OECD publishing

A QUANTUM TECHNOLOGIES POLICY PRIMER

OECD DIGITAL ECONOMY PAPERS
January 2025 **No. 371**

OECD
BETTER POLICIES FOR BETTER LIVES

This paper was approved and declassified by written procedure by the Digital Policy Committee (DPC) on 20 January 2024 and prepared for publication by the OECD Secretariat.

Note to Delegations:

This document is also available on O.N.E. Members & Partners under the reference code:

DSTI/DPC/STP(2024)3/FINAL

Revised version, February 2025

Corrigendum

Page 36:

Figure 1 has been updated with the correct value for 'European Union (total)' according to the source in the caption (USD 8.4 billion).

Page 36:

The paragraph after Figure 1 has been corrected to align with the values shown in the figure: European Union (total): USD 8.4 billion; Germany (USD 3.3 billion); United States (USD 5 billion); Canada (USD 1.1 billion); Netherlands (USD 1 billion); Japan (USD 0.7 billion); India (USD 0.7 billion).

A quantum technologies policy primer

Quantum technologies represent a new paradigm with potentially groundbreaking applications for digital economies and society. Quantum sensing, computing and communication are significantly expanding technological capabilities to gather, process and transmit information. This paper examines the transformative potential of these technologies by outlining anticipated commercial applications and contributions to tackling societal challenges, as well as the associated digital, privacy, and national security risks. It identifies key policy opportunities and challenges, including the role of government support in nurturing emerging technology ecosystems, addressing constraints in supply chains, and developing a skilled workforce. The paper emphasises the critical role of anticipatory governance and international collaboration in shaping the human-centric and values-based development and use of quantum technologies.

Keywords: quantum technologies, technology convergence, government support for research and development, technology co-operation, anticipatory governance, international collaboration.

Foreword

The OECD Global Forum on Technology (GFTech) fosters strategic dialogue and enables co-operation on topics at the forefront of the digital and technology policy debates. The Forum was launched in 2023 to foresee and get ahead of long-term opportunities and risks presented by technology. It facilitates inclusive, multi-stakeholder and values-based discussions on specific technology policy topics, responding to gaps in existing fora.

The OECD Digital Policy Committee (DPC), in co-ordination with the Committee for Scientific and Technological Policy (CSTP), asked the GFTech to study quantum technologies, considering both their potential benefits and risks. The GFTech event *Future in Flux: Global issues and national strategies* took place in November 2023 to kick off an inclusive dialogue that gathered 340 participants from 50 countries, including leading technologists and managers of national quantum programmes. Building upon this event, the GFTech focus group on quantum technologies was convened in December 2023 and has included 40 research, industry and government experts of 21 nationalities, bringing together a diverse range of perspectives. Rather than building consensus among participating experts, the focus group aims to gather evidence, insights and good practices for the human-centric and values-based governance of quantum technologies.

This paper synthesises the input provided by these experts over a period of ten months. It has been drafted by Andrés Barreneche with the oversight and contribution of Elizabeth Thomas-Raynaud. The paper is based on the substantive points experts discussed in focus group meetings or submitted through written contributions, coupled with a review of the emerging literature that incorporates relevant sources they suggested. It aims to (i) provide an early foundation for governments to understand quantum technologies, their benefits, and risks; (ii) outline the policy opportunities and challenges in unlocking these benefits and mitigating these risks; and (iii) identify ways the OECD could support the human-centric and values-based development and use of these technologies.

The paper benefited from the following experts participating in the OECD GFTech focus group on quantum technologies: Araceli Venegas-Gomez, Claudia Reinprecht, Claudius Klein, Corey Stambaugh, David Hutchinson, Désirée Ehlers, Ferdinand Griesdoorn, Florence Lewine, Geert Van Grootel, Heike Riel, Jen Sovada, Jiri Vala, João Duque, Joris van Hoboken, Josh Fedder, Kai Bongs, Kate Weber, Katsuyuki Hanai, Leonard Woody, Loïc Le Loarer, Mark Stickells, Martin Machin, Masahiro Horibe, Neil Abroug, Nga Chee Wei, Nicolas Spethmann, Nina Granqvist, Óscar Andrey Herrera, Oscar Diez, Pekka Pursula, Petr Kavalíř, Phil Kaye, Richard Parasram, Sabine Tornow, Simone Montangero, Urbasi Sinha, Vaidas Repecka, Veronica Fernandez Marmol, Vicente Martin and Vikram Sharma. They have contributed in their personal capacity, and their input does not necessarily represent the views or positions of the organisations with which they are affiliated. Kako Sugiyama provided research contributions. Colleagues from the OECD Secretariat, Alexia Gonzalez-Fanfalone and Laurent Bernat, kindly reviewed specific content areas.

Table of contents

FIGURES

INFOGRAPHICS

TABLES

BOXES

Executive summary

Quantum technologies represent a new paradigm for digital economies and society. By exploiting the unique behaviours of particles at the atomic and subatomic levels, they offer innovative capabilities to gather, process and transmit information. Quantum sensors already detect and measure physical quantities with unprecedented sensitivity and precision. Quantum computers are expected to solve complex problems that are challenging or even intractable for today's classical computers, achieving processing speeds that can be faster by several orders of magnitude. Quantum communication, in turn, is expected to interconnect multiple quantum sensing and computing devices and strengthen security.

Quantum technologies are anticipated to bring numerous benefits, including a wide range of innovative commercial applications as well as significant contributions to addressing global societal challenges. However, they also pose risks to human-centric values, particularly concerning digital security and privacy. One notable threat is the potential to break current cryptographic methods, which are fundamental to ensuring safety and trust in digital communications and transactions.

Governments have several policy opportunities to harness the benefits of quantum technologies while mitigating the associated risks. Given the long timelines and financial risks involved, many governments have introduced national strategies and funding programmes to develop quantum technologies. Government support plays a crucial role in supporting fundamental research and in helping companies bring commercial opportunities to fruition. In addition to funding measures, establishing benchmarks to assess and compare quantum technological capabilities can help monitor technological progress and guide investments.

Quantum technologies also raise various policy challenges. As international collaboration is needed to advance these technologies, governments face the delicate task of opening their technology ecosystems while safeguarding against misuse, which carries significant implications for national security. Furthermore, there are already signs of skills shortage across the quantum workforce and constraints in the emerging supply chains of critical materials and components. Moreover, the concentration of investments in developed countries risks worsening global inequalities and limiting the economic and societal benefits of quantum technologies.

Considerations around dual-use applications, digital security and privacy, research security, and technology leadership are creating important frictions for international co-operation. Multilateral consensus on what constitutes the responsible development and use of quantum technologies is needed to strengthen trust in cross-border collaborations. Building upon existing international initiatives for the governance of quantum technologies, the OECD could develop a Council Recommendation with principles to reinforce values shared by OECD members for broader engagement. Further in-depth policy work could also support international collaboration efforts.

1 Understanding quantum technologies

Infographic 1. What are quantum technologies?

Quantum physics describes the **unique behaviours** of very small particles, at the atomic and subatomic levels.

Quantum technologies use **quantum effects** directly to gather, process and transmit information. There are three types of quantum technologies:

Quantum sensing measures physical quantities with unprecedented sensitivity and precision.

Types of quantum sensors:

- **Atomic clocks** *(time)*
- **Inertial sensors** *(acceleration)*
- **Magnetometers** *(magnetic fields)*
- **Photon detectors** *(luminosity)*

Quantum computing is expected to solve problems that are challenging or even intractable for classical computers.

Types of quantum computers:

- **Annealers**
  Specialised devices designed to run specific optimisation algorithms.
- **Simulators**
  Model a given natural process that involves quantum effects (e.g. photosynthesis).
- **Universal**
  General-purpose devices designed to run any kind of quantum algorithm.

Quantum communication uses the quantum properties of particles to encode and transmit information.

Applications of quantum communication:

- **Quantum key distribution**
  Encodes cryptographic keys in qubits, aiming to strengthen digital security.
- **Distributed quantum sensing and computing**
  Networks of quantum devices working together to extend measurement and computation capabilities.

What are quantum technologies and what are their capabilities and limitations?

Atoms, electrons, photons and other particles at similar "quantum" scales[1] behave differently from the larger objects we encounter in daily life. The laws and theories of classical physics used to understand the motion of objects, heat transfer, and the interactions between electric charges become inadequate to describe the behaviour of particles at these tiny scales.[2] With the work of renowned scientists such as Max Planck, Albert Einstein, Niels Bohr and Werner Heisenberg, quantum physics emerged in the early 1900s as a revolutionary field of study to explain the peculiar behaviour observed at atomic and subatomic levels. This scientific revolution introduced concepts such as those included in Box 1.

Box 1. Selected concepts describing the unique behaviour of atomic and subatomic particles

- **Wave-particle duality**: Atoms, electrons, photons and other quantum entities can behave like a wave in the water or like a particle with discrete properties like energy and momentum.
- **Uncertainty principle**: It is impossible to simultaneously know the exact values of certain pairs of variables for a quantum system, such as the position and momentum of a particle.
- **Superposition**: A particle can be in an indeterminate, probabilistic combination of multiple places or states at the same time until it is measured.
- **Entanglement**: Particles can become so intricately linked that they cannot be measured or described independently of one another, regardless of how far apart they are.
- **Tunnelling**: Particles can pass through barriers that would be impossible for larger objects, like an electron crossing a transistor thinner than 1-3 nanometres.

Source: Adapted from (University of Waterloo, 2024[1]).

These concepts reshaped our understanding of nature at its most fundamental level, leading to technological breakthroughs in the 20th century, including the transistor, integrated circuits, lasers, the global positioning system (GPS) and nuclear power, known as the "first quantum revolution." Many of these inventions are essential components of computers and the classical[3] information and communication technologies upon which today's digital economies are built (Kleppner and Jackiw, 2000[2]). Other inventions have had significant and direct impacts on well-being across domains such as health: Magnetic resonance imaging (MRI) machines and positron emission tomography (PET) scanners, for example, have significantly advanced medical diagnostics by non-invasively generating highly detailed images of organs' internal structures and functions.

The first quantum revolution relied on classical physics and electronics to observe and process phenomena predicted by the emerging field of quantum physics. Over the past decades, quantum information science and technology (QIST) has emerged as a new field in which quantum effects are used directly to gather, process and transmit information (Hoofnagle and Garfinkel, 2022[3]). Quantum sensing, computing and communication harness the unique behaviours of tiny particles to create and extend technological capabilities, heralding a second quantum revolution.

Quantum sensing

Quantum sensors use the unique properties of quantum physics to gather information. More specifically, they detect and measure physical quantities such as mass, time and luminous intensity with unprecedented sensitivity and precision.[4] Quantum sensors enable measurements at previously unattainable scales and accuracy. They are built to be sensitive to the smallest perturbations found in

nature (Hoofnagle and Garfinkel, 2022[3]). Quantum sensors can therefore detect minute changes in physical quantities beyond the capabilities of classical sensors. Table 1 describes several types of quantum sensors, their maturity and advantages over conventional sensors.

Most mature applications of quantum technologies are found in the sensing branch, with first-generation devices that use classical physics and electronics to measure quantum effects having already resulted in innovations across various fields such as positioning, navigation, and biomedical, chemical and materials sciences (US NSTC, 2022[4]). Quantum magnetometers (devices that measure magnetic fields used in MRIs and PETs) and atomic clocks are already among the most sensitive and accurate devices that exist. Geo-localisation using GPS would not have been possible without atomic clocks.[5] Ensuring that network equipment synchronises with atomic clock standards is crucial for preventing data loss and maintaining service quality in telecommunications (Quddus Islam and Garlick, 2024[5]). Table 1 includes various examples of second-generation devices that use quantum effects to make measurements.

Table 1. Types of quantum sensors

Type	Description	Maturity	Quantum advantages
Atomic clocks	Highly precise timekeeping devices that use the properties of atoms to measure time. Unlike regular clocks that rely on mechanical parts or electrical signals, atomic clocks measure time based on the consistent and predictable oscillations of atoms.	Caesium atomic clocks are highly mature technologies, widely used and integrated into numerous critical systems, including GPS. Optical atomic clocks are in the advanced prototype and demonstration stages.	A good quality quartz wristwatch might drift by about 15 seconds per month, i.e. a few minutes per year. In comparison, a caesium-based atomic clock is 10^{11} more precise, whereas optical atomic clock is expected to be 10^{15} more precise.
Quantum gravimeters	Devices measuring the strength of gravitational fields using atoms. Atoms are ideal for precise measurements because their exact mass is known, unlike man-made objects in classical gravimeters that can vary in mass when manufactured or manipulated.	They have demonstrated promising results in controlled environments, but their deployment is still limited due to challenges in miniaturisation, cost and operational complexity.	Quantum gravimeters currently perform at similar levels of precision to classical gravimeters but are expected to yield 10-100x improvements in instrument sensitivity. They will also enable accurate measurements in moving vehicles or aircrafts.
Quantum inertial sensors	Devices that use quantum particles, like atoms or ions, to detect changes in position, speed and direction. They provide more reliable data even in environments where traditional systems might struggle, such as deep underwater, underground or in densely built urban areas without proper access to GPS signals.	Significantly more accurate gyroscopes based on cold atoms are being developed.	At least a 50x improvement in bias stability over classical accelerometers, according to recent experiments.
Quantum magnetometers	Devices using particles like electrons or atoms to measure the strength of magnetic fields.	These are already widely used in practical applications such as medical imaging. New devices are emerging that are portable and do not require cooling.	Quantum magnetometers can detect changes in magnetic fields that are approximately six orders of magnitude (10^6) weaker than what classical magnetometers can detect.
Quantum electrometers	Devices that use atoms to measure the strengths of electric fields (radio frequencies). They can measure a broad range of frequencies, making them versatile for various technological applications.	Companies already manufacture various kinds of quantum-enabled radio frequency sensing solutions.	Neutral atom-based sensors can analyse frequencies from direct current (0 Hz) to the THz (10^{12} Hz) range. The typical range for classical spectrum analysers is between around 9 kHz (10^3) up to several tens of GHz (10^9).
Photon detectors	Devices using photons and their quantum properties to detect and analyse some of the faintest possible sources of light. They are used in a wide range of applications, from cameras and telescopes to scientific experiments.	Photon counters and other types of detectors are already commercially available. More advanced quantum imaging approaches are in development.	Quantum imaging is expected to improve satellite-based sensing, enable the detection of objects that are not in direct view (ghost imaging) and counter stealth technology (quantum radar).

Source: (Quddus Islam and Garlick, 2024[5]; Ezratty, 2023[6]; Hoofnagle and Garfinkel, 2022[3]; Rauscher, Janssen and Minihold, 2001[7]).

Quantum computing

Quantum computing is emerging as a new paradigm for processing information by leveraging quantum effects. Unlike classical computers that use bits to represent either a 0 or a 1, quantum computers use quantum bits (qubits), which can represent 0, 1 or any value in between through the use of superposition. Moreover, entanglement allows qubits to become interconnected: When qubits are entangled, the state of one qubit becomes intricately correlated with the state of another. The unique abilities of superposition and entanglement are expected to allow quantum computers to solve certain complex problems that are challenging or even intractable for classical computers. John Preskill coined the term "quantum advantage" to describe the anticipated milestone when quantum computers outperform classical computers in solving certain computational problems (Preskill, 2012[8]).

Physicist and Nobel Prize winner Richard Feynman initially proposed quantum computing in 1981 as a method to simulate the quantum behaviours observed in nature, including in chemistry and biological processes, which would lead to impactful applications in fields such as energy (e.g. fusion reactions), pharmaceuticals (e.g. synthetic biology) and the automotive industry (e.g. battery development). Since the 1990s, there has been notable progress in quantum algorithms, i.e. instructions for calculations that leverage the distinct capabilities of quantum computers. By the end of the last century, key developments in cryptanalysis (leading to the digital security risks discussed later in this paper), search and optimisation highlighted the potential of quantum computing, sparking increased enthusiasm and funding in the field.[6] More specifically, researchers provided mathematical proofs demonstrating that qubit-based computers can solve certain problems more quickly than their bit-based counterparts, including Feynman's proposed simulation of quantum processes (Dalzell et al., 2023[9]).

Since the experimentations with qubits in the 1990s, several types of quantum computers have been developed. The main ones are described below:

- **Quantum emulators** allow quantum algorithms to run on standard computers, from laptops to supercomputers, depending on the number of qubits, algorithm complexity and precision needed. Emulation allows these algorithms to be tested without requiring actual quantum computers. Currently, supercomputers can emulate around 50 qubits.
- **Quantum annealers** use specific materials to achieve quantum effects. Qubits are physically linked through the material, i.e. they operate in an analogue mode akin to how punching cards were used to operate the first classical computers. This mode of operation limits annealers to a narrow set of optimisation algorithms.
- **Quantum simulators** are also analogue ad hoc devices. They are designed to simulate a given natural process that involves quantum effects, often to tackle a specific scientific problem, such as understanding photosynthesis. Unlike quantum annealers, which are constrained to optimisation, different quantum simulators have been constructed to simulate various kinds of quantum effects in fields such as materials science, chemistry and cosmology.
- **Universal quantum computers**: As opposed to annealers and simulators, these operate with quantum gates, i.e. instructions or operations to process information in qubits. This mode of operation enables them to execute any quantum algorithm, even though quantum annealers and simulators are generally more efficient in running the algorithms they are designed for. There are two types of universal (or general purpose) quantum computers:
  - **Noisy intermediate-scale quantum computers (NISQs)**: These are the most advanced quantum computers currently available. They are considered intermediate in size and capability compared to the quantum computers envisioned for the future.
  - **Fault-tolerant quantum computers**: These are the theorised large-scale and stable devices capable of reliably performing quantum computations over extended periods.

Annex A provides additional details on quantum computing. It explains the distinction between classical bits and qubits and describes selected quantum algorithms.

Quantum sensing is a foundational technology for quantum computing, as quantum computers use quantum sensors to extract information. While the extreme sensitivity to the smallest disturbances observed in nature is a strength for quantum sensing, it is a critical weakness for quantum computing (Box 2). The superposition and entangled states in qubits, necessary for computation, are susceptible to such disturbances, or "noise", thus causing qubits to "decohere" (i.e. to lose their quantum properties), resulting in loss of information and computation errors.

Box 2. Dealing with quantum noise

Environmental noise, including thermal fluctuations and electromagnetic interference, represents a significant challenge for quantum computing. While the transistor allowed classical computers to scale with stability, quantum computing requires the management of extremely fragile quantum states. Recent devices cannot maintain coherence for the length of time needed to process large numbers of operations.

Today's most advanced superconducting chips experience decoherence errors in entangling two-qubit operations every 100 or 1 000 operations, corresponding to error rates between 1% and 0.1%. Error rates of 0.1% are estimated to require over 100k physical qubits to enable impactful applications in quantum chemistry or materials science. This is far beyond the capacity of today's most advanced machines; IBM's most powerful quantum chip, Condor, has 1 121 qubits. Manufacturers aim to reduce error rates by three orders of magnitude, to about one every million operations or 0.0001%, a threshold at which error-correction techniques become more viable.

Researchers and manufacturers have developed three main solutions to decoherence errors:

- **Error suppression** focuses on using classical software and machine-learning algorithms to continuously monitor and analyse the behaviour of quantum circuits and qubits. By adjusting circuit designs and instructions, error suppression aims to better protect the information stored in qubits.
- **Error mitigation** targets errors that do not cause a computation to fail outright but rather disrupt its accuracy. Similar to noise-cancelling technology, this method applies corrections during computation based on the noise patterns observed in specific quantum systems. While not perfect and requiring multiple runs of algorithms, it effectively reduces errors in the final output.
- **Quantum error correction** is a more advanced approach where information is encoded in a set of physical qubits to form a logical qubit. Monitoring and correcting errors across logical qubits helps detect and rectify noise-induced errors before they render the information unusable. Recent breakthroughs in error correction using logical qubits have promised to resolve quantum noise sooner than previously expected.

Source: (Hoofnagle and Garfinkel, 2022[3]; Brooks, 2024[10]; Pasternack, 2024[11]; Preskill, 2021[12]).

Just like in the early days of classical computing before silicon became the standard, a diverse range of hardware platforms is currently being considered for universal (general purpose) quantum computers, including superconducting circuits, neutral atoms, trapped ions and photon-based qubits, among others. Each of these platforms has strengths and weaknesses in terms of maintaining coherence and ability to scale,[7] and it remains unclear which one, if any, may ultimately lead to fault-tolerant quantum computers. Regardless of the hardware platform, quantum computers are currently not advanced enough to perform

useful calculations beyond the capabilities of classical computers (Gamble, 2019[13]; Devitt, 2024[14]). Several quantum computing companies have made claims of quantum advantage for specific applications, but follow-up research has challenged some of these claims (Ball, 2020[15]; Patra et al., 2024[16]).

