Strengthening Europe's Collective Transition to PQC

28 AUGUST 2026

Elžbieta Rasimavičiūtė

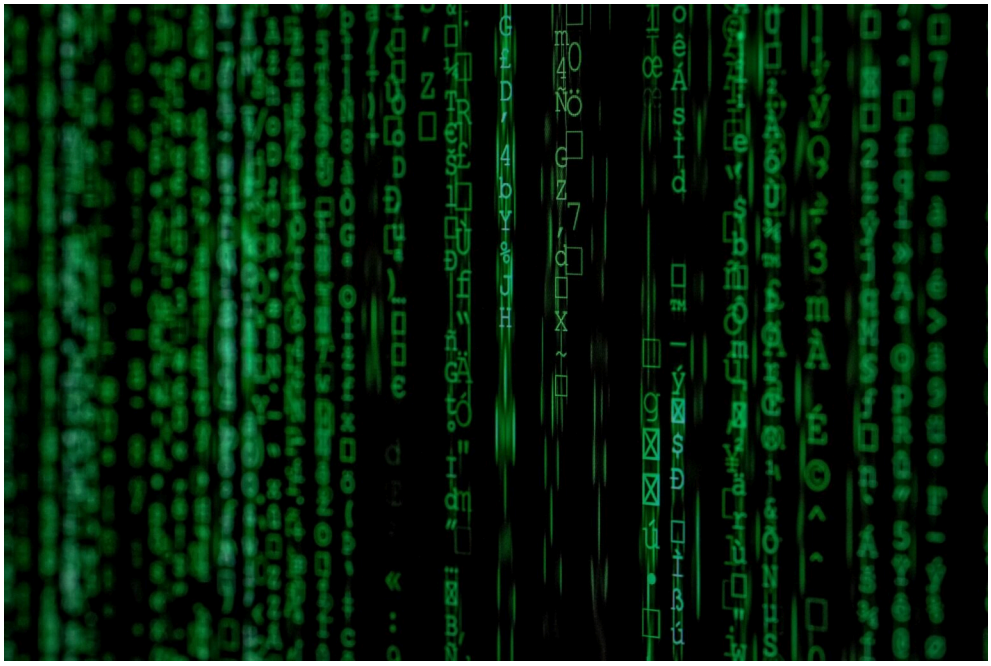

Photo by Markus Spiske on Unsplash

Europe's PQC transition at a Glance

Resilient digital infrastructure and communications to this date heavily rely on public-key cryptographic schemes (European Union Agency for Cybersecurity [ENISA], 2021; NIS Cooperation Group, 2025). Such cryptographic schemes are vital for ensuring essential security functions, including confidentiality, integrity, authentication, authorisation, and non-repudiation of data and communications (Barker, 2016). However, this status quo is increasingly being challenged by advances in quantum computing. Experts estimate that sufficiently powerful quantum computers could break existing public-key cryptographic standards by 2040, or potentially earlier, placing both future communications and sensitive data exchanged today at risk of being decrypted (Bundesamt für Sicherheit in der Informationstechnik [BSI], 2024; NIS Cooperation Group, 2025). To address this threat, the EU has pursued several initiatives, including establishing a common roadmap for the transition to post-quantum cryp-

tography (PQC). The roadmap recommends that Member States initiate their national transitions by the end of 2026, migrate high-risk systems no later than 2030, and complete the transition of as many remaining systems as practically feasible by 2035 (NIS Cooperation Group, 2025). However, deadlines alone cannot guarantee an effective and coordinated transition. This policy brief argues that, in the absence of clearly assigned institutional accountability towards PQC implementation, Europe risks missing its PQC implementation targets and further deepening existing disparities in preparedness, potentially turning fragmented implementation into a collective European security vulnerability.

Quantum computing is a direct European security threat and a collective vulnerability

While quantum computing promises considerable societal benefits, including more advanced drug development, improved detection of natural disasters, new approaches to combating climate change (European Commission, 2025), and facilitating breakthrough discoveries in solving complex finance and logistical problems (Memon et al., 2024), it consequently presents a significant strategic security challenge. Critical national infrastructure, medical records, financial information, private communications, investment plans, and governmental and military data all rely on cryptographic safeguards to prevent unauthorised access and manipulation – safeguards that advances in quantum computing increasingly threaten to compromise. This phenomenon is commonly referred to as Q-day – a possible future point where quantum computers could decrypt current encryption systems and access extremely sensitive information (Paul et al., 2024).

