Financováno Evropskou unií
NextGenerationEU

MINISTERSTVO PRŮMYSLU A OBCHODU

Grant Thornton

Quantum technologies and communication

Study 27 summary · prepared for the Ministry of Industry and Trade of the Czech Republic · June 2025

AT A GLANCE

This **study 27** explains how quantum technologies will reshape computing, communication and security — and what they mean for 5G networks. It introduces the principles of quantum computing and quantum communication, assesses **when quantum computers could break today's encryption**, and sets out the steps regulators and operators should take now to keep digital communication secure in the quantum era.

What the study covers

The study maps the fast-moving field of quantum technologies and their impact on secure communication. It introduces the physics behind quantum computing and quantum communication, reviews the global state of development, analyses the threat that quantum computers pose to the cryptography used in 5G networks, and surveys the European and Czech initiatives building a quantum-ready ecosystem. It closes with concrete recommendations for state institutions and regulators.

The second quantum revolution

Quantum mechanics behaves in ways the everyday world does not. Four principles make entirely new applications possible — **superposition**, **entanglement**, the **probabilistic nature of measurement**, and the **no-cloning of quantum information**. Together they underpin three application areas: quantum sensing, quantum communication and quantum computing.

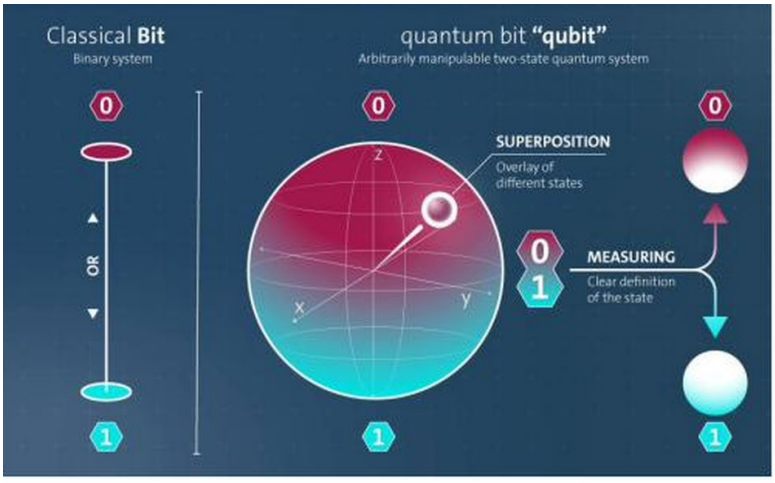

Figure 1 — A classical bit holds 0 or 1; a qubit can hold a superposition of both. Source: study.

From qubits to useful machines

The qubit is the basic building block, realised through superconducting circuits, ion traps or photonic systems. Practical machines require **quantum error correction** and scaling to hundreds or thousands of logical qubits.

By 2025 the leading players — IBM, Google, Quantinuum and Chinese and European teams — reach the order of hundreds of qubits, but devices remain experimental and very costly, with hundreds of millions of USD invested every year. A **hybrid model** — classical computers calling quantum subroutines in the cloud — is expected to dominate for the foreseeable future.

Figure 5 — An IBM quantum computer. Source: study.

Why it matters: the threat to 5G security

Quantum computers will eventually be able to break the asymmetric cryptography (**RSA, ECC**) used in 5G networks for authentication and key exchange; Grover's algorithm also weakens symmetric ciphers, though less severely. The study estimates that current encryption could be broken within **15–20 years, with the risk roughly doubling every five years**. The danger is already present: under ***"harvest now, decrypt later"***, attackers store encrypted traffic today to decrypt it once quantum hardware matures.

Two lines of defence

Post-quantum cryptography (PQC)

New algorithms designed to resist quantum attack. Software-only — runs on existing infrastructure; being standardised by NIST and ETSI.

Trade-offs: larger keys, higher performance demands, shorter security track record.

Quantum key distribution (QKD)

Uses entanglement and the no-cloning theorem to distribute keys and **detect any eavesdropping**; secure even against quantum computers.

Trade-offs: range of tens–hundreds of km without repeaters, cost, dedicated infrastructure.

Europe and the Czech Republic

The EU invests heavily through **Quantum Flagship** (€1 billion over a decade), the **EuroHPC Joint Undertaking** (six quantum systems co-funded across member states, with the Commission covering half the cost) and **EuroQCI** for quantum communication infrastructure — all aligned with the Digital Decade goals. The Czech Republic takes part via **LUMI-Q** (a 24-qubit system at IT4Innovations in Ostrava) and is building the **CZQCI** test backbone linking Prague, Brno and Ostrava, ahead of integration into EuroQCI by 2030.

BY THE NUMBERS

€1 bn	15–20 yrs	100s	2030
EU Quantum Flagship budget over a decade	until current encryption could be broken	of qubits reached by leading machines in 2025	target for Czech integration into EuroQCI

RECOMMENDATIONS FOR REGULATORS

- **Set mandatory minimum methodological rules** for operators on the cybersecurity of 5G and other networks in the quantum era — including a phased PQC migration roadmap, minimum audit and monitoring requirements, a common supplier security-audit procedure, and rules for data protection and personnel.
- **Create a reference register** of PQC-compatible devices.
- **Establish minimum interoperability requirements** between classical and QKD cryptography.

KEY TAKEAWAY

Quantum computing is still experimental, but the security clock is already ticking. Migrating to post-quantum cryptography, adopting QKD for critical infrastructure and modernising networks must begin well before quantum computers mature — a shared priority for regulators and operators across the European Union.