In addition to decoherence errors, there are other challenges before the promises of quantum computing can come to fruition (Hoefler, Häner and Troyer, 2023[17]):

- **Bandwidth**: The slow operational speeds of qubits fundamentally restrict the rate at which classical data can be transferred into and out of a quantum computer. This implies that, for the foreseeable future, quantum computers will likely be practical for solving complex problems on small datasets, rather than addressing data-intensive applications such as machine learning or database searching.
- **Limited speedup gains**: Quantum algorithms show exceptional promise in applications such as simulating quantum processes, solving complex physics problems in areas like materials science and chemistry). However, the potential for significant speedup in several other applications remains uncertain (see Annex A). Many applications may not experience substantial performance improvements over classical computers without significant developments in quantum algorithms.

Despite these challenges, several manufacturers of quantum chips are continuously demonstrating progress towards fault-tolerant quantum computers (Waters, 2024[18]; Boger, 2024[19]). In particular, recent advances show promising steps towards overcoming high error rates. Governments, researchers, large companies and startups worldwide are actively working to develop commercially viable applications and start realising the potential of quantum computing. Experts participating in the GFTech focus group on quantum technologies anticipate the first applications to emerge in the simulation of quantum processes observed in nature, as initially suggested by Feynman.

Quantum communication

Quantum communication uses the quantum properties of particles to encode and transmit information. On the one hand, this enables the exchange of information across distant quantum sensing and computing devices through quantum networks (Kimble, 2008[20]). Distributed quantum sensing involves using networks of interconnected quantum sensors that share entangled quantum states to achieve more precise and efficient measurements (Zhang and Zhuang, 2020[21]). Quantum networks also have the potential to support distributed quantum computing, where interconnected quantum processors work collectively to solve complex computations that are far beyond the capabilities of individual processors (Cuomo, Caleffi and Cacciapuoti, 2020[22]).

Today's cryptographic methods rely on classical bits both for the transmission of secret keys and encrypted data. Quantum key distribution (QKD) creates secret keys encoded in qubits and sent in a quantum network, aiming to strengthen security (OECD, 2024[23]). Unlike traditional cryptographic methods relying on mathematical calculations, QKD seeks to secure communication based on nature's physical (quantum) laws.[8] As qubits are highly sensitive to observation, any attempt to intercept them causes them to decohere and introduce detectable errors. These errors can be noticed by the recipient, alerting them to the interception, and they also render the eavesdropped information unusable. QKD thus aims to offer robust protection for transmitted data, making eavesdropping exceedingly difficult to succeed and go undetected.

Like quantum computing, quantum communication networks need to surmount several engineering and deployment challenges before they can be commercially viable (Box 3). While QKD has been successfully demonstrated over fibre, spectrum radio frequencies and satellite relays, each medium presents challenges. QKD has been limited to short distances of about 100 km, and space-to-ground applications have shown mixed results, requiring further technological progress for commercial viability. However, recent advances and experiments demonstrate progress in overcoming these challenges (Lai et al., 2023[24]; Korolov, 2024[25]; Garms et al., 2024[26]). Quantum repeaters, for example, are being developed

as intermediate network nodes that extend the transmission range of quantum information. QKD networks have already been established and trialled in countries such as the United Kingdom, the Netherlands, the United States and the People's Republic of China (hereafter "China") (OECD, 2024[23]). Section 3 elaborates on the opportunities and challenges of QKD in strengthening the security of digital communications.

Box 3. The main technical challenges of quantum communication

- **Noise, decoherence and distance limitations**: The design of a quantum network needs to account for the constraints imposed by environmental noise and quantum decoherence, which result in information loss over long distances. Entanglement eventually decays regardless of the medium. In addition, satellite-based quantum communication can be affected by weather conditions.
- **Specialised hardware and high costs**: Quantum communication requires specialised equipment, such as single-photon sources and detectors, which are currently expensive to acquire and maintain. Quantum information is typically encoded in matter qubits (like ions or superconducting circuits) and transferred via flying qubits (usually photons). Different qubit technologies and transmission mediums (such as optical fibres or free-space channels) add complexity, requiring versatile interfaces adaptable to diverse quantum hardware and environments.
- **Deployment challenges**: Implementing a quantum network involves overcoming significant technical and logistical barriers. Quantum processors and communication technologies are still in early stages of development. Integrating different quantum devices with existing classical networks poses unique challenges, requiring new protocols and infrastructure to support hybrid quantum-classical communication seamlessly.

Source: (Cacciapuoti et al., 2020[27]; ANSSI et al., 2024[28]).

While researchers often refer to quantum networks as the "quantum Internet," GFTech focus group experts consider this parallel unhelpful and misleading. On the one hand, this comparison suggests quantum networks could succeed or surpass today's Internet, whereas, in reality, the applications described above are expected to complement rather than replace existing communication infrastructures. On the other, relative to today's Internet, quantum networks are expected to remain more costly and, for the time being, limited in deployment scale.

As discussed in the preceding paragraphs, quantum technologies vary significantly in their maturity levels. Table 2 maps the estimated technology readiness levels across selected quantum technologies. Some sensing applications, like magnetometers, have achieved the highest maturity, including full operational proof and commercialisation. In contrast, radar sensing and inertial navigation are at lower readiness levels, as these have only been validated in specific lab conditions. Quantum key distribution in communication has demonstrated prototype operations in real-world settings. Quantum computing, in contrast, is further away from commercialisation. Annealers are being demonstrated in relevant environments. Universal quantum computers only display early-stage experimental proof. This diversity in readiness levels highlights the varying stages of development and implementation across quantum technologies.

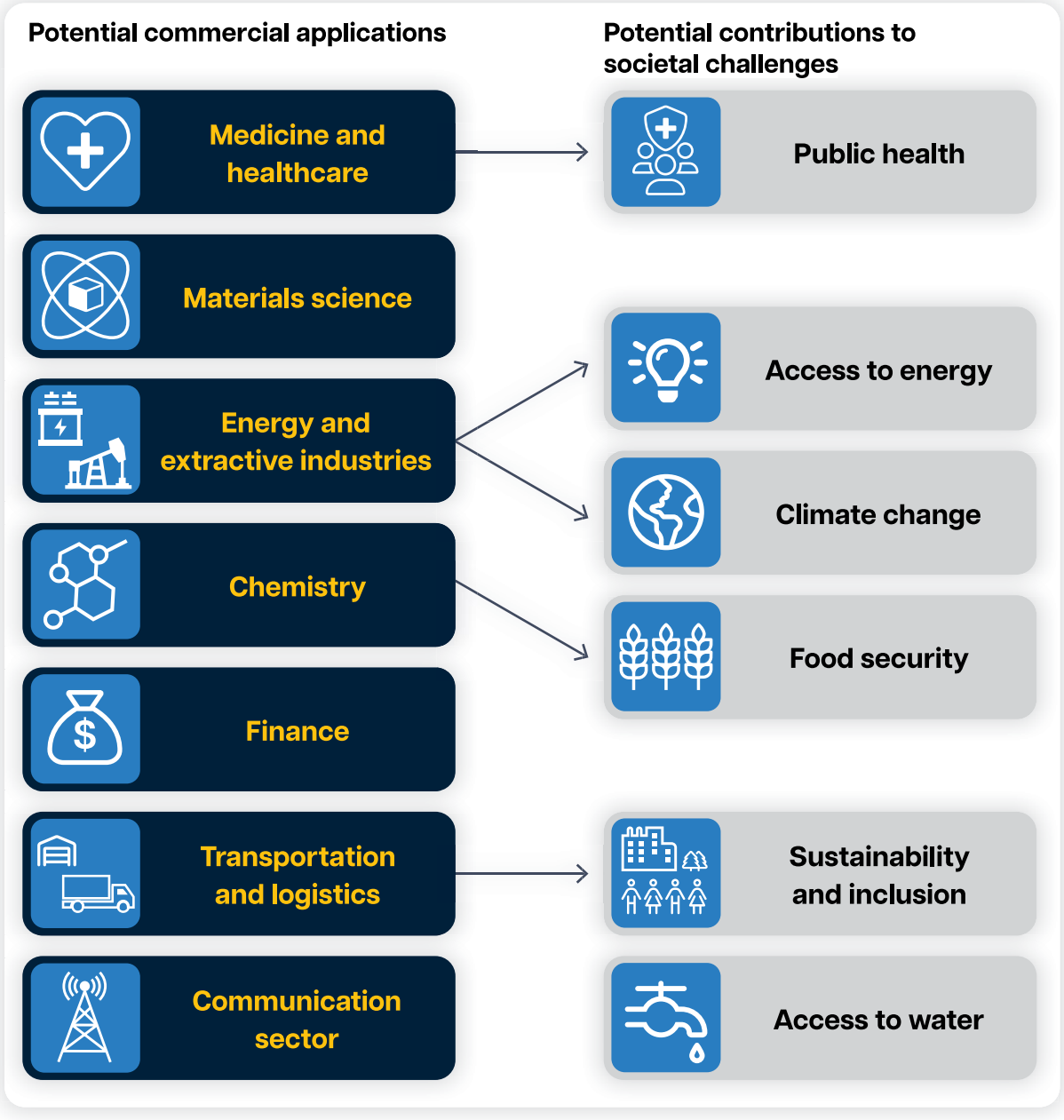
Table 2. Estimated technology readiness levels for selected quantum technologies

	Technology Readiness Level (TRL)								
Quantum technology	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
Sensing (magnetometers)									■
Sensing (radar)				■					
Sensing (inertial navigation)				■					
Communication (QKD)							■		
Computing (annealer)					■				
Computing (universal)			■						

Notes: TRL 1: Basic principles observed; TRL 2: Technology concept/application formulated; TRL 3: Analytical and experimental proof of concept; TRL 4: Technology validated in lab; TRL 5: Technology validated in relevant environment; TRL 6: Technology demonstrated in relevant environment; TRL 7: System prototype demonstration in an operational environment; TRL 8: System complete and qualified; TRL 9: Actual system proven in an operational environment.
Source: (Purohit et al., 2024[29]).

2 Technology benefits to be unlocked

Infographic 2. What are the potential socio-economic benefits of quantum technologies?



Potential commercial applications

In today's digital economies, data serve as a foundational resource that drives innovation and economic growth. Once sufficiently mature, the advanced capabilities of quantum technologies in data gathering, processing and transmission will be a source of productivity gains and competitive advantage across various business activities. This section includes a non-exhaustive review of potential commercial applications of quantum technologies. It remains uncertain whether the computing applications described below can be viable even with the arrival of large-scale fault-tolerant quantum computers. Some of these opportunities rely on specific quantum algorithms whose ability to outperform classical ones can only be assessed once sufficiently powerful quantum computers become available. Technology providers are actively working with researchers and companies to scope use cases and attract investment in quantum sensing, computing, and communication.

Medicine and healthcare

First-generation quantum sensing devices like MRI machines and PET scanners have already made significant contributions to medicine and healthcare. Second-generation technologies are expected to continue improving the quality of medical imaging and diagnosis, uncovering hidden complexities within the human body (Shams et al., 2023[30]). Quantum sensors are expected to track the effectiveness of medical treatments by monitoring the effects of medication at the cellular level in real-time (Chugh et al., 2023[31]). They could enhance the accuracy of medical diagnoses, potentially detecting diseases earlier when they are easier to treat. This includes the detection and precise monitoring of diseases such as Alzheimer's and Parkinson's (Chamkouri et al., 2024[32]). Quantum sensors enable the real-time electromagnetic monitoring of organs, enhancing the treatment of neurological and cardiac disorders (Aslam et al., 2023[33]). In cancer treatment, they offer the potential to precisely identify the boundaries of tumours (Chugh et al., 2023[31]). This can lead to more targeted and effective treatments, reduced damage to healthy tissues and better patient outcomes. Wearable biosensors can further integrate into daily life, continuously and non-invasively monitoring vital signs and biochemical markers (Das et al., 2024[34]). These sensors could also facilitate drug development, for example by monitoring drug interactions with target molecules. They support personalised medicine by enabling real-time adjustment of treatment doses, tailoring them to individual patient needs.

In recent years, there has been a surge of quantum computing experiments and scoping studies for applications in medicine and healthcare (Ur Rasool et al., 2023[35]; Flöther, 2023[36]). Quantum computers could sequence DNA at unprecedented speeds, enabling the development of tailored treatments based on an individual's genetic profile. Moreover, quantum computing shows potential in drug discovery by simulating molecular structures and interactions in ways that are unachievable or challenging using classical computers.[9] Quantum computers could raise the accuracy and speed of diagnostics and improve predictions of how patients will respond to treatments.

Materials science

Quantum sensors enable the highly sensitive detection and visualisation of even the smallest defects in materials (Fraunhofer IAF, 2024[37]). They can identify material fatigue before cracks and other visible signs appear. Early detection is essential for preventing failures in safety-critical components. This capability is crucial for industries like aerospace and automotive, where ensuring the reliability and safety of materials is paramount. Additionally, quantum sensors could shorten measurement times, enhancing efficiency in industrial processes such as component testing. Quantum sensors are also being explored to optimise heat dissipation and thermal management of materials used in electronics (Zhao et al., 2023[38]) with potential applications in the generation of thermal energy from electricity and in high-performance computing, where heat generation is a significant challenge.

Quantum computing could simulate complex materials with unprecedented accuracy (Fedorov et al., 2022[39]; Paudel et al., 2022[40]). This capacity would allow researchers to model different configurations and compositions of materials to achieve desirable characteristics such as strength, conductivity or magnetic properties. This could, for example, lead to high-temperature superconductors that enable lossless electrical transmission, potentially making electric appliances, electronic devices and overall electricity grids more efficient. Moreover, quantum computing is also being explored to simulate advanced materials like graphene and heterostructures, which have unique properties and potential applications across various industries. Quantum computers also promise to identify and predict rare failures in production processes (Bova, Goldfarb and Melko, 2021[41]). In industries where failures are infrequent but costly, such as semiconductor manufacturing, pinpointing the exact cause of these failures can be challenging due to the vast number of possible sequences and variables involved. By improving the prediction of rare failures, quantum computing solutions could lead to fewer disruptions and more consistent production, thereby improving manufacturing efficiency.

Energy and extractive industries

Quantum sensing technologies are set to significantly improve efficiency and safety in the energy sector across various applications (Crawford et al., 2021[42]). They offer new capabilities in monitoring energy infrastructure, such as early detection of equipment failures, which could enable predictive maintenance and reduce costs. In the production of nuclear energy, sensors could help improve safety through early detection of radiation breaches and facilitate remote monitoring of power plant operations.

Quantum sensors promise to bring about substantial improvements in efficiency, reliability and environmental sustainability in extractive operations (Quddus Islam and Garlick, 2024[5]). Gravimeters and magnetometers can detect oil or gas reserves and mineral deposits. In the future, they may not only pinpoint the location of these resources but potentially determine their size, shape or depth more accurately. This capability could lower exploration expenses and lead to more effective extraction methods. Moreover, by reducing the need for extensive drilling, there could be significant environmental benefits, such as reducing the risk of oil spills and groundwater contamination.

Quantum computing could expedite the development of new technologies needed to meet increasing energy demand and ensure environmental conservation (Paudel et al., 2022[40]). Quantum simulation is anticipated to lead to the discovery of new materials and processes that are more energy-efficient and environmentally friendly. Additionally, quantum machine learning could enhance carbon capture technologies by rapidly identifying materials with optimal CO2 absorption. Optimisation algorithms may help link power supply sources with consumption points like homes and industries more efficiently, supporting reliable grid operations. Quantum machine learning algorithms could improve energy demand forecasting and optimisation. Such algorithms could also contribute to the modelling, simulation and control of renewable energy systems (Ajagekar and You, 2022[43]).

Chemistry

Quantum computing has several expected applications in chemistry, as it will enable detailed simulations of molecules and their reactions (Fedorov et al., 2022[39]). Future progress could, for example, lead to breakthroughs in understanding nitrogen fixation by the enzyme nitrogenase, occurring naturally in certain bacteria, which allows obtaining ammonia at room temperature and standard pressure. Today, the established ammonia production process is significantly energy-intensive, accounting for about 2% of global final energy consumption, predominantly sourced from fossil fuels (IEA, 2021[44]). This results in a global CO2 footprint equivalent to the total emissions of South Africa's energy sector. Finding an alternative like nitrogenase could lead to cleaner ammonia production methods, thereby significantly reducing the environmental impacts of fertilisers. It is estimated that the nitrogen fixation process can be simulated using four million physical qubits in four days of runtime, under certain assumptions including error rates of 0.1%

or lower (Lee et al., 2021[45]). Quantum simulations also extend to studying how molecules interact with light, which could deepen our understanding of biological processes like photosynthesis and vision.

Finance

Atomic clocks already help ensure precise and reliable timekeeping in financial markets, particularly in the realm of High-Frequency Trading (Quddus Islam and Garlick, 2024[5]). Each GPS satellite contains multiple atomic clocks, which major financial institutions and other businesses use to create precise timestamps for transaction (GPS.gov, 2022[46]). By timestamping trades with accuracy down to microseconds (millionths of a second), atomic clocks facilitate transparent and orderly market operations. Quantum timing thereby contributes to financial regulatory compliance and mitigates risks associated with market manipulation and abrupt price fluctuations (RHC, 2024[47]).

Quantum computing could lead to several applications in the finance sector (Bruno, 2023[48]). Financial risk analysis, i.e. the assessment of the likelihood and potential impact of financial loss on loans or investments, could be done more efficiently using quantum computing algorithms. Quantum algorithms could also yield an exponential speedup in credit scoring used to assess loan applications.[10] Quantum optimisation is also being explored to support transaction settlements in clearinghouses. In particular, quantum computing annealers are being tested for various applications in finance (Fedorov et al., 2022[39]), including portfolio optimisation, forecasting crashes, finding optimal trading trajectories, optimal arbitrage opportunities, optimal feature selection in credit scoring and foreign exchange reserves management.

Transportation and logistics

Quantum sensors could significantly contribute to the development of electric vehicles by improving the assessment of battery health (Berger et al., 2021[49]). Currently, it remains challenging to accurately measure the critical aspects of battery performance that affect the efficiency and lifespan of batteries in electric vehicles. Quantum sensors could help to better understand how batteries degrade over time, potentially leading to better diagnostics and maintenance, thereby extending their usefulness and reliability. Additionally, a more accurate assessment of ground conditions enabled by quantum sensors could also benefit large-scale civil engineering projects, such as building tunnels and railways.

Applications of quantum computing in materials science are also expected to advance electric vehicles, by enabling the design of next-generation batteries and supercapacitors. In addition, quantum computing holds potential to improve transportation and logistics (QED-C, 2024[50]). One promising application is route optimisation across various transportation modes. Quantum algorithms could efficiently handle larger and more intricate routing models. Another critical area is the design of transport operations and schedules, which involves forecasting demand and fleet needs, including crew, vehicles and cargo, and developing comprehensive plans that meet those needs. Quantum computing could offer solutions that integrate these variables to help optimise operational efficiency.

Communication sector

Quantum networks hold promise for securing communications in certain applications (Singh et al., 2021[51]; Liu et al., 2022[52]). They have the potential to enhance the security of data centres and data transfer in sectors such as finance and banking, stock trading and healthcare. In London, BT and Toshiba are pioneering the world's first commercial quantum-secure metropolitan network. This network is being trialled by companies such as HSBC and EY for secure financial transactions and encrypted video communication (TechInformed, 2023[53]). Demonstrations of quantum communication technologies have been used to secure data transfers between Siemens data centres in the Netherlands (Infosecurity Magazine, 2010[54]), and for cloud services in companies like Acronis and Alibaba in China (Huang et al., 2021[55]). Researchers at the United States Oak Ridge National Labs demonstrated the feasibility of using QKD to improve the

security of critical infrastructure, namely the energy grid (Alshowkan et al., 2022[56]). The European Commission is working with all 27 EU Member States and the European Space Agency to design, develop and deploy the European Quantum Communication Infrastructure (EuroQCI), which will be composed of a terrestrial segment relying on fibre communication networks linking strategic sites at within and across countries, and a space segment based on satellites.[11] EU Member States are leading national projects developing quantum communication networks that will form the basis of the terrestrial segment. For example, EuroQCI Spain aims to design a national quantum communication architecture starting with nodes in Madrid and Barcelona, deploying QKD systems and demonstrating their functionality. It aims to make quantum networks available for public authorities (extendable to private sector use) and prepare for long-distance quantum links compatible with the EuroQCI architecture.

While the commercial applications described above could significantly contribute to socio-economic prosperity, quantum technologies have critical dual-use implications. They have impactful defence applications across various domains, including land, air, space, cyber and underwater (Box 4). Although outside of the scope of the OECD, these raise national security concerns that have implications for countries' policy approaches to developing and using quantum technologies, including support for research and development, skills development, supply chain management and international co-operation. These implications will be explored in sections 4 and 5.

