

## The EU's Quantum Act: Economic security, interoperability and Europe's techno-geopolitical choice



Quantum technologies are becoming strategic infrastructure that will shape economic security, military inter-operability and geopolitical influence. The European Union's forthcoming Quantum Act, scheduled for adoption in 2026, has three main objectives: to boost research and innovation in quantum technologies; to scale up industrial capacity; and to reinforce supply-chain resilience and governance. It will be a decisive test of whether Europe can convert scientific excellence into durable strategic capacity before dependencies harden.

- ▶ The EU's Quantum Act is less an innovation law than a **strategic economic-security framework** for a dual-use technology.
- ▶ Europe's central risk is not scientific lag, but **locked-in dependencies** across hardware, materials, cloud access and cryptography.
- ▶ Over-regulation could accelerate talent flight, while under-regulation risks **strategic irrelevance and external dependency**.
- ▶ Misalignment with quantum standards emerging among key transatlantic and Indo-Pacific partners – if not managed through a clear articulation of Europe's own strategic interests – would impose lasting costs on Europe's security and industrial competitiveness.

### GSIS 2026 News:

*Exhibitor registration for GSIS 2026 is now live – secure your stand today and benefit from our exclusive early bird offer!*



### Europe's quantum dependencies

Often framed as an innovation or industrial-policy instrument, the Quantum Act is better understood as a strategic governance framework for a dual-use technology operating at the intersection of supply chains, standards and geopolitics. As global architectures for quantum communication, post-quantum cryptography (PQC) and sensing consolidate, the EU faces a narrowing window of time in which to determine whether it will emerge as a credible rule-shaper in the global quantum order or manage technological dependence as a rule-taker.

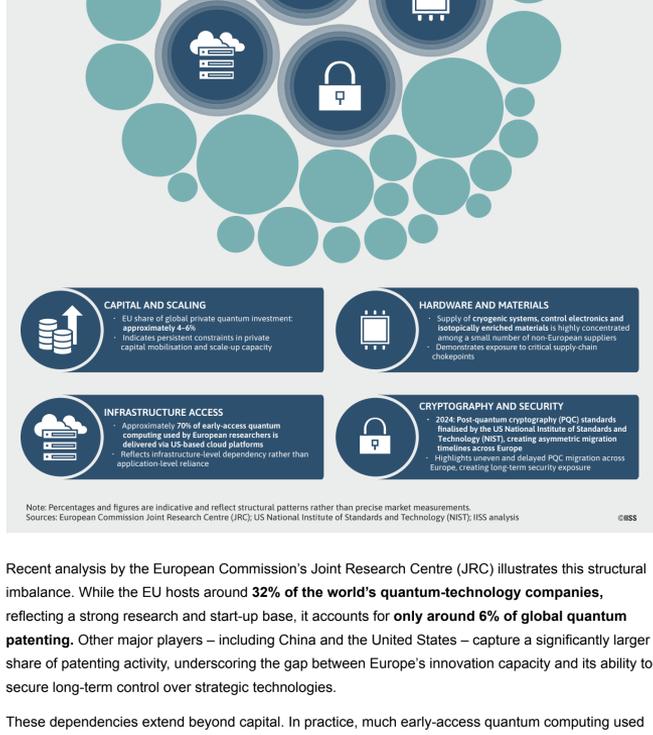
Despite substantial public funding, the EU attracts only around **4–6% of global private quantum investment**, limiting the scale-up of quantum start-ups and reinforcing Europe's reliance on non-European hardware and cloud service providers. This investment asymmetry constrains Europe's ability to translate research leadership into long-term strategic capacity. As illustrated in the graphic below, Europe's quantum vulnerabilities span multiple interlinked areas – capital, infrastructure, hardware and cryptography – rather than a single technological bottleneck.

Europe nevertheless retains world-class quantum-research capabilities and strengths in areas such as photonics, cryogenics and theoretical science. But structural dependencies narrow its strategic options as quantum technologies move from laboratories into early infrastructures. The core challenge facing the Quantum Act is therefore not innovation but governance under conditions of dependence.

*"The next big accelerator in the cloud will be quantum, and I am excited about our progress."*

▶ Satya Nadella, CEO, Microsoft, FY2025 Q4 Earnings Conference Call, 2025

### Europe's quantum dependency stack



Recent analysis by the European Commission's Joint Research Centre (JRC) illustrates this structural imbalance. While the EU hosts around **32% of the world's quantum-technology companies**, reflecting a strong research and start-up base, it accounts for **only around 6% of global quantum patenting**. Other major players – including China and the United States – capture a significantly larger share of patenting activity, underscoring the gap between Europe's innovation capacity and its ability to secure long-term control over strategic technologies.

These dependencies extend beyond capital. In practice, much early-access quantum computing used by European researchers is delivered through US-based cloud platforms, embedding reliance at the infrastructure level rather than merely at the application layer. Hardware and material supply chains are similarly narrow: key components – ranging from ultra-low-temperature cryogenic systems and control electronics to isotopically enriched materials – are produced by a limited number of suppliers concentrated outside the EU, particularly in the US and a small number of partner countries where production, export controls and technological road maps are closely coordinated. These chokepoints expose Europe to disruption, price shocks and geopolitical leverage as global demand for quantum technologies rises.

Cryptography represents a further exposure. While the US has moved to standardise and implement post-quantum cryptography (PQC), Europe's transition remains uneven. Delays increase the risk that sensitive data collected today could be decrypted in the future, undermining long-term security for government, defence and critical infrastructure. Taken together, these vulnerabilities define the strategic problem the EU's Quantum Act is designed to address: not how to invent quantum technologies, but how to govern their secure and reliable integration.