The Q-day threat is particularly significant for the European Union, where Member States increasingly depend on interconnected digital infrastructure, cross-border critical services, shared cloud and communication systems, and integrated supply chains. This interconnectedness creates a shared security challenge: vulnerabilities do not remain confined within national borders. Although no quantum-enabled attack has yet demonstrated comparable cross-border effects, attacks such as the 2017 NotPetya, which spread through compromised Ukrainian accounting software, illustrate how vulnerabilities within interconnected digital systems can produce severe and far-reaching consequences worldwide. Insufficient PQC protection in one Member State could provide an entry point into shared infrastructure or communications, thereby disrupting cross-border services and compromising the security of the wider European digital ecosystem. Thus, the collective protection of information and communications is essential to "the EU's and Member States' society, economy, security and prosperity" (NIS Cooperation Group, 2025, p. 3).

It is widely acknowledged that governments globally are engaging in

'Store Now, Decrypt Later' practices – collecting encrypted data now with the intent to decrypt it in the future once quantum capabilities allow (Cybersecurity and Infrastructure Security Agency et al., 2023; Paul et al., 2024). Due to such already present security exposure, and the considerable time required to migrate complex infrastructure, particularly old, legacy systems, to PQC, Europe's response must be timely, targeted and carefully coordinated.

Although a cohesive European strategy for addressing quantum threats is emerging, early indications suggest that Member States differ in the priority they assign to PQC, as well as in their financial resources and technical capabilities. At the national level, France, Germany, and the Netherlands have been emerging as leading Member States by developing technical guidance on PQC implementation and launching pilot projects at national and European levels, while comparable progress remains limited in other Member States (Pupillo et al., 2025). Awareness of, and investment in, PQC also remain limited among European stakeholders (ISACA, 2025).

Uneven early national action in PQC preparedness and implementation jeopardises the Union's ability to meet the 2026, 2030, and 2035 deadlines collectively and, consequently, to safeguard data and communications against present and emerging threats. For this reason, emerging fragmentation constitutes a collective European security vulnerability and directly undermines Europe's digital sovereignty.

Direction vs. Implementation

The Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography represents an important call to action for EU Member States. The roadmap explicitly calls on Member States to develop national plans for migrating high-risk entities, particularly covered by NIS2 – public administrations and critical infrastructure – to PQC (NIS Cooperation Group, 2025). The very First Steps, targeted for achievement by 2026, include developing a timeline and a clear PQC implementation plan; identifying stakeholders, digital dependencies, and supply chains; conducting a quantum risk analysis; and managing cryptographic assets. Resource allocation, adoption of certification schemes, and implementation of pilot projects are among the 2030 targets, while 2035 marks the completion of the transition to as many existing systems as possible (NIS Cooperation Group, 2025). The Roadmap establishes a clear direction and timeline for navigating PQC implementation at the national level, presented as a set of recommendations; it does not impose an explicit obligation to meet the 2026, 2030, or 2035 milestones.

Existing EU legislation provides a broader regulatory foundation. The Digital Operational Resilience Act (DORA) requires financial entities to establish and maintain frameworks for managing information and communication technology (ICT) risks (European Insurance and Occupational

Pensions Authority [EIOPA], n.d.), while NIS2 imposes cybersecurity risk-management obligations on essential and important entities, including requirements concerning cryptography and, where appropriate, encryption (Directive (EU) 2022/2555, 2022, art. 21(2)(h)). These provisions may facilitate PQC implementation as quantum-related risks emerge; however, neither DORA nor NIS2 establishes PQC-specific implementation regulations.

The overall lack of explicit, harmonised and enforceable obligations to achieve specific PQC migration outcomes risks producing uneven PQC transition, potentially resulting in missed deadlines amongst Member States and leaving shared European systems dependent on quantum-vulnerable cryptography. Given the substantial differences emerging among Member States in PQC prioritisation, resources, and technical capabilities, reliance on a non-binding framework jeopardises the timely and coordinated implementation of the transition.

Strengthening the Implementation Mechanism Through the Lens of Fragmentation

To mitigate emerging fragmentation in PQC implementation and reduce the risk that the transition remains incomplete by Q-Day, the Roadmap should be complemented by a limited binding implementation framework. This framework should establish a more precise implementation strategy, complemented by mandatory and clearly assigned institutional responsibilities for national PQC implementation and oversight, as well as standardised progress-reporting requirements.