Potential contributions to the Sustainable Development Goals

While most quantum technologies are at early stages of development, potential applications that contribute to societal benefits provide strong arguments for public investment outside of economic and defence considerations (Kop et al., 2024[57]). Potential contributions to societal challenges also motivate interdisciplinary and international collaboration, which is necessary to tackle the various science and engineering obstacles these technologies face. Several of the commercial applications raised in the previous section have the potential to advance the United Nations' 2030 Sustainable Development Goals (SDGs), including good health and well-being (SDG 3) and affordable and clean energy (SDG 7). This section describes additional potential contributions across four other SDGs: zero hunger, clear water and sanitation, sustainable cities and communities, and climate action.

SDG 2: Zero hunger

Combined with other technologies, quantum computing has the potential to support smart agriculture in various ways. Its advanced computational capabilities could help optimise farming practices, improve productivity, and contribute to a more sustainable and efficient agricultural sector (Maraveas et al., 2024[58]). Quantum technologies are being explored to optimise crop production, resource allocation, as well as to better monitor crop health and stress levels. In addition, quantum computing could aid in developing next-generation fertilisers and alternatives to pesticides and herbicides, such as protein-based crop protection, which are more cost-effective, environmentally friendlier and safer to use. It could accelerate genetic analysis in crops and breeding processes, raising productivity in agriculture.

SDG 6: Clean water and sanitation

Quantum technologies offer promising solutions for water management and purification. Quantum gravimeters could, for example, help monitor underground water reservoirs (Quddus Islam and Garlick, 2024[5]). As groundwater constitutes the majority of the Earth's freshwater, these reservoirs are vital for supplying drinking water and supporting agriculture globally. Accurate monitoring is essential for their effective management and maintenance. Additionally, quantum-enabled optimisation could improve the

efficient distribution and management of water, potentially reducing water waste and scarcity (Etim, 2022[59]).

Box 4. Potential defence applications of quantum technologies

Quantum sensing

Quantum sensors have implications for intelligence, surveillance and reconnaissance capabilities. They could improve navigation and detection systems, particularly in environments where GPS signals are unreliable, such as underwater or underground. Quantum sensors could detect minute changes in magnetic and gravitational fields, identifying hidden structures like tunnels or mines and locating submarines from greater distances than current technologies allow. They could be used for detailed environmental monitoring, such as detecting chemical, biological, radiological and nuclear threats. Additionally, quantum imaging could provide better image resolution and the ability to see through obstacles such as fog, smoke or even walls. Quantum illumination, which uses entangled photons, could significantly improve the detection of stealth aircraft. In turn, these and other quantum sensing applications enable stealth, allowing their use without detection. Quantum sensors are also expected to resist electromagnetic interference and jamming, which enhances their reliability compared to classical sensors.

Quantum computing

In a defence context, quantum computing could be applied to optimise logistics and supply chains, simulate battlefield scenarios and improve decision-making processes. Quantum algorithms could process data from quantum sensors and other intelligence sources to provide deeper insights and more accurate predictive analytics. In addition, quantum computing could be used to develop new weapons, such as advanced chemical and biological warfare agents, as well as materials and drugs that counter them. It could also extend artificial intelligence applications, leading to more autonomous and efficient military systems.

Quantum communication

In theory, quantum networks could help secure direct communication between military units and command centres. Additionally, quantum clocks could be used to improve the accuracy of coordinated military operations, ensuring that all systems operate in unison. If various technical challenges can be resolved, which remains uncertain, satellite-based quantum communication networks could provide long-distance coverage for secure military communication.

NATO's strategy for quantum technologies

NATO's strategy for quantum technologies aims to ensure the Alliance is "quantum-ready" by fostering a secure, resilient and competitive quantum ecosystem. This involves coordinated investment, technological co-operation among Allies, development of a skilled workforce, and the integration of quantum technologies into defence planning and capability development. NATO seeks to harness these technologies for superior computing, communication and situational awareness while transitioning to quantum-safe cryptography to protect against quantum-enabled threats. The strategy emphasises collaboration within a Transatlantic Quantum Community and responsible innovation. It aims to position NATO as a leading forum for defence-related quantum technology developments, ensuring the Alliance maintains a technological edge that safeguards against adversarial use.

Source: (Krelina, 2021[60]; Hoofnagle and Garfinkel, 2022[3]; Quddus Islam and Garlick, 2024[5]; NATO, 2024[61]).

Improving the quality of drinking water is a major challenge in the industry, which various quantum technologies can help tackle (Gent, Lefebvre and Dessibourg, 2022[62]; Quantum Delta NL, 2023[63]). For example, highly sensitive quantum sensors could improve the detection of harmful substances in water. Quantum simulations could aid in the development of new filters or materials that break down toxic contaminants, making water safer for consumption. Currently, classical machine learning models are being used to predict how substances distribute on the surface of liquids. In the future, quantum machine learning could extend these solutions and provide deeper insights into water quality. Taken together, these developments could make monitoring, treating and improving water quality more cost-effective.

SDG 11: Sustainable cities and communities

Sustainable cities and communities need improved urban planning and greener transportation systems. Quantum computing could contribute to the development of new materials that enhance building strength and create better urban planning models to raise air quality and reduce urban heat stress (Etim, 2022[59]). As mentioned previously, quantum technologies can help address environmental challenges linked to transportation by monitoring and optimising traffic flows, ultimately reducing the sector's carbon footprint. Quantum sensing and computing could also improve the accuracy of climate and weather forecasting, as well as the prediction of natural disasters such as droughts, earthquakes and flooding (Nammouchi, Kassler and Theorachis, 2023[64]).

SDG 13: Climate action

Quantum optimisation and simulation could accelerate decarbonisation by optimising energy usage and reducing carbon emissions. Several commercial applications in energy and extractive industries raised above could contribute to reaching net zero targets. In particular, the use of quantum simulation algorithms in chemistry and materials science could aid in the development of renewable energy technologies, battery technologies or carbon emission elimination methods (Berger et al., 2021[49]; Etim, 2022[59]). Moreover, the use of quantum computing for climate and weather models could support climate action through better forecasting of wind and solar energy production and carbon prices (Nammouchi, Kassler and Theorachis, 2023[64]).

Technology providers and universities are organising competitions to engage researchers and industry experts in identifying and exploring quantum technology use cases that contribute to attaining the SDGs. For instance, the French quantum computing company PASQAL organised a contest in October 2023 (de Castro et al., 2023[65]), proposing six application areas linked with SDGs where neutral atom-based quantum computing could make impacts: sustainable agriculture, drug discovery, smart cities, smart grids and affordable/clean energy, sustainable transport, industry and circular economy, and environment, climate and biodiversity. The University of NYU Abu Dhabi hosted a competition in May 2024, focusing on applying quantum computing and artificial intelligence to address global challenges aligned with SDGs (NYU Abu Dhabi, 2024[66]). The competition yielded innovative proposals, such as using quantum sensing and machine learning for gas pipeline monitoring, optimising resource allocation in emergency settings, and resource optimisation for coral restoration.

Convergence with other digital technologies

The existing classical computing and communication networks

The conventional semiconductors powering classical computers are approaching physical limits in miniaturisation, raising significant engineering challenges (Box 5). As a result, the semiconductor industry has had to invest more heavily in the design and production of new microchips with higher processing

power. Economists from Stanford and MIT have estimated that the research funding dedicated to maintaining Moore's Law has increased by 18 times since 1971 (MIT Technology Review, 2020[67]). In this context, quantum technologies offer promising opportunities to further expand the frontiers of computing.

Box 5. The end of Moore's Law and the future of classical computers

Moore's Law refers to the observation made by Gordon Moore in 1965 that the number of transistors on a microchip doubles approximately every two years, leading to an exponential increase in computing power. This trend has been a driving force behind the many innovations in electronic devices and the progress of computing capabilities over the past several decades.

However, Moore's Law has begun to slow down primarily due to physical limitations in transistor scaling. As transistors become smaller, approaching atomic scales, it becomes increasingly difficult and costly to maintain the pace of doubling transistor density every two years. Challenges such as gate width limitations, issues with photolithography at extremely small scales and increased production costs are the main limiting factors.

Despite the slowdown of Moore's Law in terms of transistor scaling, innovation in classical computing systems continues through other avenues. For instance, progress in three-dimensional chip architectures, where transistors are stacked vertically to increase density and efficiency, represents one approach to extending computing power. Additionally, innovations in integrating different functionalities (like logic processing, memory and communication) on a single chip are helping drive performance improvements.

Source: (Kressel, 2023[68]).

However, as described in section 1, quantum computers excel only in specific types of problems that are challenging or intractable for classical computers. It is unclear whether quantum computers will outperform tasks that conventional computers can handle. Classical computers are expected to coexist with fault-tolerant quantum computers. Today's desktops and laptops will continue to support everyday functions like word processing, Internet browsing and email, where quantum computing does not offer advantages. Essentially, if an application is outside the scope of quantum algorithms (see Annex A), it will most likely continue to be handled by classical computers. Moreover, conventional computers will be needed to operate quantum hardware, playing a role in several functions like preprocessing data, applying algorithms, managing error correction and analysing results.

Hybrid computing approaches are being explored to combine the strengths of both classical and quantum computing to solve problems more effectively than either could alone. According to GFTech focus group experts, the first commercial applications of quantum computing will most probably involve classical supercomputers, where a given problem is decomposed into distinct parts that can be efficiently solved using quantum algorithms and others that are better suited to classical algorithms. Several computing infrastructures are following this approach, such as the Finnish Quantum-Computing Infrastructure. The European High Performance Computing Joint Undertaking (EuroHPC) is in the process of integrating quantum computers into existing supercomputers in the Czech Republic, France, Germany, Italy, Poland and Spain. In the latter, for example, a quantum annealer will be hosted and operated by the Barcelona Supercomputing Center and integrated into the EuroHPC supercomputer MareNostrum 5.

Large cloud service providers have started making quantum computing accessible to the general public, though with limited processing capabilities. Cloud services are particularly beneficial because they allow users from anywhere to tap into quantum processing power without needing to own the necessary hardware. One of the key advantages of quantum cloud computing is its flexibility in allocating computing

power, which can be adjusted based on user needs (Golec et al., 2024[69]). This adaptability makes cloud services appropriate for both small-scale experiments and large-scale projects. Moreover, service providers can also analyse how users interact with the device to identify the most skilled programmers while safeguarding their engineering secrets in secure facilities, making reverse engineering impossible (Hoofnagle and Garfinkel, 2022[3]).

As 6G research progresses worldwide, including in 15 OECD member countries, the future 6G standard, expected to start rolling out by 2030, will be influenced by four key factors: (i) overarching policy objectives, (ii) spectrum policy, (iii) technological standards, and (iv) business models tailored to specific use cases (OECD, 2024[70]). Concurrently, there is ongoing research on several applications and use cases, including how to integrate quantum technologies into 6G with "security by design features" (OECD, 2024[70]). . According to some researchers, quantum communication could improve the security of wireless networks and raise their data-handling capacity and performance (Ali et al., 2023[71]). 6G networks could also be used to transmit quantum information and provide access to quantum computing services on the cloud (Rozenman et al., 2023[72]).

Artificial intelligence

As classical machine learning continues to deliver new large language models and other innovations, it is an increasingly resource-intensive activity. The cost of training OpenAI's model behind the first version of ChatGPT, GPT-3, is estimated at USD 4.6 million, while the second version, GPT-4, is estimated to have cost more than USD 100 million (Fortune, 2024[73]). As this trend is likely to persist, it is unsurprising that more machine learning researchers are exploring the potential benefits of quantum computing (Zeguendry, Jarir and Quafafou, 2023[74]). Researchers are, for example, exploring how to reduce the processing power and energy required to train artificial intelligence (AI) models using quantum computing, e.g. to optimise the training dataset (Nivelkar and Bhirud, 2021[75]). Many of the commercial applications described in section 2 included potential uses of quantum-enabled AI.

Scientific publications and patents that jointly tackle artificial intelligence and quantum technologies are growing at a fast pace, suggesting a convergence in both fields (Coccia, 2024[76]). However, despite these promising directions, quantum-enabled AI faces several challenges in addition to decoherence errors (Biamonte et al., 2017[77]; Gujju, Matsuo and Raymond, 2024[78]), including:

- the limited bandwidth mentioned in section 1, which makes it inefficient or even unfeasible to convert training datasets (classical data) into quantum states and quantum outputs into bits for classical computers to read and interpret;
- uncertainties about the hardware requirements for quantum machine learning algorithms; and,
- uncertainties about the relative advantage quantum algorithms can yield over increasingly improving classical algorithms (see Annex A).

In light of these challenges, experts in the GFTech focus group do not consider quantum machine learning viable within a 10-year timeframe. By contrast, experts highlight that AI is already supporting the development of quantum technologies. Machine learning assists quantum sensors in refining their measurements to make them more resource-efficient and accurate (Krenn et al., 2023[79]), supporting several of the commercial applications mentioned in section 2. AI can also help design quantum sensing experiments by suggesting optimal settings and configurations (Belliardo, Zoratti and Giovannetti, 2024[80]). It also helps to make sense of complex data gathered by quantum sensors as well as computing outputs based on such data.

Using AI on the large amounts of data gathered by quantum sensors offers great potential for improving medical diagnostics and healthcare (Das et al., 2024[34]). For example, AI can help process quantum biosensors data, enable pattern recognition, identify biomarkers and reduce noise in sensor outputs. Classical machine learning and deep learning algorithms are crucial to extracting useful information from

biosensors for enhanced disease detection and monitoring. Coupled with quantum sensors, AI can also support real-time health monitoring and tracking of medication levels, assisting doctors in making personalised treatment decisions. The partnership between quantum sensing and AI can boost diagnostic accuracy and speed, paving the way for precision medicine.

Machine learning techniques can also optimise the performance of quantum devices (Krenn et al., 2023[79]). As mentioned in section 1, measurements can be noisy and unclear on such devices. Machine learning algorithms help to identify and correct decoherence errors and can improve the accuracy of qubit measurements, helping to determine their states more reliably. This is crucial for developing more robust quantum computing systems. AI can also predict the behaviour of quantum systems based on data from past experiments, improving our understanding of these systems and supporting the development of quantum simulations and other computing applications.

3 Digital security and privacy risks to be mitigated

Infographic 3. What digital security and privacy risks do quantum technologies pose?

Digital security

Risks

- In the future, quantum computers may break existing cryptographic methods, jeopardising the security of nearly all data transmitted today over the internet.
- Data could be intercepted today and stored for its decryption in the future by a quantum computer.
- Transition to quantum-resilient solutions requires significant time and resource investment.

Mitigation pathways

- Development and adoption of post-quantum cryptography, which uses new methods that are resistant to known quantum attacks.
- Exploring the complementary use of quantum key distribution to strengthen security.
- Raising awareness in public and private organisations of quantum risks and the need to transition to quantum-resilient solutions.

Privacy

Risks

- Quantum sensors are expected to enable advanced surveillance and privacy intrusion, such as seeing through barriers and intercepting near-field communication signals (e.g. in smartphones and credit cards).
- Some applications challenge the notion of informed consent in data collection (e.g. in healthcare).

Mitigation pathways

- Gap analysis of existing laws and regulatory frameworks governing data privacy.

Cloud-based quantum computing

Risks

- Cloud services enable global access to quantum computers, but their capabilities also pose risks of unethical use, such as data decryption or weapons development.

Mitigation pathways

- Cloud service providers are a natural place to monitor signs of misuse. However, detecting such misuse poses significant technical challenges that need to be resolved.

The quantum threat to cryptography

Cryptography involves various practices, means, methods and techniques used to transform data and ensure their confidentiality, integrity, authentication and non-repudiation, or a mix of these aspects (OECD, 2024[23]). Cryptography is crucial for today's digital economies because it enables the security and privacy of digital systems at all levels, from personal smartphones to government networks and global business communications. It is integral to protecting hardware, software, networks and data. Cryptography enables secure web browsing, authenticates individuals and documents, protects the privacy of instant messaging, secures wireless communications, and ensures safe data storage both locally and in the cloud. It also supports the functionality of virtual private networks, the security of chips in credit and ID cards and is fundamental to blockchain distributed ledger technologies.

Most of today's digital communications use cryptography that relies on maths problems such as integer factorisation,[12] i.e. the process of taking a large number that is created by multiplying two smaller prime numbers and figuring out what those original prime numbers were. Security relies on the fact that, while it is easy to multiply these two primes to obtain a large product, it is extremely difficult to reverse the process. For example, breaking RSA-2048, a commonly used cryptographic algorithm based on integer factorisation, would take today's fastest supercomputers 300 trillion years (Shamshad et al., 2022[81]), far longer than the age of the universe. A sufficiently powerful quantum computer could, in theory, solve integer factorisation in just a matter of hours. This is known as a "cryptographically relevant quantum computer." This capability would compromise the security of nearly all transmitted data that is encrypted today, including public or private sector data with strategic, financial or intellectual property value.

As previously noted, quantum computing faces fundamental challenges, requiring breakthroughs in engineering as well as basic science, making the development of a cryptographically relevant quantum computer very unlikely in the near future. Breaking RSA-2048 in about 8 hours using current quantum computing technology would require 20 million physical qubits (Gidney and Ekerå, 2021[82]), which is roughly 18 000 times more than the qubit capacity of the largest quantum computer available today. One forecast, based on a statistical model projecting past progress in quantum computing technology, suggests there is less than a 5% chance that RSA-2048 encryption will be broken before 2039 (Sevilla and Riedel, 2020[83]). In a survey of 37 leading experts from science and industry in quantum computing, the majority estimated a 5% or lower likelihood of a cryptographically relevant quantum computer arriving within the next 10 years, but a 50% or greater likelihood of its arrival within the next 15 years (Mosca and Piani, 2023[84]).

Despite this timeline, cybersecurity agencies recommend starting to implement quantum-resilient solutions already now (OECD, 2024[23]), for several key reasons, such as (Trzcisnki et al., 2023[85]):

- **The widespread use** of cryptographic methods that are both fundamental to securing most digital communications and vulnerable to quantum computing attacks.
- **The present threat of "store now, decrypt later" attacks**, where data transmitted at present could be intercepted and stored for its decryption in the future with the arrival of cryptographically relevant quantum computers.
- **The lengthy process of transitioning to new cryptographic systems**, which can take up to 20 years for wide adoption, given the vast number of actors and devices involved (NSA, 2021[86]).

Towards quantum-resilient solutions

Cryptography standard-setting organisations have long recognised the potential threat posed by quantum computing, particularly the algorithm developed in 1994 by the American mathematician Peter Shor. In response, they are developing and introducing new cryptographic methods designed to be resistant to quantum computers, known as post-quantum cryptography (PQC), also referred to as quantum-resistant

cryptography (Box 6). PQC employs classical computing algorithms for encryption, much like integer factorisation. However, it derives additional security from different classes of maths problems that remain difficult to solve even for quantum algorithms (Trzcisnki et al., 2023[85]). PQC is designed to be implemented on existing computing and networking infrastructures. This makes it practical for widespread adoption, enabling a smooth transition while maintaining robust security across information systems. At the same time, state-of-the-art PQC has specific requirements, e.g. on key length, which requires more computational resources and a higher power budget per exchanged key than today's cryptographic methods. Many older devices (e.g. Internet of Things) do not meet these additional requirements.

Box 6. Global efforts for the transition to post-quantum cryptography

Since 2006, an international community of researchers has been working to improve existing cryptographic solutions, with significant progress made through publicly funded research projects in the European Union and Japan. In 2016, the United States National Institute of Standards and Technology initiated an 8-year global competition to evaluate and select the most promising quantum-resistant algorithms, leading to the first three finalised post-quantum cryptography (PQC) standards being released in August 2024.

Recognising the long timeline required for transitioning to new cryptographic systems, cybersecurity agencies have issued guidance to organisations on how to prepare for this change. The UK National Cyber Security Centre has encouraged organisations to start taking steps to prepare and migrate to PQC. They recommend supporting current public key cryptography during the transition period to ensure continued security. Similarly, Germany's Federal Office for Information Security and France's National Cybersecurity Agency (ANSSI) have advocated for a hybrid approach, i.e. combining traditional cryptographic algorithms with PQC to provide an added layer of security without completely abandoning pre-quantum methods. The US Department of Homeland Security and its Cybersecurity and Infrastructure Security Agency have developed roadmaps to help organisations prepare for the transition to PQC. Key steps include assessing risks, fostering the adoption of PQC policies and standards, and engaging IT departments, vendors and staff to develop migration strategies.

Source: (OECD, 2024[23]; NIST, 2024[87]; NCSC, 2024[88]).