*"The transition to post-quantum cryptography is not a future problem – it is a present security challenge that governments must address now."*

▶ Jen Easterly, Director, US Cybersecurity and Infrastructure Security Agency (CISA), 2024

**4–6%**

**EU SHARE OF GLOBAL PRIVATE QUANTUM INVESTMENT**

**~70%**

**SHARE OF EARLY-ACCESS QUANTUM COMPUTING DELIVERED TO EUROPEAN CLOUD PLATFORMS**

**2024**

**NIST FINALISED PQC STANDARDS**



### Governing quantum technologies without repeating the AI Act's mistakes

The EU's experience with the 2024 Artificial Intelligence (AI) Act offers a cautionary reference point for quantum governance. Three design risks stand out:

- **Timing:** Early drafts of the AI Act were overtaken by rapid advances in large language models (LLMs), necessitating substantial revisions. Quantum technologies – particularly in error correction, networking and sensing – are evolving unevenly but quickly. A rigid regulatory framework risks obsolescence before implementation. The Quantum Act will therefore require built-in flexibility, including delegated acts and periodic review mechanisms, to adapt without reopening the entire legislative process.
- **Overbreadth:** Compliance burdens under the AI Act raised concerns about innovation drag and talent flight. Europe's quantum ecosystem is smaller and more fragile than its AI sector. Overly broad definitions of 'high-risk' quantum systems or heavy-handed requirements could push start-ups and researchers toward more permissive jurisdictions. Proportionality will be essential, focusing regulatory attention on genuinely security-critical applications while preserving space for experimentation.
- **Fragmentation:** The AI Act exposed divergent national priorities within the EU, with tensions between precautionary and competitiveness-oriented approaches. Quantum technologies, given their defence and intelligence implications, are likely to sharpen these divides. Without robust coordination across EU institutions and member states, national initiatives could proliferate in parallel, undermining coherence. Governance structures that link industrial, security and trade authorities will be critical to avoid a patchwork of regimes.



### Inter-operability and the geopolitics of quantum standards

Quantum governance is inherently geopolitical. Decisions taken under the Quantum Act will shape Europe's alignment with key security and technology partners, and its influence in global standard-setting bodies. This is particularly acute in areas such as PQC, quantum communication networks and sensing, where inter-operability is essential for military cooperation and secure data exchange.

Across the transatlantic and Asia-Pacific landscape, key partners are moving ahead with national quantum programmes while deepening coordination on supply chains, standards and inter-operability. For example, emerging coordination on PQC standards among the US, Japan and several European partners is already shaping procurement and inter-operability decisions in government and defence systems. In this context, divergence carries costs. Regulatory misalignment could limit European access to partner infrastructures, complicate secure data exchange, defence cooperation and NATO-led inter-operability efforts, and weaken Europe's voice in emerging governance forums. For Europe, the objective is not technological autonomy, but credible participation in shaping inter-operable architectures alongside like-minded partners.

The Quantum Act will therefore be read internationally as a signal of Europe's strategic orientation. Close coordination with NATO, International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) and International Telecommunication Union (ITU) ensures, as well as with export-control and security frameworks among key partners, will be essential to ensure that EU rules reinforce rather than fragment the broader partner technology ecosystem.

### Implications of the Quantum Act

With the legislative draft not yet public, assessments are preliminary at this point. Nonetheless, three implications of the Quantum Act already stand out:

1. It will test whether the EU can integrate industrial policy and economic security in a single framework for an emerging dual-use technology. Failure to do so would risk repeating past patterns in which Europe regulated without scaling, leaving dependencies intact.
2. It will serve as a litmus test for Europe's role under the emerging global-technology governance. Flexibility and alignment will determine whether the EU is seen as a trusted partner shaping shared standards or as a regulatory outlier.
3. It is a race against technological and institutional time. Key quantum architectures and standards have largely consolidated, narrowing the space for late-stage governance intervention. Europe's influence will depend on whether its governance choices embed adaptability, scaling incentives and partner coordination from the outset.

*"Technical standards are of strategic importance. Europe's technological sovereignty, ability to reduce dependencies and protection of EU values will rely on our ability to be a global standard-setter."*

▶ Thierry Breton, former European Commissioner for the Internal Market, on the EU Standardisation Strategy, 2022

Handled carefully, the Quantum Act could secure Europe a meaningful role in shaping the global quantum order. Mishandled, it would risk heavier regulation, persistent dependencies and diminishing strategic influence in a technology domain that will underpin economic and security power for decades to come.

organised by: Hamburg Messe + Congress IISS

*To stay ahead of emerging threats and insights follow GSIS on LinkedIn*

### Our Partners 2025

**Founding Partner** AIRBUS **Founding Partner** Microsoft **Alliance Partner** Peregrine **Alliance Partner** SPECIAL COMPETITIVE STRIKE PROJECT

**Alliance Partner** eraneos **Official Partner** EDGE **Venture Partner** SPEED GROUP

### CONTACT US

Hamburg Messe und Congress GmbH · Messeplatz 1 · 20357 Hamburg · Germany  
Phone +49 40 3569-0 · Fax +49 40 3569-2203 · info@gsis-hamburg.com · www.gsis-hamburg.com

Follow us: LinkedIn

Management Board: Uwe Fischer (CEO), Heiko M. Stutzinger (CEO)  
Hamburg Municipal Court, Reg. No. HRB 12 054  
VAT No. DE811214125