

(English version)

**Question for written answer E-004525/25  
to the Commission  
Moritz Körner (Renew)  
(13 November 2025)**

*Subject:* Post-quantum cybersecurity

1. According to the Commission's assessment, when is quantum computing expected to reach a level of maturity that would have significant practical or security implications for the EU's digital infrastructure?
2. What preparations or measures is the Commission undertaking to ensure that the data of EU citizens, public institutions, and businesses remain secure in the face of potential decryption capabilities enabled by quantum technologies?
3. Is the Commission coordinating with the Member States or international partners to develop quantum-resistant encryption standards and a unified European strategy for post-quantum cybersecurity?

Submitted: 13.11.2025

**Answer given by Executive Vice-President Virkkunen on behalf of the European Commission  
(7 January 2026)**

The Commission closely monitors progress in quantum computing and is actively engaged in advancing this field. While it is not possible to predict an exact date, experts estimate that a large-scale quantum computer threatening public-key cryptography could be available within the next 16 years <sup>(1)</sup>.

In April 2024 the Commission adopted a recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography (PQC) <sup>(2)</sup>, followed in June 2025 by a Roadmap <sup>(3)</sup> with timelines agreed among the Member States.

These are complemented by the work of the European Union Agency for Cybersecurity (ENISA) on post-quantum cryptography and by EU cybersecurity legislation, including the NIS2 Directive, the Digital Operational Resilience Act and the Cyber Resilience Act <sup>(4)</sup>, which require entities to manage cryptographic risks, support crypto-agility and implement security-by-design in digital products.

Given the already existing risk of harvest now-decrypt later attacks and the long time needed for cryptographic migrations, the EU Roadmap recommends migration of high-risk use cases to PQC by 2030, and for as many systems as practicable by 2035.

The Commission coordinates closely with Member States through the PQC workstream of the Network and Information Systems (NIS) Cooperation Group and engages with international partners and standardisation bodies, such as the United States' National Institute of Standards and Technology (NIST), the Internet Engineering Task Force (IETF) and the European Telecommunications Standards Institute (ETSI), to ensure interoperability and a unified European approach to PQC recognising the relevance of international collaboration.

---

<sup>(1)</sup> Status of quantum computer development BSI — Status of quantum computer development — The status of quantum computer development, <https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Quantentechnologien-und-Post-Quanten-Kryptografie/Entwicklungsstand-Quantencomputer/entwicklungsstand-quantencomputer.html>.

<sup>(2)</sup> Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography | Shaping Europe's digital future, <https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography#:~:text=This%20Commission%20Recommendation%20encourages%20Member%20States%20to%20develop,the%20different%20Member%20States%20and%20their%20public%20sectors.>

<sup>(3)</sup> A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography | Shaping Europe's digital future, <https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography>.

<sup>(4)</sup> <https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng>, <https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng>, <https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng>.