The quantum communication technologies described in section 1 also promise resistance to quantum computing attacks. Quantum key distribution (QKD) aims to ensure (i) that any attempt by an outside party to intercept the key exchange is detectable, and (ii) that the intercepted information is rendered invalid for use. PQC methods were explicitly developed to protect against attacks enabled by Shor's algorithm, as well as all other known threats posed by classical and quantum algorithms. However, unlike QKD, the security of PQC is not proven by the laws of physics and instead relies on the difficulty of certain maths problems. Thus, PQC may be compromised in the future if breakthroughs in algorithms, classical or quantum computing-based, occur.

GFTech focus group experts consider QKD to be a promising technology that could add a layer of security to PQC in specific contexts (e.g. to secure information exchanges between data centres) and see both approaches to quantum resilience as complementary rather than mutually exclusive. However, the additional logistical and deployment challenges of QKD impose limitations on its scalability to secure the much broader digital economies. As mentioned earlier, QKD has been limited to short distances of about 100 km, and space-to-ground applications have shown mixed results. QKD requires specialised hardware that is more costly and complex to install and maintain relative to PQC. This can make integrating QKD with existing network infrastructures challenging, which is an obstacle to widespread use across large geographic areas. Since PQC can be integrated into many current systems and networks, its

implementation can scale much more easily than QKD. Moreover, practical implementations of QKD can still be vulnerable to certain attacks (BSI, 2023[89]).[13] In light of these challenges, although national cybersecurity agencies are encouraging further research in quantum communication, none currently recommends its use for protecting sensitive data (ANSSI et al., 2024[28]; OECD, 2024[23]). The study and resolution of QKD vulnerabilities and practical challenges is an active area of research and development. Experts expect that such efforts will strengthen the robustness of QKD solutions while simultaneously reducing implementation and operational costs.

Given that the transition to new cryptographic methods is known to be a lengthy process, experts in the GFTech focus group emphasise the need to start planning and creating roadmaps for quantum resilience immediately, with the first step being raising awareness. Policymakers need to develop their understanding of quantum technologies and their security implications, while IT professionals need a deeper understanding of these issues to support the transition. Experts recommend public and private organisations to identify and categorise the different types of data they hold and inventory their current cryptographic methods to develop protection strategies for each data type. They also suggest evaluating quantum-resilient solutions through trials and pilot programmes, allocating resources towards understanding and transitioning towards them. As an example, Box 7 provides the roadmap suggested by the United States Department of Homeland Security, developed in partnership with the Department of Commerce's National Institute of Standards and Technology (NIST).

Box 7. Steps organisations can take to plan the transition to post-quantum cryptography

1. **Engage standard-setting organisations**: Work with standard-setting organisations to identify which current standards are affected by quantum computing threats. This helps stay updated on necessary changes to algorithms and protocols.
2. **Inventory of critical data**: Identify which data might be at risk of being decrypted by future quantum computers.
3. **Inventory of cryptographic technologies**: Make a list of all systems using cryptography. Knowing what needs updating helps ensure a smooth transition.
4. **Identification of internal standards**: Review and update current standards related to data security and cybersecurity to meet post-quantum requirements.
5. **Identification of public key cryptography**: Determine where and why public key cryptography is used in your systems. Mark these as vulnerable to quantum threats.
6. **Prioritisation of systems for replacement**: Evaluate which systems should be updated first by considering their value, what they protect, their interactions with other systems and their importance to critical infrastructure.
7. **Plan for transition**: Using the inventory and prioritisation, develop a detailed plan for updating systems to new cryptographic standards. Ensure this plan is flexible to accommodate future changes and provide guidance for smooth implementation.

Source: (Homeland Security, 2022[90]).

Following the release of three new PQC standards in August 2024 (NIST, 2024[87]), the U.S. government will soon require agencies to develop transition plans, including the integration of these standards in all relevant procurement processes (White House, 2022[91]). The G7 Cyber Expert Group, chaired by the U.S. Department of the Treasury and the Bank of England, released a public statement in September 2024 advising finance authorities and institutions to take similar steps as soon as possible and prepare themselves to handle impending threats (G7 CEG, 2024[92]). In alignment with the European Commission's

Recommendation on a Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography (European Commission, 2024[93]), cybersecurity authorities from 18 EU member states issued a joint statement in November 2024, urging public administrations, critical infrastructure providers, IT providers, and industry actors to "make the transition to post-quantum cryptography a top priority" and to "start the transition now" (A-SIT et al., 2024[94]).

Risks to privacy

Digital economies rely on extensive and innovative uses of personal data, which bring greater economic and social benefits but also raise privacy risks. The continuous flow of personal data across global networks increases vulnerability to unauthorised access and misuse. The OECD Privacy Guidelines aim to mitigate these risks by promoting and protecting fundamental values of privacy and individual liberties while ensuring the global free flow of information (OECD, 2013[95]). However, emerging digital technologies challenge existing privacy safeguards (OECD, 2023[96]). The prospect of a cryptographically relevant quantum computer that can decrypt today's digital communications raises significant privacy concerns, as malicious actors could access individuals' personal data without consent. As described below, quantum technologies introduce other privacy risks.

Quantum sensors are anticipated to enable unprecedented surveillance and intrusion into private spheres, as they can see through clothes, buildings, rocks and other materials much better than current technologies (Hoofnagle and Garfinkel, 2022[3]; Krishnamurthy, 2022[97]; ICO, 2024[98]). Experiments have demonstrated the capability known as "quantum illumination", in which sensors can detect objects not directly in their line of sight. This technique could also enable observation with cameras in extremely low-light conditions. Quantum magnetic sensors could allow malicious actors to intercept near-field communication (NFC) signals from a distance, e.g. to capture payment information from bank cards or smartphones.

While quantum-based surveillance capabilities are expected to be first developed and used by military and national security agencies, they will likely become accessible to local law enforcement agencies, the private sector and malicious actors (Hoofnagle and Garfinkel, 2022[3]). Moreover, commercial applications that analyse personal data gathered using quantum sensors, for example in medicine and healthcare, raise issues around autonomy and consent. The data they collect may be difficult for patients to fully understand. This complexity challenges the traditional notion of informed consent, as patients may not fully grasp what data is being collected, how it will be used, and the implications of its use. Patients may lose autonomy over their personal data if the data collected by quantum sensors is used in ways they did not explicitly agree to or are unaware of. Quantum sensors may enable the collection of highly detailed and sensitive data, which could reveal intimate insights about a person's health or behaviour. In finance, the use of quantum algorithms in credit scoring similarly raises concerns around data privacy, fairness and the explainability of the models (Bruno, 2023[48]). Quantum technologies may therefore require that existing laws governing their use be re-assessed and, if needed, adjusted to protect privacy and ensure public trust, necessary for enabling commercial uptake (RHC, 2024[47]).

It is well documented in the policy literature that artificial intelligence can interfere with human rights by compromising privacy, perpetuating discrimination, and threatening freedom of expression through technologies like facial recognition and generative AI (OECD, 2024[99]). While quantum machine applications could exacerbate such risks in principle, as previously explained such applications face significant technical challenges in their implementation.

Quantum communication can also act as a privacy-enhancing technology:[14]

- **Quantum networks enable blind quantum computations**, where a user performs computations on one or more remote servers without revealing their data or the nature of their calculations (Fitzsimons, 2017[100]; Singh et al., 2021[51]). This approach ensures that the structure of the

computation remains hidden from the server performing the tasks. Although the server can see the resources used, such as the depth and width of the quantum circuits, it cannot discern the actual computation details. Blind quantum computations aim to securely outsource quantum computation to one or more untrusted devices while preserving the privacy and integrity of the computation.

- **Quantum random number generators**[15] help protect privacy by creating truly random numbers, which are crucial for secure data encryption (Mannalatha, Mishra and Pathak, 2023[101]). This protects data in various ways, such as making encryption keys harder to crack and generating safer pin codes for online transactions and one-time passwords for accessing online accounts.

Other considerations for risk mitigation

Experts in the GFTech focus group highlight that while cloud services make quantum computers more accessible to research and industry actors, such capabilities could also be used by individuals and entities with malicious intent. Currently, only a few companies are able to develop or host their own quantum computers. In theory, this makes cloud service providers a natural place to monitor signs of misuse. However, detecting such misuse may be technically challenging (NQCO, 2022[102]):

- Homomorphic encryption,[16] which allows users to hide the contents of their computations from remote servers, might make it impossible to monitor ethical use on cloud quantum computers. Although quantum computers will be limited in resources for some time, making this encryption method difficult to use, simpler methods to evade detection could still be developed.
- A given quantum computing technique can be used ethically or unethically. For instance, a technique known as phase estimation is essential for both Shor's cryptanalysis algorithm and for quantum chemistry algorithms.
- Restricting a general-purpose quantum device to certain applications is challenging. A device restricted to solving chemistry problems, for example, could still perform other quantum algorithms by encoding them as chemistry problems. However, the complexity of such encodings makes them impractical in the near future.

While quantum communication promises enhanced privacy because they are difficult to intercept without detection, it could also interfere with government agencies' ability to conduct lawful investigations (Krishnamurthy, 2022[97]; Bambauer, 2024[103]). As with other privacy-enhancing technologies, quantum networks and blind quantum computations could impact public safety because the increased privacy and security might make some forms of legal surveillance and investigation more difficult. Such capabilities could enable new quantum-assisted crimes, such as decrypting data and creating new biological weapons. It is therefore necessary to balance individual privacy rights with public safety needs. Experts in the GFTech focus group also underscore the unique security challenges faced by quantum computing data centres. The sensitivity of data entering and leaving such centres makes security paramount.

Quantum technologies could also mitigate digital security risks. Cyber-attacks on clock synchronisation systems in networks can disrupt the precise timing needed in telecommunications and financial services (Alghamdi and Schukat, 2021[104]). Attacks such as GPS signal[17] jamming and spoofing, and the malicious manipulation of time-keeping devices, can lead to inaccurate timestamps and synchronisation errors, which may result in disruptions to system operations, data corruption or financial losses. Having several distributed high-precision atomic clocks could make it easier to detect and mitigate such attacks (Balakrishnan et al., 2023[105]).

Quantum AI could not only perform certain tasks faster and more accurately but also be more robust against adversarial attacks (West et al., 2023[106]). In the context of machine learning, adversarial attacks refer to efforts to fool AI systems through manipulated inputs that appear normal to human observers but lead to incorrect conclusions by the AI. For example, minor, calculated tweaks to an image can trick an AI

into misidentifying its contents. These attacks exploit vulnerabilities in AI systems, particularly neural networks, which, while generally robust against random errors, can be surprisingly fragile against these specific, deliberate perturbations. Such vulnerabilities pose significant risks, especially in security-sensitive applications like facial recognition, autonomous driving and surveillance. The natural randomness introduced by quantum noise could disrupt adversarial attacks, making it harder for them to succeed. Initial studies, however, suggest that quantum machine learning could also be vulnerable to its own unique types of adversarial attacks (West et al., 2023[106]). Despite these concerns, the unique properties of quantum systems might also unlock new methods to protect against such attacks.

4 Policy opportunities

Infographic 4. What policy opportunities can help advance quantum technologies?

Government support for quantum technology ecosystems

Despite the many potential applications of quantum technologies, the largely nascent field poses substantial financial risks for private investors. While the prospect of high returns from these pioneering technologies is attracting private funding, it could be challenging to sustain investments due to the extended timeframes required to achieve profitability (Gibney, 2019[107]). Experts in the GFTech focus group agree that quantum technologies will ultimately yield valuable and potentially groundbreaking products and services. However, the time required before they reach maturity could cause investors to lose interest, potentially leading to a "quantum winter."

Given the potential benefits and risks described in previous sections, governments are allocating substantial resources to fund the development of quantum technologies. They have taken a central role in nurturing quantum technology ecosystems through the implementation of national strategies, dedicated funding programmes and the formation of international partnerships. As of April 2024, global public investment in quantum technologies is estimated by private sources to have reached USD 42 billion (McKinsey, 2024[108]).

Stakeholders shaping quantum technology ecosystems include government ministries and agencies, manufacturers, universities, software developers, public and private research labs, startups, investors, accelerators and businesses (end users). Adjacent organisations, such as management consulting companies advising on quantum, also play a role in technology commercialisation and in developing the overall ecosystem. The following sections describe how governments are supporting research and development in quantum technologies as well as assisting firms in building quantum readiness and resilience in anticipation of their arrival.

Support for research and development

Experts in the GFTech focus group agree that governments play a crucial role in supporting fundamental and early-stage research for quantum technologies. As described above, most commercial applications of quantum technologies are uncertain and too distant for the private sector to drive investment. Governments are implementing large-scale funding programmes to lay the groundwork for future breakthroughs while ensuring they have oversight on developments that involve risks to digital security or have defence implications. Selected examples of research funding programmes include:

- **Critical Technologies Challenge Program, Australia (Department of Industry, Science and Resources), 2023 – ongoing**: This initiative aims to boost awareness and adoption of quantum technologies by fostering stronger connections between researchers, companies, industry and society. The programme is designed in collaboration with industry and research institutions to ensure projects address real-world needs, are challenging yet achievable and meet market demands.
- **European Quantum Flagship, European Union, 2018 – 2028**: This programme gathers research institutions, academia, industry, enterprises and policymakers in a large-scale collaborative effort. The primary goal is to strengthen and expand European scientific leadership in quantum research and to transition quantum physics from the lab to the market through commercial applications and disruptive technologies. The initiative aims to develop next-generation technologies that will significantly impact European society and establish the region as a global leader in QIST. In addition to participating in the European Quantum Flagship, many EU Member States have launched or are developing their own national strategies and programmes to strengthen their domestic capabilities in quantum technologies.
- **Quantum Leap Flagship Programme, Japan (Ministry of Education, Culture, Sports, Science and Technology, MEXT), 2018 – 2027**: This initiative aims to significantly contribute to economic

and societal goals through quantum technologies. The programme focuses on three key technology areas: Quantum simulation and computing, quantum metrology and sensing, and next-generation lasers. Additionally, it includes a Human Resources Development Program to cultivate the next generation of quantum technology leaders and promote common education programmes.

- **National Quantum Technologies Programme, United Kingdom (Department for Science, Innovation and Technology), 2014 – ongoing**: This programme is a collaboration between industry, academia and government aimed at transforming cutting-edge quantum science into new products and services. The programme supports innovation and investment to secure the country's competitive advantage in the global quantum era, focusing on scientific research, skills development and international collaboration. It features five Quantum Technology Hubs based at universities, with distinct focus areas, including computing and simulation, communication, and sensing (biomedical, metrology, and position, navigation and timing). The programme also includes missions that seek to achieve long-term, ambitious technological outcomes that benefit the economy and society.
- **National Quantum Initiative, United States (National Science and Technology Council), 2018 – ongoing**: This initiative is a comprehensive government effort to maintain and enhance U.S. leadership in quantum technologies and their applications. Established by the National Quantum Initiative Act of 2018 and further supported by the National Defense Authorisation Acts and the CHIPS and Science Act of 2022, the initiative focuses on advancing quantum computing, networking and sensing technologies. The initiative is coordinated by multiple federal agencies, including the National Institute of Standards and Technology, the National Science Foundation and the Department of Energy, and involves the creation of funding programmes, centres and consortia. The initiative promotes collaboration across the government, academia and industry, aiming to accelerate quantum research, development and commercialisation, ensuring economic prosperity and national security.

Many of these programmes take a high-risk/high-reward approach to funding research (Box 8). This approach targets ambitious scientific projects that aim to significantly impact society, technology or knowledge (OECD, 2021[109]). The "high-risk" aspect refers to the exploration of novel ideas or methods that may not align with established scientific knowledge or are at such an early stage of development that predicting their success is difficult. However, they are considered "high-reward" because, if successful, they could lead to significant progress, such as breakthrough technologies or solutions to major societal challenges. This type of research often transcends traditional disciplinary boundaries and challenges existing scientific paradigms, making it a potential catalyst for radical transformation in understanding or practice. Nevertheless, due to its unconventional nature, such research might struggle to secure support through standard review processes, which typically favour more predictable and incremental research approaches.

Box 8. What is high-risk/high-reward research?

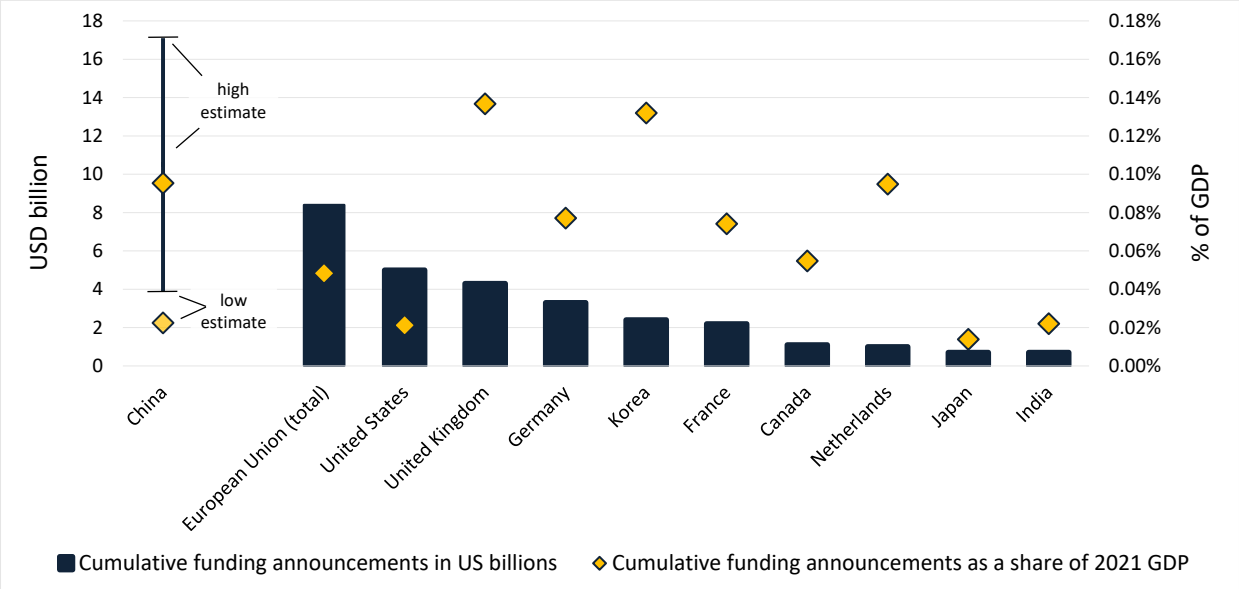
High-risk, high-reward research is research that (i) strives to understand or support solutions to ambitious scientific, technological or societal challenges; (ii) strives to cross scientific, technological or societal paradigms in a revolutionary way; (iii) involves a high degree of novelty; and (iv) carries a high risk of not realising its full ambition as well as the potential for high, transformational impact on a scientific, technological or societal challenge.

Source: (OECD, 2021[109]).

Figure 1 illustrates government quantum technology funding announcements as of 2024, highlighting significant pledges across various countries and regions. It is important to note that the figure lumps past, current and future funding announcements. Countries do not announce funding in the same way, and future commitments are not guaranteed to translate into actual expenditures, as changes in political priorities and leadership can influence them. Consequently, these discrepancies complicate comparisons of funding announcements. Nonetheless, the Figure underscores countries' substantial interest in advancing quantum technologies.

Figure 1. Quantum funding announcements in selected countries as of 2024

In USD billion and as a share of 2021 GDP



Notes: The figure lumps past, current and future funding announcements. Countries do not announce funding in the same way and future commitments are not guaranteed to lead to expenditures. These discrepancies complicate comparisons of funding announcements. The total for the European Union lumps national and EU-wide announcements.
Source: (Qureca, 2024[110]); Estimates for China are provided by (Quantum Insider, 2023[111]); GDP data provided by (OECD, 2024[112]).

The European Union leads in funding announcements with around USD 8.4 billion, combining national and EU-wide commitments. This amount is primarily driven by contributions from Germany (USD 3.3 billion), France (USD 2.2 billion) and the Netherlands (USD 1 billion). China's pledges range between USD 4-17 billion, reflecting different estimates. The United States has announced USD 5 billion, while the United Kingdom has committed USD 4.3 billion. Other notable announced investments include Korea (USD 2.4 billion), Canada (USD 1.1 billion), Japan (USD 0.7 billion) and India (USD 0.7 billion). When considering quantum investment announcements as a percentage of GDP, the United Kingdom and Korea are at the forefront, suggesting a strong relative commitment to developing QIST.

Although official information on spending for China is limited, one report suggests the country committed about USD 1 billion by 2017 to the National Laboratory of Quantum Information Science in Hefei, west of Shanghai (Kania and Costello, 2018[113]). The same report points to a pledge of nearly USD 15 billion to further develop the laboratory over a 5-year timeframe. While China's total public investment is disputed, the country has demonstrated technological prowess. Chinese researchers have achieved significant publications, often in prestigious peer-reviewed journals including *Science* and *Nature*, in quantum communication (fibre-based quantum networks and satellite-based QKD), computing[18] and sensors (quantum sonar) (Hoofnagle and Garfinkel, 2022[3]). Bibliographic and patent data suggest that China holds

a leading position in quantum communication, is competitive in quantum sensing and lags behind in quantum computing (Omaar and Makaryan, 2024[114]).