Sector-specific PQC obligations could be integrated into existing frameworks, including DORA and the NIS2 Directive, which already establish binding risk-management, reporting, supervisory, and enforcement mechanisms. However, establishing uniform PQC planning and reporting across the Union may require a new horizontal instrument or targeted amendment to existing legislation. Building requirements could include selected measures outlined in the Roadmap, such as mandatory cryptographic inventories, quantum-risk assessments, the mapping and updating of digital dependencies, PQC transition plans and their completion, and the adoption of appropriate certification requirements. Relevant entities should report to designated national authorities, which could subsequently submit consolidated national progress reports to the European Commission. Technical support and progress assessment could be provided by ENISA, while the relevant national and EU authorities could require corrective action when milestones are missed.

Given the already existing differences in national PQC priorities and capabilities, some Member States may experience delays in the targeted implementation of PQC. Alongside progress reporting, the EU should maintain funding and ensure technical assistance is directed to Member

States and sectors with more limited financial and technical capacities, prioritising capacity-building. This approach would preserve national flexibility regarding the practical means of migration while ensuring that all Member States progress towards a common minimum level of PQC readiness within the agreed timeframe.

Europe's quantum resilience will ultimately be measured by its collective preparedness

Europe's quantum resilience depends heavily on the effective implementation of PQC across all Member States. Differences in national priorities, resources, and technical capabilities risk undermining the Union's collective ability to complete the transition within a shared timeframe. Establishing a coherent accountability framework that complements existing EU legislation would help ensure that Member States prioritise implementation and meet the 2026, 2030, and 2035 milestones, thereby strengthening Europe's overall quantum resilience and safeguarding its digital sovereignty.

Bibliography

Barker, E. (2016). Recommendation for key management: Part 1—General (Revision 4; NIST Special Publication 800-57 Part 1). National Institute of Standards and Technology. https://csrc.nist.rip/library/alt-SP 800-57part1rev4.pdf

Bundesamt für Sicherheit in der Informationstechnik. (2024). Status of quantum computer development (Version 2.1). https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ Publikationen/Studien/Quantencomputer/Entwicklungstand_QC_V_2_1.html

Cybersecurity and Infrastructure Security Agency, National Security Agency, & National Institute of Standards and Technology. (2023). Quantum-readiness: Migration to post-quantum cryptography.https://media.defense.gov/2023/Aug/21/2003284212/-1/-1/0/CSI-QUANTUM-READINESS.PDF

Directive (EU) 2022/2555 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, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), 2022 O.J. (L 333) 80. http://data.europa.eu/eli/dir/2022/2555/oj

European Commission. (2025, June 23). EU reinforces its cybersecurity with post-quantum cryptography. https://digital-strategy.ec.europa.eu/en/news/eu-reinforces-its-cybersecurity-post-quantum-cryptography

European Insurance and Occupational Pensions Authority. (n.d.). Digital Operational Resilience Act (DORA). Retrieved August 25, 2026, from https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

European Union Agency for Cybersecurity. (2021, May 3). Post-quantum cryptography: Current state and quantum mitigation. https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation

ISACA. (2025, April 28). Despite rising concerns, 95% of organizations lack a quantum computing roadmap, ISACA finds. https://www.isaca.org/about-us/newsroom/press-releases/2025/organizations-lack-a-quantum-computing-roadmap-isaca-finds

Memon, Q. A., Al Ahmad, M., & Pecht, M. (2024). Quantum computing: Navigating the future of computation, challenges, and technological breakthroughs. Quantum Reports, 6(4), 627–663. https://doi.org/10.3390/quantum6040039

NIS Cooperation Group. (2025). A coordinated implementation roadmap for the transition to post-quantum cryptography (Part 1, Version 1.1, EU PQC Workstream). European Commission. https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography

Paul, I., Ehlen, S., & Weitkämper, C. (2024). Preparations for Q-Day: IT systems worldwide need to be converted to post-quantum cryptography—A complex undertaking. BSI Magazine, 2024/02, 8–9. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Magazin/BSI-Magazin_2024-02.pdf?__blob=publicationFile&v=2

Pupillo, L., Ashworth, S., & Polito, C. (2025, December 3). We need to urgently strengthen the EU's transition to a quantum-safe world. Centre for European Policy Studies. https://www.ceps.eu/we-need-to-urgently-strengthen-the-eus-transition-to-a-quantum-safe-world/