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/05/US-Gov-National-Standards-Strategy-2023.pdf

White House. (2025, December 19). Fact sheet: President Donald J. Trump takes action to win the 6G race. https://www.whitehouse.gov/fact-sheets/2025/12/fact-sheet-president-donald-j-trump-takes-action-to-win-the-6g-race/

World Trade Organisation. (2025). DS632: China — Worldwide licensing terms for Standard Essential Patents. https://www.wto.org/english/tratop_e/dispu_e/cases_e/ds632_e.htm