While government support is vital to help quantum technologies reach maturity, private investment is also already playing a significant role in quantum ecosystems. Private investment in quantum technology start-ups more than doubled between 2020 and 2022, reaching USD 2.35 billion before decreasing to USD 1.71 billion in 2023 (McKinsey, 2024[108]). Like public funding, private quantum technology investment is also geographically concentrated. Canada, the European Union, the United Kingdom and the United States are estimated to account for about 90% of global private investment in quantum start-ups (McKinsey, 2024[108]). In addition, several multinational companies are internally carrying out extensive research and development programmes.

Experts in the GFTech focus group highlight that it can be challenging to align research funding goals between public research organisations and the private sector, especially in the field of quantum computing. Companies often prioritise short-term objectives, such as demonstrating quantum advantage, while public research tends to focus on long-term goals, like developing new quantum algorithms. However, combining public and private funds has been a successful strategy in many cases, enabling shared risk while aligning long-term public benefits with short-term private gains. For example, several countries are building research infrastructures to support quantum science while also addressing the present-day research and development needs of the private sector. The United Kingdom, via its Industrial Strategy Challenge Fund, launched the Quantum Technologies Challenge, which has committed GBP 174 million to 139 projects involving 141 organisations across the country between 2018-2025 (UKRI, 2023[115]). This initiative has helped de-risk industry investment in quantum research and development, enabling participating companies to raise close to GBP 400 million in private capital.

The OECD is mapping the landscape of national strategies and policies in support of quantum technologies. This work will identify and characterise government efforts, including the main objectives, sectors targeted, timelines, societal challenges addressed, modes of implementation and subsequent monitoring, among other characteristics. National strategies will be contextualised by examining associated governance policies, such as stakeholder consultation, technology assessments and foresight exercises, to gain insights into the broader engagement processes and policy intelligence tools that have shaped them. This work will also analyse the key instruments countries have introduced to support quantum ecosystems, e.g. business grants, equity financing, infrastructure funding, procurement programmes, technology extension and business advisory services, collaborative platforms (hubs for ecosystem actors) and skills development programmes.

Building quantum readiness and resilience

As described earlier, quantum technologies operate fundamentally differently from other digital technologies and can offer substantial benefits. The private sector will require significant time and investment to prepare for the adoption of quantum technologies (Purohit et al., 2024[29]). Several companies across various industries have already started efforts to harness quantum technologies, with the goals of improving their operations, products and services, and ultimately gain a competitive edge. Experts in the GFTech focus group indicate that public and private organisations aiming to develop capabilities in quantum technologies will need to:

- **Develop their understanding of these technologies** and their relevance for their business models and operations. This will involve hiring new talent and upskilling existing staff, including technicians and managers, to build their knowledge around use cases and potential applications.
- **Estimate near and long-term economic impacts**. In quantum computing, for example, quantum algorithms are unlikely to yield benefits in the short or medium term, but they could have strong strategic relevance for businesses in the long term. Companies have several tools at their disposal

to assess quantum computing applications. They can use classical computers to run small-scale experiments with quantum algorithms and assess their potential relevance. Companies can also run trials with technology providers and request independent validation of use cases. Other tools include cost-benefit analysis, benchmarking and scalability analysis of solutions.

- **Build capabilities in quantum technologies by developing partnerships** with various actors in the technology ecosystem, such as universities, public research institutes, government agencies, quantum hardware and software development companies, startups and other companies involved in supply chains.

In addition to developing capabilities in quantum technologies, GFTech focus group experts emphasise that public and private organisations need to start mitigating security risks emerging from quantum technology. Specifically, organisations should work closely with PQC standard-setting organisations to identify high-risk data assets, inventory current cryptographic methods and develop roadmaps for ensuring quantum resilience.

Future OECD work will investigate how technology providers and government agencies are assisting companies in digital economies to prepare for the advent of quantum technologies. This work will analyse the modus operandi of these organisations across multiple countries via desk research, structured interviews and written contributions from their representatives. The goal is to identify best practices that policymakers can use to develop roadmaps for quantum readiness and resilience. The work will outline and describe the steps companies are undertaking to adapt. Such guidance will be particularly valuable for emerging economies that have yet to formulate flagship national quantum strategies or programmes, helping them take the initial steps towards integrating quantum technologies into their digital economies.

Metrics to benchmark quantum technological capabilities

In the QIST field, benchmarks are emerging as standardised measurements and tests used to evaluate and compare the capabilities and performance of quantum technologies. These benchmarks help both providers and users understand how these technologies are evolving and which types of sensors, computers or networks are best suited for specific needs or tasks. Key performance metrics help identify strengths and weaknesses within and across different quantum systems, guiding improvements (Lubinski et al., 2024[116]). Emerging performance benchmarks focus on three main areas (Finzgar et al., 2022[117]):

- **System-level benchmarks** focus on evaluating the fundamental hardware and system components of quantum devices. These benchmarks examine aspects such as the accuracy, sensitivity and resolution in sensors, coherence times and error rates in computing, and the speed of exchanging keys in a QKD system. These measures are evaluated individually and then composed into system-level performance indicators that assess the overall system's efficiency. The Quantum Volume benchmark, for example, measures the largest quantum circuit that can be reliably executed, providing more valuable insights into a quantum computer's capabilities.
- **Algorithmic-level benchmarks**, specific to computing, evaluate how well individual components of a quantum algorithm perform. For instance, the Circuit Layer Operations Per Second (CLOPS) metric evaluates the speed of executing quantum circuits, which is crucial for applications in machine learning and optimisation. These benchmarks are essential for understanding the efficiency and effectiveness of quantum subroutines, allowing developers to refine algorithms and improve overall system performance. They also help in comparing different types of quantum computer systems by measuring the performance of critical tasks.
- **Application-level benchmarks** assess the performance of an entire quantum system in achieving specific tasks. They assess the combined performance of hardware, operating systems, middleware, classical resources and their interactions. Unlike benchmarks focusing on specific

components or algorithms, application-level benchmarks provide a holistic view of performance when executing a real-world task. These benchmarks are crucial for understanding the feasibility of commercial applications, identifying performance bottlenecks, and guiding research and development efforts. They also help evaluate what quantum systems can effectively accomplish relative to classical systems in terms of speed, precision and energy consumption, among other factors.

Experts in the GFTech focus group underscore the absence of standardised benchmarks in quantum technologies. In classical computing, for example, matrix inversion is used as a universal benchmark, but the quantum computing field currently lacks a similar common standard. Establishing performance measures would help track technology progress and maturity. System-level benchmarks would provide upstream insights into value chains and clarify the interactions between foundries, component manufacturers, and system integrators. Application-level benchmarks will become more significant downstream, as the ultimate test of a quantum system lies in its practical ability to provide customer value in commercial applications.

Robust benchmarking is also critical for attracting sustainable investment. The ability to measure and compare technologies helps distinguish genuine progress from hype, which helps guide public and private investment decisions. However, experts caution against focusing benchmarks solely on comparing quantum systems to classical systems. This narrow view is misleading, as quantum technologies are likely to complement rather than replace classical technologies in most applications. Additionally, experts stress the importance of careful benchmarking between different types of quantum technologies. Inaccurate comparisons could lead to uneven or misplaced investments and discourage the exploration of emerging technologies. For example, comparing different types of quantum computers can be challenging, as they are often optimised for different types of computations or algorithms. While benchmarks can allow for systematic assessment of emerging quantum devices, experts believe comparisons should be flexible and adaptable to new discoveries and breakthroughs, such as innovations in logical and physical qubits, which can challenge previously held assumptions and require new metrics to be introduced and previous ones to be adapted or discarded.

Co-operation in research and development

Science-industry co-operation helps turn promising research into commercial applications, supporting industrial competitiveness and tackling societal issues by turning scientific insights into innovative products and services (Kreiling and Paunov, 2021[118]). To advance quantum technologies, it is imperative that scientists and industry professionals work together (US GAO, 2021[119]). Achieving breakthroughs in quantum computing will require collaboration across scientific fields like physics, materials science and engineering. Moreover, science-industry co-operation will be needed to understand how the potential applications described in section 2 perform in practical, real-world scenarios. Indeed, several scientific articles cited in this paper are co-authored by science and industry experts.

Public-private partnerships help expose theoretical or experimental QIST applications to real-world use cases (QED-C, 2022[120]). Participants in these partnerships can develop a shared understanding of how scientific and technical knowledge will be used to achieve clearly defined goals, often framed around national priorities or societal challenges. Governments provide administrative and financial support for participating researchers and industry actors, ensuring alignment with such goals. Research and technology organisations (RTOs) can help bridge the gap between academic research and industrial capabilities, translating scientific discoveries into practical, market-ready technologies (Stierle et al., 2020[121]). RTOs can help foster public-private partnerships and promote quantum technology transfer and interoperability.[19]

Companies also drive collaborations with public research actors seeking to identify and scope use cases, as exemplified by the various competitions mentioned in section 2 contributing to advancing the SDGs. Other examples include Google's XPRIZE Quantum Applications, a 3-year, USD 5 million global competition designed to generate practical quantum computing algorithms that can help solve real-world challenges. The United Kingdom's National Quantum Computing Centre organises an annual hackathon that brings together teams of students, early career researchers and industry mentors to tackle practical challenges and develop solutions using quantum computing. Many startups working on quantum technologies are academic spin-offs, i.e. founded by researchers to commercialise their research activity and scientific knowledge, where their university or research institute often engages as partners. Businesses also seek partnerships with universities to identify and recruit talents with specialised QIST skills.

Despite these examples of successful science-industry co-operation, experts in the GFTech focus group view quantum technology ecosystems as generally fragmented, with limited co-operation between quantum researchers and engineers and their counterparts in established industry sectors. Co-operation is often restricted not only across different quantum technologies (sensing, computing and communication) but also within individual technologies themselves. As discussed in section 1, various types of quantum devices operate in fundamentally different ways. Experts acknowledge that some degree of fragmentation in research and development is inevitable, reflecting the early stages of development of most of these technologies.

The role of standardisation

GFTech focus group experts believe that some types of standardisation and best practices could reduce fragmentation in research and development. Yet, some experts warned of the negative effects of setting standards in rapidly developing areas as it could stifle innovation. In particular, establishing basic standards related to terminology and measurement can support quantum technologies that are still at the early stages of development (van Deventer et al., 2022[122]). These standards can help provide ecosystem actors (whether from research, industry or government) a clear and shared understanding of the technology, which is crucial for further progress and innovation. Establishing standardised processes and benchmarks for assessing the performance of quantum technologies is necessary to ensure that developments adhere to existing industry standards (RHC, 2024[47]). Standardisation efforts need to be co-developed with industry actors to ensure that standards support, rather than obstruct, quantum technology ecosystems. A challenge to a collaborative approach in developing QIST standards is the limited involvement of small and medium-sized enterprises (SMEs) in standard-setting exercises, especially on an international scale (RHC, 2024[47]).[20] Engaging stakeholders in emerging economies is also challenging (BIPM, 2024[123]).

National metrology institutes (NMIs) can provide independent and objective testing and evaluation of quantum materials, components, devices and systems, and contribute to the development of reliable and standardised benchmarks (Tzalenchuk et al., 2022[124]). At a workshop at BIPM, the intergovernmental organisation through which governments act together on matters related to measurement science and measurement standards, a new collaborative initiative called "NMI-Q" was recently introduced. This initiative aims to use the collective expertise of NMIs to jointly develop and share measurement best practices in support of future standardisation in quantum technologies (BIPM, 2024[123]).

Other international organisations working with multiple stakeholders to develop standards in this field include:

- The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), which established a new Joint Technical Committee on Quantum Technologies (JTC-3) and recently developed a joint vocabulary for quantum computing;

- The International Telecommunication Union (ITU), which hosted a focus group on quantum information technology for networks between 2019-2021;
- The Internet Engineering Task Force (IETF) and the European Telecommunications Standards Institute (ETSI), which have separately created post-quantum cryptography working groups;
- The Institute of Electrical and Electronics Engineers (IEEE), which has created various standards working groups spanning quantum sensing, computing and communication; and,
- The European Committee for Standardization and the European Electrotechnical Committee for Standardization (CEN-CENELEC), which in 2022 established a Joint Technical Committee to develop standards relevant to quantum technologies.[21]

Experts in the GFTech focus group also stress the role of standardisation in ensuring interoperability within and across quantum technologies. Section 2 provided several examples of how quantum sensing and computing technologies could work together in health and environmental applications, highlighting the need for seamless integration. Experts also underscore the importance of interoperability between quantum computers and quantum communication devices to ensure they can function cohesively. While certain types of standardisation could support the development of emerging quantum technologies, experts also caution that premature standards could hinder exploration and potentially close off valuable research avenues.

5 Policy challenges

Infographic 5. What policy challenges could hinder the development of quantum technologies?

International co-operation

Recent trends in international science and technology collaboration highlight the delicate balance between maintaining strategic autonomy and fostering global partnerships (OECD, 2023[125]). As technology becomes increasingly central to geopolitical competition, countries are putting safeguards in place for critical technologies, particularly those with dual-use applications. This focus on security coexists with the inherently collaborative nature of modern research and development, which is global, interdependent and rooted in a wide array of technologies. At the same time, the convergence of economic and security goals has led countries to seek greater self-sufficiency and resilience, particularly by reducing dependencies on strategic competitors. Despite these complexities, robust international partnerships remain essential for addressing global challenges and advancing shared technological goals.

These trends are also shaping quantum technology development. While the knowledge generated from QIST promises significant benefits, it also carries potential digital security risks and military applications. These concerns are driving countries to view support for quantum technologies as a matter of national security. As a result, there has been a decrease in government funding for international collaborations and increased competition among countries for leadership in quantum technologies (Everett, 2021[126]). The potential for strategic surprises (Box 9) induce countries to invest in and develop capacity in quantum technologies domestically, aiming to reduce reliance on other countries. Experts in the GFTech focus group note that as quantum technologies mature, their capabilities, limitations and associated risks will become clearer. This could either increase or reduce governments' perceived risks of cross-country collaboration on certain types of research and applications.

A specific area of concern is the perceived increasing threat to national and economic security that arises from international scientific collaboration. Research security refers to protecting the integrity of research institutions from undue influence by foreign actors, whether state-sponsored or independent (OECD, 2022[127]). Its primary purpose is to shield the research environment to preserve national and economic security and prevent detrimental research practices such as research coercion and theft or misuse of data, among others. By ensuring research security, countries can maintain the reliability and integrity of their research efforts, guarding them against external threats that could potentially compromise or manipulate outcomes.

Research and development collaborations for the development of quantum technologies often need to be international to pool resources and the complementary skills and expertise in talent that can only be found across countries. Governments thus face the challenge of maintaining a balance between fostering open, trust-based international scientific collaborations and imposing protective regulations that may restrict scientific freedom. Over-regulation can hinder progress, while a lack of research security can lead to the misappropriation of research results and the exploitation of an open research environment for foreign interests (OECD, 2022[127]). Geopolitical competition and security concerns over quantum technologies may result in more nationalised, closed ecosystems that are increasingly siloed in countries (Vermaas and Mans, 2024[128]). International scientific collaborations and trade could become more conditional, potentially leading to exclusionary practices such as denying visas for foreign researchers or other forms of technological protectionism that restrict the flow of knowledge (Shelley-Egan and Vermaas, 2024[129]).

Synchronising funding initiatives across borders can help reduce duplication and amplify the impact of public and private investments in quantum technologies, accelerating progress toward the necessary breakthroughs that can help address societal challenges and improve human well-being. Working together, countries can achieve economies of scale and create stronger incentives for investment in research and innovation, making large-scale projects more feasible and cost-effective (OECD, 2024[130]). Sharing experiences and collaborating across borders distributes risks among countries and industries, allowing them to unlock synergies and efficiencies that might not be possible when working in isolation. Moreover, the participation of low- and middle-income countries in international initiatives is crucial for inclusive

progress, as these countries often suffer the most from global challenges like climate change. Their inclusion in international collaboration can help these countries pursue sustainable development paths.

Box 9. Quantum technologies may lead to strategic surprises

One of the main drivers of government investment in quantum technologies is the risk of strategic surprise. Strategic surprise refers to situations where a country gains a substantial advantage over competitors because of unexpected or anticipated breakthroughs or advances. Quantum technologies may result in three main types of strategic surprises:

Remote sensing

Quantum sensing is enabling significant improvements in intelligence, surveillance, reconnaissance, positioning, navigation and timing, providing both strategic and tactical advantages. For example, quantum sensors could detect underground resources and hidden military assets, even those camouflaged or hidden using stealth technology. This capability could enable a nation to map out an adversary's critical infrastructure or detect submarines and other military equipment with unprecedented accuracy. Such developments could disrupt existing military strategies, undermine stealth technologies and expose critical vulnerabilities, thereby altering the balance of power and creating significant security challenges.

Cryptanalysis

A cryptographically relevant quantum computer could allow a well-equipped adversary to decrypt sensitive information, resulting in major security breaches. Quantum cryptanalysis could also forge digital signatures, compromising the integrity of software updates and electronic documents. These capabilities would give attackers the ability to access and manipulate data undetected, making cryptographically relevant quantum computers a profound and disruptive threat.

Weapons development

Quantum simulation could facilitate the rapid development of nuclear, chemical, biological and genetic weapons without the need for physical testing. These developments could occur in secrecy, as simulations could be conducted in small facilities in the privacy of computing environments, making it difficult for other nations to detect and monitor them through traditional intelligence methods. Such capabilities would represent a significant challenge to global security and arms control efforts, as it lowers barriers to creating and stockpiling advanced weapons.

Source: (Hoofnagle and Garfinkel, 2022[3]).

Consensus standards can support international co-operation and act as an alternative to hard regulation (RHC, 2024[47]). These standards help build a shared understanding of quantum technologies, their potential benefits and risks, and contribute to determining optimal strategies for their responsible future development and management. Consensus standards can include principles for responsible innovation, which could help ensure the ethical development of quantum technologies.

Experts in the GFTech focus group acknowledge the challenge of balancing reliable and trustworthy QIST partnerships with global and inclusive collaborations. They emphasise the importance of inclusive multilateral fora for global discussions to ensure the responsible development and use of quantum technologies. Clearly defined and shared expectations on what constitutes responsible development and use, together with the exploration of contributions towards the SDGs, could further facilitate international collaborations and shape countries' ambitions for the quantum future. Various international partnerships

have emerged (Table 3), but participation is often limited, with some countries facing difficulties in joining or engaging them. The OECD can contribute to international co-operation based on shared, human-centric values for quantum technologies.

Table 3. Examples of international initiatives for the governance of quantum technologies

Initiative	Hosted by	Description	Type	More information at
Quantum Development Group	Participating countries	High-level government meetings to discuss potential coordinated approaches to QIST to promote resilient and reliable supply chains, deeper collaboration between innovation ecosystems, and a quantum future in line with shared interests and values, while enabling each country to maintain a competitive environment for quantum developments.	Government driven, with the participation of Australia, Denmark, Finland, France, Germany, Japan, Korea, the United Kingdom and the United States	https://2021-2025.state.gov/deputy-secretary-campbells-inaugural-quantum-development-group-meeting/
Multilateral Dialogue on Quantum	Participating countries	A group of policymakers and technical experts from like-minded countries with significant expertise and programmes in QIST meet on a regular basis to work together to advance the field and grow the global QIST ecosystem.	Government driven, with the participation of Australia, Canada, Denmark, Finland, France, Germany, Japan, Korea, Netherlands, Sweden, Switzerland, United Kingdom and the United States	Meeting readouts: https://www.quantum.gov/readout-international-roundtable-2n/ https://www.quantumwithoutborders.org/multilateral-dialogue-on-quantum
World Commission on the Ethics of Scientific Knowledge and Technology (COMEST)	UNESCO	COMEST is an advisory body and forum of reflection that was set up in 1998. As part of its 2024-2025 work programme, COMEST will address the Ethics of Research, Development and Deployment of Quantum Computing Technologies.	Expert driven, including 18 participants, each from a different nationality. Member States and Associate Members of UNESCO may participate in meetings as observers.	https://www.unesco.org/en/ethics-science-technology/comest
The Quantum Economy Network	World Economic Forum	A global platform for governments, businesses and academia to understand the potential of quantum technologies, shape their development and prepare for their introduction into the economy.	Industry driven	https://initiatives.weforum.org/quantum/home
The Open Quantum Institute	CERN (incubated at GESDA)	A multilateral governance initiative that promotes global and inclusive access to quantum computing and the development of applications for the benefit of humanity.	Research driven	https://open-quantum-institute.cern/
Transatlantic Quantum Community	NATO	Community bringing together quantum experts from national governments, industry, academia, funding bodies, and research institutions to help NATO protect its technological edge.	Defence driven, with the voluntary participation of NATO Member Countries	https://www.nato.int/cps/en/natohq/news_227241.htm
The AUKUS Quantum Arrangement	Participating countries	Partnership aiming to accelerate investments that deliver generation-after-next quantum capabilities.	Defence driven, trilateral security partnership between Australia, the United Kingdom and the United States	https://sgp.fas.org/crs/row/R47599.pdf

Limited and competitive access to skills in the workforce

Quantum technology ecosystems currently offer five main types of technical careers, each requiring a distinct skillset and educational background: engineers, experimental scientists, theoretical physicists, technicians and applications researchers or solutions architects (Table 4). Each career can span various disciplines, such as different branches of engineering and specialisations in computer science. Expertise in QIST, often at the PhD level, is in strong demand, particularly in areas such as quantum theory, quantum

information theory and quantum hardware (Fox, Zwickl and Lewandowski, 2020[131]). The quantum computing industry actively seeks for skills and expertise in quantum algorithms. However, ecosystem actors are also recruiting individuals with varying levels of proficiency in QIST, as well as science, technology, engineering and maths (STEM) professionals who bring complementary skills (Asfaw et al., 2022[132]). Profound expertise in all skills is rarely required, and targeted courses may be sufficient for acquiring the necessary skills rather than pursuing a full, separate degree (Hughes et al., 2021[133]; Asfaw et al., 2022[132]). Experts in the GFTech focus group highlight the importance of recognising both the overlapping and differing skill needs between quantum sensing, computing and communication technologies. Each of these technologies can be further divided into numerous sub-areas with distinct skill requirements. Moreover, their varying levels of maturity make it necessary to closely monitor technological and application developments, as these can lead to significant shifts in skill needs.

