

Quantum: What is it and where does the EU stand?

The emergence of quantum information science and technologies marks a pivotal moment in technological progress. As the strategic importance of quantum gains global recognition, efforts are intensifying to harness its potential while also addressing security and regulatory challenges. With China, the United States and the European Union investing heavily in quantum, the race for technological dominance is well under way.

Introduction

Quantum technologies, a growing branch of physics and engineering, encompass <u>technologies</u> that utilise quantum phenomena to achieve specific goals. With new <u>advances</u> in these technologies, policymakers have started focusing on the opportunities and challenges they present, considering their potential impact in the future. However, the commercialisation of quantum technologies, such as <u>decryption</u> using quantum computers, may take decades to become market-ready, while others, such as quantum-sensing <u>applications</u> for <u>biomedical research</u>, could be ready sooner. In general, the different technologies are based on **quantum information science** (QIS), also referred to simply as **quantum**, which <u>explores</u> how information is processed and transmitted using quantum computing (with quantum simulation as a crucial subfield), quantum communication and quantum sensing. Many governments have realised that financial investment in quantum is crucial for the future, as it offers the possibility to solve complex tasks in a faster and more efficient way – something existing technologies cannot achieve. Currently, policy initiatives in the European Union (EU) and <u>other regions</u> are focusing primarily on funding research and development projects and creating an environment that fosters innovation.

Main quantum technologies

In quantum computing, the multiple positions of '<u>qubits</u>', the basic unit of information in a quantum computer, allow the performance of more <u>complex calculations</u> much faster than by classical computers, thanks to the ability to process a larger volume of data and run extremely intricate simulations. Opportunities for this technology lie, for example, in developing and testing new vaccines and drugs by simulating chemical reactions, saving time and reducing costs. Quantum communication, meanwhile, seeks to provide more secure long-distance communications, making use of two quantum features; first, the creation of encryption keys based on gubits makes it much harder for hackers to break into cryptographic systems; second, qubits are extremely sensitive to external influence, meaning that any third party attempt to intercept the transmitted communication introduces errors that can make the interception attempt visible to both the sender and the receiver. A safe quantum communication method is guantum key distribution (QKD); it enables the secure exchange of cryptographic keys between two parties based on the laws of quantum physics (e.g. entanglement and interference). Quantum sensing uses the high sensitivity and accuracy of particles to measure the slightest changes in physical matter or geographical position. Quantum sensors could supersede the Global Positioning System (GPS) in navigation systems, eliminating the risk of external influence, such as the jamming of GPS signals. The high cost of quantum sensors and their size present major challenges to the broad adoption of this technology however.

How China and the United States are approaching quantum

China's <u>14th five-year plan (2021-2025)</u> provides insight into the country's stance on quantum technology. The plan identifies QIS as a strategic priority for China in terms of strengthening its national defence and fostering economic growth. In accordance with the plan, China has become a <u>pioneer</u> in building **quantum communication infrastructure**, having established a network connecting Beijing and Shanghai through



which data is reportedly transferred with absolute security. Furthermore, China is working on cutting-edge <u>quantum communication satellites</u>, such as the <u>Micius Satellite</u> project for quantum science experiments. In 2018, the United States (US) released its national quantum <u>strategy</u> and launched legislative <u>initiatives</u> envisaging a coordinated approach at the federal level to improve research and development in quantum technology for economic and national security purposes. For example, the US has placed emphasis on <u>advancing</u> the standardisation of **quantum-safe cryptography protocols**, which involves developing new algorithms that are resistant to hacking, including by means of a <u>supercomputer</u>. Furthermore, the <u>National</u> <u>Quantum Initiative</u> allocates funding for investment to advance QIS research and development and to address a wide range of quantum challenges such as workforce development and industry engagement.

What the EU is doing

As part of its overarching digital transformation strategy – the Digital Decade – the EU aims to be 'at the cutting edge of guantum capabilities by 2030'. To this end, the EU has been running a variety of programmes and initiatives, ranging from supporting research in quantum to deploying a quantum secure infrastructure. The Quantum Technologies Flagship initiative provides financial support for EU scientific and industrial excellence. In the area of infrastructure, the EU plans to have its first quantum computers by 2025, at six specific sites. Additionally, the European Quantum Communication Infrastructure Initiative (EuroQCI) envisages safeguarding sensitive data and critical infrastructure by utilising guantum communication technologies to build a terrestrial fibre network connecting strategic sites and space-based secure connectivity using satellites (IRIS²). With its nearly €7 billion public investment in quantum, the EU ranks second only to China. Recognising the strategic value and dual-use nature (civilian and military) of guantum technologies, the Commission has identified them as critical for the EU's economic security, as they are 'considered highly likely to present the most sensitive and immediate risks related to technology security and technology leakage'. The Commission therefore recommends that Member States initiate collective risk assessments of quantum technology. In January 2024, it proposed new initiatives to strengthen economic security. For instance, in the proposal to review the existing regulation on the screening of foreign investments, the Commission proposed listing quantum technologies as crucial for EU security or for public order interests. Some Member States, such as France and Germany, have their own programmes to develop quantum technologies. Member States and the Commission are also working to shield the value chains of these technologies from outside players. In March 2024, 21 Member States committed to making Europe the 'quantum valley' of the world, by signing the European Declaration on Quantum Technologies. The EU cooperates on quantum internationally, for instance with Canada, Japan, South Korea and the US (not least through the EU-US quantum task force).

Recommendations for an EU fit for the quantum age

In September 2023, the Commissioner for the Internal Market, Thierry Breton, announced that he was 'working on a new strategy to make Europe the world quantum valley'. However, despite significant EU public funding for quantum, the EU continues to lags behind its major global competitors, such as the US, in terms of private investment in the sector. In view of this, the Commission's 2023 Report on the state of the Digital Decade recommends supporting start-ups in the budding quantum ecosystem, in terms of technological needs and scaling up. The report also stresses the need to continue the work on establishing an EU federated quantum infrastructure to ensure a secure and hyper-connected quantum ecosystem. On the sovereignty and security front, the **European Policy Centre** (EPC) suggests using the European Chips Act to establish a future European quantum chips factory. However, it advises that restrictive export and import policies should be implemented cautiously, as quantum technologies have low maturity. Finally, the EPC argues that an EU coordinated action plan on the quantum transition is crucial to prevent cybersecurity loopholes and safeguard all Member States. It further recommends creating a new expert group on guantum within the EU Agency for Cybersecurity (ENISA). From an educational and technical standpoint, IBM advises organisations to prepare for potential quantum threats by educating policymakers and other key stakeholders on quantum-safe cryptography. This involves developing new algorithms that are immune to hacking by a quantum computer. Organisations should identify the potential vulnerabilities in their information technology systems and mitigate them by implementing quantum-safe cryptography. Once these measures are in place, they should adjust their operations to ensure that all data are protected.

This document is prepared for, and addressed to, the Members and staff of the European Parliament as background material to assist them in their parliamentary work. The content of the document is the sole responsibility of its author(s) and any opinions expressed herein should not be taken to represent an official position of the Parliament. Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy. © European Union, 2024.