Table 4. Technical careers in quantum technology ecosystems require different skills, expertise and educational degrees

Technical career	Role	Skill and expertise needs	Relevant educational degree(s)
Engineer	Design, develop and maintain quantum hardware and software components.	• Strong coding skills for designing and controlling experimental devices. • Knowledge of electronics for controlling and powering hardware. • Experience in troubleshooting and problem-solving in lab environments. • Material science knowledge for designing and building new hardware.	Ranges from bachelor's degree to PhD
Experimental scientist	Test quantum theories and principles.	• Advanced lab experience, typically gained during a PhD programme. • Proficiency in documenting experiments and preparing reports. • Coding skills for data collection and analysis. • Electronics knowledge for manipulating quantum systems.	PhD
Theoretical physicist	Develop and refine theoretical models of quantum phenomena.	• Profound understanding of quantum theory and quantum information science. • Ability to develop new algorithms and translate them to real-world applications. • Strong background in mathematics and computer science.	PhD
Technician	Support engineers and scientists by maintaining and operating equipment.	• Practical experience with quantum laboratory equipment. • Basic coding skills for operating and troubleshooting devices. • Knowledge of electronics, mechanical systems and systems architecture.	Vocational training or bachelor's degree[22]
Application researcher / Solutions architect	Apply quantum technologies to solve real-world problems.	• Knowledge of quantum algorithms and their implementation. • Data science skills, with experience in interpreting results from quantum systems. • Understanding of specific industry applications, such as cryptography or quantum computing.	Ranges from master's degree to PhD

Source: Based on (Fox, Zwickl and Lewandowski, 2020[131]; Hughes et al., 2021[133]).

Prior studies, job board data and other sources suggest a QIST talent shortage at all levels (White House OSTP, 2022[134]; US GAO, 2021[119]; European Commission, 2023[135]). A survey of 501 executives in the United Kingdom revealed that their top priority for preparing their organisations for quantum computing is the development of skills and talent (EY, 2022[136]). Optimistic projections estimate that the growth in the market size for quantum technologies will create approximately 600 000 new jobs by 2040 (Venegas-Gomez, 2020[137]). However, as most quantum technologies are in early stages of development and remain contingent on various challenges being resolved, there is no definitive data that allows anticipating future quantum workforce needs (US GAO, 2021[119]; Dudley and Brazil, 2024[138]).

Several national quantum strategies and programmes address skills shortages, working on the assumption that the demand for talent will likely continue to grow. Selected examples are included below.

- **The European Quantum Flagship** fosters skills development through three key projects: QUCATS, DigiQ and QTIndu (European Quantum Flagship, n.d.[139]). QUCATS focuses on co-ordination and standardisation by analysing industrial needs and developing the European Competence Framework for Quantum Technologies. DigiQ aims to transform the quantum educational ecosystem by launching or upgrading 16 quantum master's degree programmes across 20 European universities. QTIndu provides training and courses to upskill and reskill the workforce both within and outside the quantum technology ecosystem, seeking to address the needs of industry sectors.
- **The United Kingdom's National Quantum Strategy** promotes skills development through several key initiatives (DSIT, 2023[140]). It aims to expand entry pathways into the quantum sector beyond doctoral training, extending pipelines to schools and professionalising quantum engineering skills. Collaborations with professional bodies like the Institution of Engineering and Technology and the Institute of Physics seek to raise awareness and support continuous professional development. The strategy highlights the need for skilled technicians and vocational training, with programmes like the National Physical Laboratory's Apprenticeship Scheme serving as an example. The UK Science and Technology Framework aims to address the broader STEM skills gap, focusing on agile skills systems, STEM teacher recruitment, diverse participation, lifelong training opportunities and attracting international talent.
- **The United States National Quantum Initiative** supports the development of skills through various strategic efforts (White House OSTP, 2022[134]). For instance, the National Science Foundation (NSF), in collaboration with the White House Office of Science and Technology Policy, launched the National Q-12 Education Partnership. This initiative aims to provide quantum education at middle schools, community colleges, and through online courses, preparing students for careers in quantum technologies. Additionally, the NSF's ExpandQISE funding programme aims to increase research capacity and broaden participation in QIST. At the postsecondary level, some colleges and universities have started offering introductory quantum courses designed for non-STEM students, which raise awareness and attract a diverse range of students and professionals to the field. Efforts are also being made to establish new and upgraded undergraduate and master's degree programmes in QIST.

The private sector and other non-government actors have also taken an active role in supporting skills and talent development, for example:

- **IQM**, a Finnish-German quantum computing company, offers an online resource called IQM Academy. This platform provides learning materials for all levels, from beginners to advanced users.
- **IBM** introduced Qiskit, an open-source software platform that helps developers create quantum algorithms using popular programming languages such as Python and JavaScript. This resource makes it easier for programmers to start working with quantum computing. Additionally, Qiskit integrates with various cloud services beyond IBM, which serve as accessible educational tools for a wide audience (Golec et al., 2024[69]).
- **Qubit by Qubit**, a non-profit initiative, provides quantum training programmes for various audiences, from middle school students to educators. Through summer camps, online courses, training sessions and internships, they have trained over 22 500 students. The initiative partners with leading universities and tech companies, including Google, IBM, Microsoft, the University of Maryland and Caltech, to offer high-quality learning resources.

No country is able to meet its QIST skill needs exclusively with its domestic workforce. International talent is crucial for advancing quantum technologies because it brings a diverse array of scientific ideas, experiences and skills that drive innovation and progress (White House OSTP, 2021[141]). Foreign-born researchers and students often have the requisite education and training, which helps quickly bolster the

domestic workforce in critical technical areas. Additionally, the presence of international talent promotes scientific excellence, accelerates technical progress and supports collaborative efforts, both within and across countries.

Maintaining and promoting the flow of international talent is essential for the development of quantum technologies. However, experts in the GFTech focus group also emphasise the importance of addressing research security risks associated with this mobility. Furthermore, while global talent exchange enriches domestic technology ecosystems, it may disadvantage countries that invest in training individuals who subsequently move abroad for work. These concerns extend beyond quantum technologies, applying equally to other specialised fields such as artificial intelligence.

Experts in the GFTech focus group also expressed concerns about the potential pitfalls of relying too heavily on industry demand to shape education systems. They noted that this approach could prioritise immediate QIST needs at the expense of broader educational goals and long-term adaptability for students. Developing a workforce tailored solely to current industry demands is risky, as these needs may be influenced by hype and can shift over time. Therefore, robust technology assessments are essential to forecast future skill requirements and adjust educational programmes accordingly. A broader, more flexible education system could foster skill adaptability, ensuring that new graduates possess competencies beyond quantum technologies, thus enhancing their employability across different fields. In addition, experts highlight the need to assess the competition between the public and private sectors for skilled talent. In particular, they stress the risk of the private sector siphoning talent away from public research organisations, which could hinder the development of quantum technologies. These technologies still face significant technical challenges that require solutions rooted in basic science and engineering, making sustained public research essential.

Constraints in supply chains

As quantum technologies are at early stages of development, supply chains are still developing (Riekeles, 2023[142]). Instead of establishing production lines, technology ecosystems currently focus on exploring different ideas. For example, industry actors are experimenting with different kinds of qubits, including superconductors, photons and neutral atoms (among others), each involving different suppliers. The emerging supply chains are highly global and specialised, involving critical components sourced from various countries (US GAO, 2021[119]). Essential components have limited suppliers, which can create critical dependencies. There is also a risk of key providers being purchased by foreign entities.

Quantum technologies also rely on advanced equipment not widely available due to the small market size. Development is further hindered by the need for expensive, specialised components and materials like helium-3 for cooling. China dominates the mining and refining sector for fourteen of twenty key materials required for QIST, and it controls over half of the global supply for nine of these materials (Mans, Rabbie and Hopman, 2023[143]). In 2023, China implemented export restrictions for gallium and germanium, two critical materials, and has recently taken additional steps to make it harder for foreign companies to purchase rare earth metals (Bradsher, 2024[144]). A survey of 47 quantum computer suppliers in the United States revealed that 60% of respondents anticipate supply chain disruptions involving materials, components or sub-assemblies within the next three years (Sorensen and Sorensen, 2022[145]). Experts in the GFTech focus group highlight that supply chains could shift substantially if a significant breakthrough happens in a particular technology or geographic region.

The considerations around dual-use applications, digital security and privacy, research security and technology leadership described in this paper are also shaping quantum technology supply chains, as countries aim to build domestic capabilities and robust technology ecosystems. Countries are increasingly using export controls to tackle such concerns and mitigate risks (US GAO, 2021[119]; Okano-Heijmans, Gomes and Dekker, 2024[146]; European Quantum Flagship, 2024[147]). France, Spain, the Netherlands,

the United Kingdom and the United States have prohibited the export of quantum computers with 34 or more qubits and error rates below certain thresholds (New Scientist, 2024[148]; Federal Register, 2024[149]). While such controls in principle ensure that legitimate trade can occur, science-industry stakeholders in quantum technology ecosystems are worried that these measures are harming international collaboration and disrupting global supply chains (RHC, 2024[47]). Startups, for instance, find navigating these controls challenging due to their complexity and the fast-paced evolution of the technology. GFTech focus group experts anticipate that export controls will introduce a broader "cooling effect" in quantum technology ecosystems: Uncertainties over compliance costs and the potential for additional regulatory constraints in the future can deter private investment and hinder the creation of academic positions in QIST, among other unintended consequences. Stakeholders are requesting that risk assessments and any subsequent controls on quantum technologies be specific and account for their technological readiness. Overly broad export controls applied equally across quantum sensing, computing, and communication do not consider their varying stages of development and specific risks.

Ensuring access and inclusion to avoid deepening divides

As described in section 4, current investment in quantum technologies is concentrated in developed countries. This concentration raises concerns that quantum technologies may become dominated by a few key players, potentially marginalising other actors (Vermaas, 2017[150]). While commercial concentration is not unique to quantum technologies, the exceptional potential of quantum technologies, particularly quantum computers,[23] might lead to significant "first mover advantages" potentially resulting in monopolies and anti-competitive practices (RHC, 2024[47]). While early quantum computers might initially seem limited, they can offer significant benefits to early adopters, raising concerns about fair and equitable access. Due to their complexity and cost, access to quantum computers may be dominated by large technology companies, potentially restricting access and stifling innovation. Conversely, overly restrictive regulations could hinder technological development and innovation.

The concentration of investment and technological protectionism could also exacerbate divides between emerging and developed countries. Quantum computers are expensive to build and maintain, requiring specialised hardware and technical skills. With the exception of Singapore and India, G77 countries[24] do not have their own quantum computing systems (AWO, 2024[151]). A "quantum divide" would limit the potential socio-economic contributions quantum technologies have to offer. Such a divide also exacerbates digital security concerns in emerging economies, where a lack of capabilities in quantum technologies would imply additional exposure to the risks raised in section 3. Moreover, such a divide could deepen economic inequalities across countries and hinder the most vulnerable nations from leveraging quantum technologies to address pressing societal challenges.

G77 countries are advocating for a greater role in international technology governance, including in the realm of quantum technologies, emphasising the importance of open, equitable scientific collaboration (AWO, 2024[151]). According to GFTech focus group experts, leading countries in quantum technologies may find mutually beneficial collaboration opportunities with emerging economies. This includes addressing the supply chain vulnerabilities mentioned above. An inclusive approach can also help emerging economies engage in human-centric and values-based approaches to developing and using quantum technologies.

Cloud computing services help democratise access to quantum computing, allowing for collaboration across different geographic locations (Golec et al., 2024[69]). These services can make quantum computing more accessible to research and industry actors worldwide. However, in practice, access to such services is subject to the terms of use and restrictions set by cloud computing providers. These are often subject to export control regulations (AWO, 2024[151]). This means that access to quantum cloud services may not be available to individuals residing in or accessing services from affected countries. Even with access, the

costs of cloud-based quantum computing are non-negligible for research and industry actors in emerging economies.[25] Some providers waive these costs under certain conditions. One GFTech focus group expert cited the example of a service provider that offered to waive costs only for specific research areas aligned with the technology company's interests, which may not align with the priorities of research groups in emerging economies.

Other types of divides that could play a role in the development of quantum technologies include connectivity divides and divides related to the under-representation of social groups in research and innovation activities.

- **Communication infrastructures** are the backbone of digital transformation and vital for the use of digital technologies. As digital transformation progresses, the demand for high-quality networks is growing in OECD member countries and networks are evolving to meet such requirements (OECD, 2022[152]). However, connectivity divides between developed and emerging economies and between urban and rural areas remain pervasive worldwide, even within the G20 (OECD, 2021[153]). Given the importance of cloud services for enabling access to quantum computing, divides in access to high-quality networks are likely to hinder the diffusion of this technology across regions and markets. From connecting the unconnected to upgrading existing broadband networks for next-generation access, continuous investments are needed to foster inclusive access to high-quality connectivity (OECD, 2024[154]).
- **The participation of women and other underrepresented social groups** in STEM fields has long been a concern (OECD, 2018[155]), and this is also a significant issue in the QIST field (Physics World, 2023[156]). Experts in the GFTech focus group emphasise the need for long-term strategies to promote an inclusive research environment with opportunities for everyone regardless of gender, race, ethnicity or other factors that may lead to exclusion.

Public engagement in quantum technologies is necessary to ensure their responsible development and broader benefits (Seskir et al., 2023[157]). Engaging citizens helps demystify complex technologies and ensure that societal and ethical implications are understood and addressed (ESPRC, 2018[158]). Experts in the GFTech focus group highlight the importance of building trust among civil society in quantum technologies. Excessive hype can lead to unrealistic expectations and potential mistrust when these are not met. Building trust thus requires raising awareness with open and transparent communication about the goals, limitations and risks of developing and using quantum technologies. Public engagement in the design and implementation of related strategies and policies also fosters a sense of inclusiveness and accountability, which also contributes to building public trust.

The United Nations' proclamation of 2025 as the International Year of Quantum Science and Technology (UNGA, 2024[159]) offers unique opportunities for public engagement. This initiative aims to celebrate the historical contributions of quantum science, raise global awareness of the significance of these technologies in sustainable development and inspire young people to pursue careers in related fields (APS, 2024[160]). It also plans to involve emerging economies by promoting inclusive access to quantum education and opportunities.

6 Outlook

The case for the anticipatory governance of quantum technologies

Quantum technologies promise significant benefits, including commercial applications in a wide range of business sectors and contributions to advancing SDGs. At the same time, these technologies involve digital security and privacy risks, including the potential to compromise data that is being transmitted today. Furthermore, defence applications raise serious concerns for national security, potentially hindering international co-operation and the anticipated benefits of quantum technologies. The OECD Framework for the Anticipatory Governance of Emerging Technologies has identified a set of relevant values (Box 10) that could inform principles of the human-centric and values-based development and use of quantum technologies.

The benefits and risks of quantum technologies identified in this paper could bolster or undermine the Framework's foundational values, as shown by Table 5. Conversely, the policy opportunities and challenges discussed in this paper can reinforce or weaken key technology-specific values (Table 6).

Anticipatory governance and policies are essential to safeguard foundational and technology-specific values (OECD, 2024[161]). This paper highlights the critical role of international co-operation in shaping the impacts quantum technologies will have on these values. Without a consensus on their responsible development and use, and without coordinated efforts, the diffusion of quantum technologies will likely exacerbate risks and diminish potential benefits. Experts in the GFTech focus group warn that an excessive focus on security-related concerns may lead to a multilateral chokehold and can slow down the progress of quantum technologies. Protectionism could stifle commercial applications and impede progress in addressing societal challenges. Furthermore, insufficient international co-operation could result in unethical use and widen technology divides across countries. Ultimately, the lack of coordinated efforts compromises the potential of quantum technologies to contribute to global development and well-being.

Taking stock of the benefits and risks of quantum technologies, along with the policy opportunities and challenges outlined in this paper, the OECD could contribute to the human-centric and values-based development and use of quantum technologies in two main ways:

- Building upon existing international initiatives for the governance of quantum technologies, the OECD could develop a Council Recommendation with principles to reinforce values shared by OECD members. Such a Recommendation could help broaden engagement and build trust in domestic and cross-border collaborations on quantum technologies.
- The OECD could also pursue policy work in areas that could inform and support international co-operation. This includes topics identified in this paper, such as access to skills in the workforce, mapping specialisations in supply chains, and scoping metrics to benchmark quantum technological capabilities. Such work would facilitate identifying and sharing best practices among OECD members and contribute to broader international multistakeholder exchanges that discuss shared values and how these should drive the development and use of quantum technologies.

Box 10. Values for the anticipatory governance of emerging technologies

Foundational values

- **Respect for human rights**, including protections of human dignity and basic liberties such as freedom of thought, freedom of expression and freedom from harms.
- **Safety and security** involve the adoption of measures to minimise risk of harm to economy, environment and human well-being.
- **Privacy**, including the basic interest in being free from interference with other basic rights and liberties, including the protection of personal data.
- **Democratic values**, including the rule of law, equality under law, representation and participation in public life and debate, procedural justice and the advancing the public interest.
- **Sustainable development**, including the responsibility to protect and enhance biodiversity and ecosystems, promote nature-based solutions, and address climate change while promoting human well-being.
- **Equity and inclusion**, recognising diversity and accessibility in its many forms, ensuring fair treatment and full participation of individuals or groups that are vulnerable and/or have been historically excluded or marginalised, and providing fair access to the benefits of innovation.

Technology-specific values

- **Trustworthiness** includes ensuring that technologies, actors and their decisions can be counted on for accuracy, reliability and regulatory compliance.
- **Responsibility** involves the attribution of the consequences, positive or negative, of actions and decisions related to technologies, as well as accountability to those affected or to society in general.
- **Transparency** involves giving an open and honest description of information conveyed, its justification, and limitations, in language that is understandable and accessible.
- **Technology stewardship** places a duty on those with sufficient expertise and knowledge to create and use technology in ways that are aligned with foundational values (e.g. those above) and promote public goods.
- **Innovation for public good** emphasises the important benefits to society from technology innovation, and the need to lower unnecessary barriers to achieve that goal.
- **Responsiveness** requires meeting the expectation that promised technological outcomes are delivered in a timely way.

Source: (OECD, 2024[161]).

Table 5. Quantum technologies could both bolster or undermine the foundational values identified in the Framework for the Anticipatory Governance of Emerging Technology

Foundational value	Potential technology benefits	Potential technology risks
Respect for human rights	• Better health outcomes and more advanced medical care, with early disease detection and improved personalised treatments. • Raising living standards and well-being, by exploring new ways to increase access to food, water and affordable energy.	• Quantum computers could break current cryptographic methods, compromising digital security and threatening individuals' ability to securely participate in economic activities. • The use of quantum technologies for gathering and analysing personal data in areas such as healthcare and finance could expose individuals to discriminatory or prejudicial treatment.
Safety and security	• Improving disaster response, enhancing resilience against environmental and economic disruptions. • Improved monitoring and protection of critical infrastructure, including the early detection of potential faults or threats.	• Military applications of quantum technologies may significantly enhance detection capabilities, optimise logistics and secure the communications of adversaries. • Blind quantum computations could obstruct legal surveillance, making it more difficult to prevent and respond to crimes, including potential quantum-assisted crimes like decrypting sensitive data or developing biological weapons.
Privacy	• Post-quantum cryptography is designed to secure data against the advanced capabilities of quantum computers. It can thereby strengthen privacy, ensuring the confidentiality and integrity of personal data. • In certain cases, quantum communication could ensure secure data transmission, protecting sensitive information across various sectors from cyber threats.	• Quantum sensors, with their advanced capabilities to see through materials and detect objects in unprecedented detail, could lead to intrusive surveillance practices. • Cryptographically relevant quantum computers could lead to unauthorised access to personal data, including data transmitted today.
Democratic values	• The ethical use of quantum sensors could facilitate legal surveillance efforts by law enforcement agencies, • Citizen engagement can help align quantum technology development and use with the broader public interest, and promote public trust, inclusiveness and accountability.	• Quantum computing's ability to break current cryptographic methods could result in widespread data breaches, including sensitive government data. • Misuse or perceived misuse of quantum technologies could erode public trust in institutions and technologies, hindering their potential benefits for society.
Sustainable development	• Quantum computing could contribute to addressing climate change, including by optimising energy usage, improving renewable energy technologies and enhancing carbon capture methods. • Highly sensitive quantum sensors can detect minute changes in environmental parameters, enabling real-time monitoring of ecosystems.	• An increased demand of critical minerals for the development of quantum technologies could have adverse environmental impacts. • Some implementations of quantum computing are energy-intensive.
Equity and inclusion	• The potential contributions to advancing the SDGs in food security and water management would particularly benefit vulnerable and historically excluded communities. • Quantum technologies could optimise the allocation and management of public resources, including in transportation and urban planning.	• Quantum computing technology is highly complex and expensive, likely to be initially accessible only to developed countries. This could exacerbate economic inequalities, limiting the benefits of quantum technologies.

Table 6. Quantum technology policy could both strengthen or weaken technology-specific values identified in the Framework for the Anticipatory Governance of Emerging Technology

Technology-specific value	Potential policy achievements	Potential policy pitfalls
Trustworthiness	• Government support can help quantum technologies reach sufficient maturity and reliability to deliver commercial applications. • Science-industry collaborations can help ensure quantum technologies meet industry demand and standards. • Standards can support the interoperability of quantum technologies.	• Excessive hype can lead to unrealistic expectations and potential mistrust when these expectations are not met. • Supply chain vulnerabilities and limited access to skills in the workforce can compromise the reliability and trustworthiness of quantum technology ecosystems.
Responsibility	• National strategies and funding programmes can help guide the responsible development and use of these technologies.	• Limited international co-operation can lead to potential gaps in regulatory oversight. Technological developments may be siloed and not subjected to broad scrutiny or ethical considerations.
Transparency	• Benchmarks can help stakeholders understand the capabilities of quantum technologies and track their progress. • National security implications require restricting the public dissemination of certain information.	• The complexity of quantum technologies can lead to misunderstandings among the general public and even some actors within the technology ecosystem.
Technology stewardship	• Building quantum readiness and resilience can help make businesses proactive in the responsible integration and use of these technologies. • Science-industry collaborations can help steer the development of quantum technologies in ways that benefit society.	• Economic competition and national security concerns can lead to barriers in technology access and research and development co-operation. This can prevent the sharing of critical information and expertise necessary for advancing quantum technologies in ways that align with foundational values and promote public goods.
Innovation for public good	• Government funding can support the development and use of quantum technologies in line with national priorities and pressing societal challenges.	• A lack of international co-operation can limit the potential of quantum technologies to address global societal challenges. Moreover, a "quantum divide" would exclude emerging economies from the benefits of these technologies. • Insufficient engagement with civil society can lead to a disconnect between technological developments and societal needs. • Market concentration would restrict access to these technologies, reducing the overall socio-economic benefits.
Responsiveness	• Collaboration between public research organisations and the private sector can support the practical applicability of quantum technologies. Moreover, these collaborations can help align short-term and long-term goals.	• Market concentration and premature standardisation and regulation can hinder the commercialisation of quantum technologies. • Limited international co-operation can lead to duplicated efforts and inefficient use of resources.

References

Aiello, C. et al. (2021), "Achieving a quantum smart workforce", *Quantum Science and Technology*, Vol. 6/3, p. 030501, https://doi.org/10.1088/2058-9565/abfa64. [191]

Ajagekar, A. and F. You (2022), "Quantum computing and quantum artificial intelligence for renewable and sustainable energy: A emerging prospect towards climate neutrality", *Renewable and Sustainable Energy Reviews*, Vol. 165, p. 112493, https://doi.org/10.1016/j.rser.2022.112493. [43]

Akarvardar, K. and H. Wong (2023), "Technology Prospects for Data-Intensive Computing", *Proceedings of the IEEE*, Vol. 111/1, pp. 92-112, https://doi.org/10.1109/JPROC.2022.3218057. [178]

Alghamdi, W. and M. Schukat (2021), "Precision time protocol attack strategies and their resistance to existing security extensions", *Cybersecurity*, Vol. 4/1, p. 12, https://doi.org/10.1186/s42400-021-00080-y. [104]

Ali, M. et al. (2023), "Quantum for 6G communication: A perspective", *IET Quantum Communication*, Vol. 4/3, pp. 112-124, https://doi.org/10.1049/qtc2.12060. [71]

Alshowkan, M. et al. (2022), "Authentication of smart grid communications using quantum key distribution", *Scientific Reports 2022 12:1*, Vol. 12/1, pp. 1-13, https://doi.org/10.1038/s41598-022-16090-w. [56]

Altman, E. et al. (2021), "Quantum Simulators: Architectures and Opportunities", *PRX Quantum*, Vol. 2/1, p. 017003, https://doi.org/10.1103/PRXQuantum.2.017003. [176]

ANSSI et al. (2024), *Position Paper on Quantum Key Distribution*, https://cyber.gouv.fr/sites/default/files/document/Quantum_Key_Distribution_Position_Paper.pdf (accessed on 26 July 2024). [28]

APS (2024), *The United Nations Proclaims 2025 as the International Year of Quantum Science and Technology*, https://www.aps.org/about/news/2024/06/united-nations-2025-iyq (accessed on 25 July 2024). [160]

Asfaw, A. et al. (2022), "Building a Quantum Engineering Undergraduate Program", *IEEE Transactions on Education*, Vol. 65/2, pp. 220-242, https://doi.org/10.1109/TE.2022.3144943. [132]

A-SIT et al. (2024), *Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography*, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/PQC-joint-statement.pdf?__blob=publicationFile&v=5 (accessed on 10 December 2024). [94]

Aslam, N. et al. (2023), "Quantum sensors for biomedical applications", *Nature Reviews Physics 2023 5:3*, Vol. 5/3, pp. 157-169, https://doi.org/10.1038/s42254-023-00558-3. [33]

AWO (2024), *Quantum Computing and the G-77*, https://www.ivir.nl/publicaties/download/Quantum-Computing-and-the-G-77.pdf (accessed on 24 July 2024). [151]

Awschalom, D. et al. (2021), "Development of Quantum Interconnects (QuICs) for Next-Generation Information Technologies", *PRX Quantum*, Vol. 2/1, p. 017002, https://doi.org/10.1103/PRXQuantum.2.017002. [180]

Balakrishnan, K. et al. (2023), "Clock synchronization in industrial Internet of Things and potential works in precision time protocol: Review, challenges and future directions", *International Journal of Cognitive Computing in Engineering*, Vol. 4, pp. 205-219, https://doi.org/10.1016/j.ijcce.2023.06.001. [105]

Ball, P. (2020), "Physicists in China challenge Google's 'quantum advantage'", *Nature*, Vol. 588/7838, pp. 380-380, https://doi.org/10.1038/d41586-020-03434-7. [15]

Bambauer, J. (2024), *Quantum Policy: A Primer for Policymakers*, Abundance Institute, https://abundance.institute/articles/a-quantum-policy-primer (accessed on 29 July 2024). [103]

Barak, B. et al. (eds.) (2023), *Technology Primer: Post-Quantum Cryptography*, Belfer Center for Science and International Affairs, Harvard Kennedy School. [185]

Barak, B. et al. (eds.) (2023), *Technology Primer: Post-Quantum Cryptography*, Belfer Center for Science and International Affairs, Harvard Kennedy School, https://www.belfercenter.org/sites/default/files/files/publication/Post%20Quantum%20Cryptography_Tech%20Primer.pdf (accessed on 31 July 2024). [85]

Battarbee, C. et al. (2024), "On the Semidirect Discrete Logarithm Problem in Finite Groups", *Cryptology ePrint Archive* 2024/905, https://eprint.iacr.org/2024/905 (accessed on 10 December 2024). [194]

Belliardo, F., F. Zoratti and V. Giovannetti (2024), "Application of machine learning to experimental design in quantum mechanics", *International Journal of Quantum Information*, https://doi.org/10.1142/S0219749924500023. [80]

Berger, C. et al. (2021), "Quantum technologies for climate change: Preliminary assessment", https://arxiv.org/abs/2107.05362v1 (accessed on 15 July 2024). [49]

Biamonte, J. et al. (2017), "Quantum machine learning", *Nature 2017 549:7671*, Vol. 549/7671, pp. 195-202, https://doi.org/10.1038/nature23474. [77]

BIPM (2024), *Report of BIPM workshop on accelerating the adoption of quantum technologies through measurements and standards*, Bureau International des Poids et Mesures, https://www.bipm.org/documents/20126/259516863/BIPM-WS-QANTUM-TECH+-+Final+Report/687bc6fe-3efb-4003-e074-1f23b2251dcf (accessed on 29 July 2024). [123]

Boger, Y. (2024), *Quantum Computing Has Entered the Logical Qubit Era. Why Does That Matter?*, Built In, https://builtin.com/articles/quantum-computing-logical-qubit-era (accessed on 4 July 2024). [19]

Bova, F., A. Goldfarb and R. Melko (2021), "Commercial applications of quantum computing", [41]

EPJ Quantum Technology 2021 8:1, Vol. 8/1, pp. 1-13, https://doi.org/10.1140/EPJQT/S40507-021-00091-1.

Bradsher, K. (2024), "China Tightens Its Hold on Minerals Needed to Make Computer Chips", *The New York Times*, https://www.nytimes.com/2024/10/26/business/china-critical-minerals-semiconductors.html (accessed on 30 October 2024). [144]

Brooks, M. (2024), *Quantum computing is taking on its biggest challenge — noise*, MIT Technology Review, https://www.technologyreview.com/2024/01/04/1084783/quantum-computing-noise-google-ibm-microsoft/ (accessed on 3 July 2024). [10]

Bruno, G. (2023), "Quantum Computing: A Bubble Ready to Burst or a Looming Breakthrough?", *Bank of Italy Occasional Paper*, No. 716, https://doi.org/10.2139/SSRN.4462929. [48]

BSI (2023), *Implementation Attacks against QKD Systems*, Federal Office for Information Security, Bonn, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/QKD-Systems/QKD-Systems.pdf?__blob=publicationFile&v=3 (accessed on 26 July 2024). [89]

BSI (2018), *Status of quantum computer development*, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Quantencomputer/Entwicklungstand_QC_V_2_0.pdf?__blob=publicationFile&v=2 (accessed on 3 July 2024). [175]

Cacciapuoti, A. et al. (2020), "Quantum Internet: Networking Challenges in Distributed Quantum Computing", *IEEE Network*, Vol. 34/1, pp. 137-143, https://doi.org/10.1109/MNET.001.1900092. [27]

Cao, Y. et al. (2022), "The Evolution of Quantum Key Distribution Networks: On the Road to the Qinternet", *IEEE Communications Surveys and Tutorials*, Vol. 24/2, pp. 839-894, https://doi.org/10.1109/COMST.2022.3144219. [181]

CEN/CENELEC (2023), *Standardization Roadmap on Quantum Technologies*, https://www.cencenelec.eu/media/CEN-CENELEC/AreasOfWork/CEN-CENELEC_Topics/Quantum%20technologies/Documentation%20and%20Materials/fgqt_q04_standardizationroadmapquantumtechnologies_release1.pdf (accessed on 30 July 2024). [188]

Chamkouri, H. et al. (2024), "A first step to develop quantum medicine: Radiometers, detectors, and biosensors", *Sensing and Bio-Sensing Research*, Vol. 44, p. 100658, https://doi.org/10.1016/J.SBSR.2024.100658. [32]

Charley, S. (2022), *From bits to qubits*, Symmetry Magazine, https://www.symmetrymagazine.org/article/from-bits-to-qubits (accessed on 3 July 2024). [162]

Chugh, V. et al. (2023), "Progression in Quantum Sensing/Bio-Sensing Technologies for Healthcare", *ECS Sensors Plus*, Vol. 2/1, p. 015001, https://doi.org/10.1149/2754-2726/acc190. [31]

Coccia, M. (2024), "Converging Artificial Intelligence and Quantum Technologies: Accelerated Growth Effects in Technological Evolution", *Technologies*, Vol. 12/5, p. 66, https://doi.org/10.3390/technologies12050066. [76]

Crawford, S. et al. (2021), "Quantum Sensing for Energy Applications: Review and [42]

Perspective", *Advanced Quantum Technologies*, Vol. 4/8, https://doi.org/10.1002/qute.202100049.

Cuomo, D., M. Caleffi and A. Cacciapuoti (2020), "Towards a distributed quantum computing ecosystem", *IET Quantum Communication*, Vol. 1/1, pp. 3-8, https://doi.org/10.1049/IET-QTC.2020.0002. [22]

Dalzell, A. et al. (2023), "Quantum algorithms: A survey of applications and end-to-end complexities", https://arxiv.org/abs/2310.03011v1 (accessed on 3 July 2024). [9]

Das, S. et al. (2024), "Review—Quantum Biosensors: Principles and Applications in Medical Diagnostics", *ECS Sensors Plus*, Vol. 3/2, p. 025001, https://doi.org/10.1149/2754-2726/AD47E2. [34]

de Castro, A. et al. (2023), *Towards regenerative quantum computing with proven positive sustainability impact*, https://doi.org/10.34734/FZJ-2023-05910. [65]

Degen, C., F. Reinhard and P. Cappellaro (2017), "Quantum sensing", *Reviews of Modern Physics*, Vol. 89/3, p. 035002, https://doi.org/10.1103/REVMODPHYS.89.035002. [177]

Devitt, J. (2024), *Researchers show classical computers can keep up with, and surpass, their quantum counterparts*, Phys.org, https://phys.org/news/2024-02-classical-surpass-quantum-counterparts.html (accessed on 2 July 2024). [14]

Dowling, J. and G. Milburn (2003), "Quantum technology: the second quantum revolution", *Philosophical Transactions of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, Vol. 361/1809, pp. 1655-1674, https://doi.org/10.1098/RSTA.2003.1227. [168]

DSIT (2023), *National Quantum Strategy*, Department for Science, Innovation and Technology, https://assets.publishing.service.gov.uk/media/6411a602e90e0776996a4ade/national_quantum_strategy.pdf (accessed on 8 August 2024). [140]

Dudley, S. and M. Brazil (2024), "Building the Quantum Workforce", *Issues in Science and Technology*, Vol. 40/2, https://issues.org/building-quantum-workforce-education-dudley-brazil-forum/ (accessed on 8 August 2024). [138]

ESPRC (2018), *Quantum Technologies Public Dialogue Report*, https://nqit.ox.ac.uk/content/quantum-technologies-public-dialogue-report.html (accessed on 25 July 2024). [158]

Etim, I. (2022), *Role of quantum technology in sustainable development according to the United Nations*, Quantum Zeitgeist, https://quantumzeitgeist.com/role-of-quantum-technology-in-sustainable-development-according-to-the-united-nations/ (accessed on 15 July 2024). [59]

European Commission (2024), *Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography*, https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography (accessed on 10 December 2024). [93]

European Commission (2023), *The EU's Quantum Technologies Flagship*, https://digital-strategy.ec.europa.eu/en/library/eus-quantum-technologies-flagship (accessed on 8 August 2024). [135]

European Quantum Flagship (2024), *Strategic research and industry agenda*, https://qt.eu/media/pdf/Strategic-Reseach-and-Industry-Agenda-2030.pdf (accessed on 30 July 2024). [147]

European Quantum Flagship (n.d.), *Education and Training: Readying the workforce of Europe's quantum future*, https://qt.eu/ecosystem/education-and-training (accessed on 8 August 2024). [139]

Everett, M. (2021), *EU–US Collaboration on Quantum Technologies*, Chatham House, https://www.chathamhouse.org/sites/default/files/2021-01/2021-01-28-eu-us-quantum-tech-everett.pdf (accessed on 22 July 2024). [126]

EY (2022), *How can you prepare now for the quantum computing future? EY Quantum Readiness Survey 2022*, https://assets.ey.com/content/dam/ey-sites/ey-com/en_uk/topics/emerging-technology/quantum/ey-quantum-readiness-survey-2022.pdf (accessed on 8 August 2024). [136]

Ezratty, O. (2023), "Understanding Quantum Technologies 2023", https://arxiv.org/abs/2111.15352v4 (accessed on 28 June 2024). [6]

Federal Register (2024), *Commerce Control List: Implementation of Controls on Advanced Technologies Consistent with Controls Implemented by International Partners*, https://www.federalregister.gov/d/2024-19633 (accessed on 6 September 2024). [149]

Fedorov, A. et al. (2022), "Quantum computing at the quantum advantage threshold: a down-to-business review", https://arxiv.org/abs/2203.17181v1 (accessed on 10 July 2024). [39]

Finzgar, J. et al. (2022), *QUARK: A Framework for Quantum Computing Application Benchmarking*, IEEE, https://doi.org/10.1109/QCE53715.2022.00042. [117]

Fitzsimons, J. (2017), "Private quantum computation: an introduction to blind quantum computing and related protocols", *npj Quantum Information*, Vol. 3/1, p. 23, https://doi.org/10.1038/s41534-017-0025-3. [100]

Flöther, F. (2023), "The state of quantum computing applications in health and medicine", *Research Directions: Quantum Technologies*, pp. 1-21, https://doi.org/10.1017/qut.2023.4. [36]

Forbes (2023), *DARPA Gets Serious About Quantum: Five-Year Funding To Build Fault-Tolerant Quantum Computers Goes To Atom Computing, Microsoft And PsiQuantum*, https://www.forbes.com/sites/moorinsights/2023/02/01/darpa-gets-serious-about-quantum-five-year-funding-to-build-fault-tolerant-quantum-computers-goes-to-atom-computing-microsoft-and-psiquantum/ (accessed on 18 July 2024). [182]

Fore, M. (2024), *Quantum fiber optics in the brain enhance processing, may protect against degenerative diseases*, Phys.org, https://phys.org/news/2024-04-quantum-fiber-optics-brain-degenerative.html (accessed on 6 August 2024). [190]

Fortune (2024), *The cost of training AI could soon become too much to bear*, https://fortune.com/2024/04/04/ai-training-costs-how-much-is-too-much-openai-gpt-anthropic-microsoft/ (accessed on 15 July 2024). [73]

Fox, M., B. Zwickl and H. Lewandowski (2020), "Preparing for the quantum revolution: What is the role of higher education?", *Physical Review Physics Education Research*, Vol. 16/2, p. 020131, https://doi.org/10.1103/PhysRevPhysEducRes.16.020131. [131]

Fraunhofer IAF (2024), *Quantum magnetometers detect the smallest material defects at an early stage*, https://www.iaf.fraunhofer.de/en/media-library/press-releases/QMag-project-completion.html (accessed on 11 July 2024). [37]

G7 CEG (2024), *G7 Cyber Expert Group Statement on Planning for the Opportunities and Risks of Quantum Computing*. [92]

Gamble, S. (2019), "Quantum Computing: What It Is, Why We Want It, and How We're Trying to Get It", *Frontiers of Engineering*, https://doi.org/10.17226/25333. [13]

Garisto, D. (2023), "The Universe Is Not Locally Real", *Scientific American*, Vol. 328, p. 48, https://doi.org/10.1038/SCIENTIFICAMERICAN0123-48. [173]

Garms, L. et al. (2024), "Experimental Integration of Quantum Key Distribution and Post-Quantum Cryptography in a Hybrid Quantum-Safe Cryptosystem", *Advanced Quantum Technologies*, Vol. 7/4, https://doi.org/10.1002/qute.202300304. [26]

Gent, E., C. Lefebvre and O. Dessibourg (2022), *GESDA impact story: Quantum computing*, GESDA, Geneva, https://gesda.global/wp-content/uploads/2022/09/GESDA-Quantum-Computing-Impact-Story-Apr2022-1.pdf (accessed on 15 July 2024). [62]

Gibney, E. (2019), "Quantum gold rush: the private funding pouring into quantum start-ups", *Nature*, Vol. 574/7776, pp. 22-24, https://doi.org/10.1038/d41586-019-02935-4. [107]

Gidney, C. and M. Ekerå (2021), "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits", *Quantum*, Vol. 5, p. 433, https://doi.org/10.22331/q-2021-04-15-433. [82]

Golec, M. et al. (2024), "Quantum cloud computing: Trends and challenges", *Journal of Economy and Technology*, Vol. 2, pp. 190-199, https://doi.org/10.1016/j.ject.2024.05.001. [69]

GPS.gov (2022), *Timing Applications*, https://www.gps.gov/applications/timing/ (accessed on 27 September 2024). [46]

Gujju, Y., A. Matsuo and R. Raymond (2024), "Quantum machine learning on near-term quantum devices: Current state of supervised and unsupervised techniques for real-world applications", *Physical Review Applied*, Vol. 21/6, p. 067001, https://doi.org/10.1103/PhysRevApplied.21.067001. [78]

Hasan, S. et al. (2023), "Quantum Communication Systems: Vision, Protocols, Applications, and Challenges", *IEEE Access*, Vol. 11, pp. 15855-15877, https://doi.org/10.1109/ACCESS.2023.3244395. [179]

Hoefler, T., T. Häner and M. Troyer (2023), "Disentangling Hype from Practicality: On Realistically Achieving Quantum Advantage", *Communications of the ACM*, Vol. 66/5, pp. 82-87, https://doi.org/10.1145/3571725/ASSETS/HTML/CACM6605_E.GIF. [17]

Homeland Security (2022), *Post-Quantum Cryptography*, https://www.dhs.gov/quantum (accessed on 23 July 2024). [90]

Hoofnagle, C. and S. Garfinkel (2022), *Law and Policy for the Quantum Age*, Cambridge University Press, https://doi.org/10.1017/9781108883719. [3]

Huang, L. et al. (2021), "Quantum random number cloud platform", *npj Quantum Information*, Vol. 7/1, p. 107, https://doi.org/10.1038/s41534-021-00442-x. [55]

Hughes, C. et al. (2021), "Assessing the Needs of the Quantum Industry", *IEEE Transactions on Education*, Vol. 65/4, pp. 592-601, https://doi.org/10.1109/TE.2022.3153841. [133]

ICO (2024), *ICO tech futures: quantum technologies*, https://ico.org.uk/about-the-ico/research-reports-impact-and-evaluation/research-and-reports/technology-and-innovation/ico-tech-futures-quantum-technologies/ (accessed on 11 November 2024). [98]

IEA (2021), *New IEA study examines the future of the ammonia industry amid efforts to reach net zero emissions*, https://www.iea.org/news/new-iea-study-examines-the-future-of-the-ammonia-industry-amid-efforts-to-reach-net-zero-emissions (accessed on 10 July 2024). [44]

Infosecurity Magazine (2010), *Companies undertake first Dutch commercial quantum cryptography project*, https://www.infosecurity-magazine.com/news/companies-undertake-first-dutch-commercial/ (accessed on 12 July 2024). [54]

ISO/IEC (2024), *Information technology — Quantum computing — Vocabulary*, https://www.iso.org/obp/ui/en/#iso:std:iso-iec:4879:ed-1:v1:en (accessed on 29 July 2024). [187]

Jordan, S. (2024), *Quantum Algorithm Zoo*, https://quantumalgorithmzoo.org/ (accessed on 23 July 2024). [166]

Kania, E. and J. Costello (2018), *Quantum hegemony. China's ambitions and the challenge to US innovation leadership*, Center for New American Security (CNAS), Washington, DC. [113]

Kimble, H. (2008), "The quantum internet", *Nature*, Vol. 453/7198, pp. 1023-1030, https://doi.org/10.1038/nature07127. [20]

Kleppner, D. and R. Jackiw (2000), "One Hundred Years of Quantum Physics", *Science*, Vol. 289/5481, pp. 893-898, https://doi.org/10.1126/science.289.5481.893. [2]

Kop, M. et al. (2024), "Ten principles for responsible quantum innovation", *Quantum Science and Technology*, Vol. 9/3, p. 035013, https://doi.org/10.1088/2058-9565/ad3776. [57]

Korolov, M. (2024), *Proof-of-concept quantum repeaters bring quantum networks a big step closer*, Network World, https://www.networkworld.com/article/2114720/proof-of-concept-quantum-repeaters-bring-quantum-networks-a-big-step-closer.html (accessed on 4 July 2024). [25]

Kreiling, L. and C. Paunov (2021), "Knowledge co-creation in the 21st century: A cross-country experience-based policy report", *OECD Science, Technology and Industry Policy Papers*, No. 115, OECD Publishing, Paris, https://doi.org/10.1787/c067606f-en. [118]

Krelina, M. (2021), "Quantum technology for military applications", *EPJ Quantum Technology*, Vol. 8/1, p. 24, https://doi.org/10.1140/epjqt/s40507-021-00113-y. [60]

Krenn, M. et al. (2023), "Artificial intelligence and machine learning for quantum technologies", *Physical Review A*, Vol. 107/1, p. 010101, https://doi.org/10.1103/PhysRevA.107.010101. [79]

Kressel, H. (2023), "The end of Moore's Law? Innovation in computer systems continues at a high pace", in *Artificial Intelligence in Science: Challenges, Opportunities and the Future of Research*, OECD Publishing, Paris, https://doi.org/10.1787/63e48242-en. [68]

Krishnamurthy, V. (2022), "Quantum technology and human rights: an agenda for collaboration*", *Quantum Science and Technology*, Vol. 7/4, p. 044003, [97]

https://doi.org/10.1088/2058-9565/AC81E7.

Lai, J. et al. (2023), "Application and Development of QKD-Based Quantum Secure Communication", *Entropy 2023, Vol. 25, Page 627*, Vol. 25/4, p. 627, https://doi.org/10.3390/E25040627. [24]

Larrue, P. and O. Strauka (2022), "The contribution of RTOs to socio-economic recovery, resilience and transitions", *OECD Science, Technology and Industry Policy Papers*, No. 129, OECD Publishing, Paris, https://www.oecd-ilibrary.org/science-and-technology/the-contribution-of-rtos-to-socio-economic-recovery-resilience-and-transitions_ae93dc1d-en (accessed on 4 November 2022). [183]

Lee, J. et al. (2021), "Even More Efficient Quantum Computations of Chemistry through Tensor Hypercontraction", *PRX Quantum*, Vol. 2/3, p. 030305, https://doi.org/10.1103/PRXQUANTUM.2.030305/FIGURES/20/MEDIUM. [45]

Lewis, J. and G. Wood (2023), *Quantum Technology: Applications and Implications*, Center for Strategic and International Studies, https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-05/230526_Lewis_Quantum_Technology.pdf?VersionId=iCOWm7k02Ms846I0Eb5DLeyD6dZN8K5F (accessed on 28 June 2024). [167]

Liu, R. et al. (2022), "Towards the industrialisation of quantum key distribution in communication networks: A short survey", *IET Quantum Communication*, Vol. 3/3, pp. 151-163, https://doi.org/10.1049/qtc2.12044. [52]

Lubinski, T. et al. (2024), "Quantum Algorithm Exploration using Application-Oriented Performance Benchmarks", https://arxiv.org/abs/2402.08985v1 (accessed on 29 July 2024). [116]

Mannalatha, V., S. Mishra and A. Pathak (2023), "A comprehensive review of quantum random number generators: concepts, classification and the origin of randomness", *Quantum Information Processing*, Vol. 22/12, p. 439, https://doi.org/10.1007/s11128-023-04175-y. [101]

Mans, U., J. Rabbie and B. Hopman (2023), *Critical raw materials for quantum technologies: Towards European technology sovereignty in an emerging industry*, Quantum Delta NL. [143]

Maraveas, C. et al. (2024), "Harnessing quantum computing for smart agriculture: Empowering sustainable crop management and yield optimization", *Computers and Electronics in Agriculture*, Vol. 218, p. 108680, https://doi.org/10.1016/j.compag.2024.108680. [58]

McKinsey (2024), *Quantum Technology Monitor*, https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/steady-progress-in-approaching-the-quantum-advantage (accessed on 16 July 2024). [108]

MIT Technology Review (2020), *We're not prepared for the end of Moore's Law*, https://www.technologyreview.com/2020/02/24/905789/were-not-prepared-for-the-end-of-moores-law/ (accessed on 10 July 2024). [67]

Montanaro, A. (2016), "Quantum algorithms: an overview", *npj Quantum Information 2016 2:1*, Vol. 2/1, pp. 1-8, https://doi.org/10.1038/npjqi.2015.23. [165]

Mosca, M. and M. Piani (2023), *Quantum threat timeline report 2023*, Global Risk Institute, https://globalriskinstitute.org/mp-files/quantum-threat-timeline-report-2023.pdf/ (accessed on 26 July 2024). [84]

Nammouchi, A., A. Kassler and A. Theorachis (2023), "Quantum Machine Learning in Climate Change and Sustainability: a Review", *Proceedings of the AAAI Symposium Series*, Vol. 2/1, pp. 107-114, https://doi.org/10.1609/aaaiss.v2i1.27657. [64]

NATO (2024), *Summary of NATO's Quantum Technologies Strategy*, https://www.nato.int/cps/en/natohq/official_texts_221777.htm (accessed on 13 July 2024). [61]

NCSC (2024), *Next steps in preparing for post-quantum cryptography*, https://www.ncsc.gov.uk/whitepaper/next-steps-preparing-for-post-quantum-cryptography (accessed on 27 September 2024). [88]

New Scientist (2024), *Multiple nations enact mysterious export controls on quantum computers*, https://www.newscientist.com/article/2436023-multiple-nations-enact-mysterious-export-controls-on-quantum-computers/ (accessed on 30 July 2024). [148]

NIST (2024), *NIST Releases First 3 Finalized Post-Quantum Encryption Standards*, https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards (accessed on 29 August 2024). [87]

Nivelkar, M. and S. Bhirud (2021), *Optimized Machine Learning: Training and Classification Performance Using Quantum Computing*, IEEE, https://doi.org/10.1109/ICCCA52192.2021.9666429. [75]

NQCO (2022), *Summary of the workshop on cybersecurity of quantum computing*, National Quantum Coordination Office, https://www.quantum.gov/wp-content/uploads/2022/11/2022-Workshop-Cybersecurity-Quantum-Computing.pdf (accessed on 29 July 2024). [102]

NSA (2021), *Quantum Computing and Post-Quantum Cryptography*, https://media.defense.gov/2021/Aug/04/2002821837/-1/-1/1/Quantum_FAQs_20210804.PDF (accessed on 26 July 2024). [86]

NYU Abu Dhabi (2024), *NYUAD Hackathon for Social Good Concludes With Innovative AI and Quantum Computing Solutions for UN Sustainable Development Goals*, https://nyuad.nyu.edu/en/news/latest-news/science-and-technology/2024/may/twelfth-nyuad-hackathon.html (accessed on 15 July 2024). [66]

O'Connell, C. (2019), *Quantum computing for the qubit curious*, Cosmos Magazine, https://cosmosmagazine.com/science/quantum-computing-for-the-qubit-curious/ (accessed on 3 July 2024). [171]

OECD (2024), "Financing broadband networks of the future", *OECD Digital Economy Papers*, No. 365, OECD Publishing, Paris, https://doi.org/10.1787/eafc728b-en. [154]

OECD (2024), "Framework for Anticipatory Governance of Emerging Technologies", *OECD Science, Technology and Industry Policy Papers*, No. 165, OECD Publishing, Paris. [161]

OECD (2024), *Key concepts and current technical trends in cryptography for policy makers*, OECD Publishing, Paris, https://doi.org/10.1787/29d9fbad-en (accessed on 4 July 2024). [23]

OECD (2024), "National Accounts at a Glance", *OECD National Accounts Statistics (database)*. [112]

OECD (2024), "OECD Agenda for Transformative Science, Technology and Innovation Policies", *OECD Science, Technology and Industry Policy Papers*, No. 164, OECD Publishing, Paris, https://doi.org/10.1787/ba2aaf7b-en. [130]

OECD (2024), *OECD Digital Economy Outlook 2024 (Volume 1): Embracing the Technology Frontier*, OECD Publishing, Paris, https://doi.org/10.1787/a1689dc5-en. [70]

OECD (2024), *Recommendation of the Council on Artificial Intelligence*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 (accessed on 4 September 2024). [193]

OECD (2024), "Shaping a rights-oriented digital transformation", *OECD Digital Economy Papers*, No. 368, OECD Publishing, Paris, https://doi.org/10.1787/86ee84e2-en. [99]

OECD (2023), "Emerging privacy-enhancing technologies: Current regulatory and policy approaches", *OECD Digital Economy Papers*, No. 351, OECD Publishing, Paris, https://doi.org/10.1787/bf121be4-en. [186]

OECD (2023), "Report on the implementation of the OECD Privacy Guidelines", *OECD Digital Economy Papers*, No. 361, OECD Publishing, Paris. [96]

OECD (2023), "Science, technology and innovation policy in times of strategic competition", in *OECD Science, Technology and Innovation Outlook 2023: Enabling Transitions in Times of Disruption*, OECD Publishing, Paris, https://doi.org/10.1787/f3c247fc-en. [125]

OECD (2022), "Broadband networks of the future", *OECD Digital Economy Papers*, No. 327, OECD Publishing, Paris, https://doi.org/10.1787/755e2d0c-en. [152]

OECD (2022), "Integrity and security in the global research ecosystem", *OECD Science, Technology and Industry Policy Papers*, No. 130, OECD Publishing, Paris, https://doi.org/10.1787/1c416f43-en. [127]

OECD (2021), *Bridging digital divides in G20 countries*, OECD Publishing, Paris, https://doi.org/10.1787/35c1d850-en. [153]

OECD (2021), "Effective policies to foster high-risk/high-reward research", *OECD Science, Technology and Industry Policy Papers*, No. 112, OECD Publishing, Paris, https://doi.org/10.1787/06913b3b-en. [109]

OECD (2018), "Gender in a changing context for STI", in *OECD Science, Technology and Innovation Outlook 2018: Adapting to Technological and Societal Disruption*, OECD Publishing, Paris, https://doi.org/10.1787/sti_in_outlook-2018-12-en. [155]

OECD (2013), *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188 (accessed on 29 July 2024). [95]

Okano-Heijmans, M., A. Gomes and B. Dekker (2024), *Balancing openness, economic security and national security: The future of export controls on quantum technologies*, Netherlands Institute of International Relations 'Clingendael', The Hague, https://www.clingendael.org/sites/default/files/2024-04/Clingendael_report_The_future_of_export_controls_on_quantum_technologie.pdf (accessed on 30 July 2024). [146]

Omaar, H. and M. Makaryan (2024), "How Innovative Is China in Quantum?", *Information Technology and Innovation Foundation (ITIF)*, https://itif.org/publications/2024/09/09/how-innovative-is-china-in-quantum/ (accessed on 30 October 2024). [114]

Pasternack, A. (2024), *IBM built the biggest quantum computer. Now comes the hard part*, Fast Company, https://www.fastcompany.com/90992708/ibm-quantum-system-two (accessed on 3 July 2024). [11]

Patra, S. et al. (2024), "Efficient tensor network simulation of IBM's largest quantum processors", *Physical Review Research*, Vol. 6/1, p. 013326, https://doi.org/10.1103/PhysRevResearch.6.013326. [16]

Paudel, H. et al. (2022), "Quantum Computing and Simulations for Energy Applications: Review and Perspective", *ACS Engineering Au*, Vol. 2/3, pp. 151-196, https://doi.org/10.1021/ACSENGINEERINGAU.1C00033. [40]

Physics World (2023), *Why we must build an inclusive quantum community*, https://physicsworld.com/a/why-we-must-build-an-inclusive-quantum-community/ (accessed on 25 July 2024). [156]

Preskill, J. (2021), "Quantum computing 40 years later", *Feynman Lectures on Computation: Anniversary Edition*, pp. 193-243, https://doi.org/10.1201/9781003358817-7. [12]

Preskill, J. (2012), "Quantum computing and the entanglement frontier", https://arxiv.org/abs/1203.5813v3 (accessed on 4 July 2024). [8]

Purohit, A. et al. (2024), "Building a quantum-ready ecosystem", *IET Quantum Communication*, Vol. 5/1, pp. 1-18, https://doi.org/10.1049/QTC2.12072. [29]

QED-C (2024), *Quantum Computing for Transportation and Logistics*, https://quantumconsortium.org/mp-files/quantum-computing-for-transportation-and-logistics-2024.pdf/ (accessed on 10 July 2024). [50]

QED-C (2023), *Guide to Building a Quantum Technician Workforce*, Quantum Economic Development Consortium, Arlington, VA, https://quantumconsortium.org/workforce23/ (accessed on 8 August 2024). [192]

QED-C (2022), *Public-Private Partnerships in Quantum Computing: The Potential for Accelerating Near-Term Quantum Applications*, Quantum Economic Development Consortium, Arlington, VA, https://quantumconsortium.org/ppp22/ (accessed on 18 July 2024). [120]

Quantum Delta NL (2023), *Exploratory quantum technology assessment: Direct the impact of quantum technology*, https://assets.quantum-delta.prod.verveagency.com/assets/exploratory-quantum-technology-assessment---engels.pdf (accessed on 15 July 2024). [63]

Quantum Insider (2023), *The Quantum Insider Report Details China's Emergence as a Global Leader in Quantum Investment and Research*, https://thequantuminsider.com/2023/03/23/the-quantum-insider-report-details-chinas-emergence-as-a-global-leader-in-quantum-investment-and-research/ (accessed on 21 October 2024). [111]

Quddus Islam, T. and R. Garlick (2024), *Quantum Sensing: Tech's New Eyes and Ears*, Citi, https://www.citivelocity.com/t/r/eppublic/2zlpv (accessed on 27 June 2024). [5]

QuEra (2023), *What is Measurement in Quantum Computing*, https://www.quera.com/glossary/measurement (accessed on 3 July 2024). [163]

Qureca (2024), *Quantum Initiatives Worldwide 2024*, https://www.qureca.com/quantum-initiatives-worldwide/ (accessed on 21 October 2024). [110]

Rauscher, C., V. Janssen and R. Minihold (2001), *Fundamentals of spectrum analysis*, Rohde & Schwarz GmbH & Co. KG, Munich. [7]

RHC (2024), *The regulation of quantum technology applications*, Regulatory Horizons Council, https://assets.publishing.service.gov.uk/media/65ddc83bcf7eb10015f57f9f/RHC_regulation_of_quantum_technology_applications.pdf (accessed on 10 July 2024). [47]

Riekeles, G. (2023), "Quantum technologies and value chains: Why and how Europe must act now", *Discussion Paper*, European Policy Centre, https://www.epc.eu/content/PDF/2023/Quantum_Technologies_DP.pdf (accessed on 30 July 2024). [142]

Rozenman, G. et al. (2023), "The quantum internet: A synergy of quantum information technologies and 6G networks", *IET Quantum Communication*, Vol. 4/4, pp. 147-166, https://doi.org/10.1049/qtc2.12069. [72]

Schuld, M. and N. Killoran (2022), "Is Quantum Advantage the Right Goal for Quantum Machine Learning?", *PRX Quantum*, Vol. 3/3, p. 030101, https://doi.org/10.1103/PRXQuantum.3.030101. [164]

Seskir, Z. et al. (2023), "Democratization of quantum technologies", *Quantum Science and Technology*, Vol. 8/2, p. 024005, https://doi.org/10.1088/2058-9565/acb6ae. [157]

Sevilla, J. and C. Riedel (2020), "Forecasting timelines of quantum computing", https://arxiv.org/abs/2009.05045v2 (accessed on 26 July 2024). [83]

Shamshad, S. et al. (2022), "An Enhanced Architecture to Resolve Public-Key Cryptographic Issues in the Internet of Things (IoT), Employing Quantum Computing Supremacy", *Sensors*, Vol. 22/21, p. 8151, https://doi.org/10.3390/s22218151. [81]

Shams, M. et al. (2023), "The Quantum-Medical Nexus: Understanding the Impact of Quantum Technologies on Healthcare", *Cureus*, Vol. 15/10, https://doi.org/10.7759/CUREUS.48077. [30]

Shelley-Egan, C. and P. Vermaas (2024), "European technological protectionism and the risk of moral isolationism: The case of quantum technology development", *Journal of Responsible Technology*, Vol. 18, p. 100084, https://doi.org/10.1016/j.jrt.2024.100084. [129]

Singh, A. et al. (2021), "Quantum Internet - Applications, Functionalities, Enabling Technologies, Challenges, and Research Directions", *IEEE Communications Surveys and Tutorials*, Vol. 23/4, pp. 2218-2247, https://doi.org/10.1109/COMST.2021.3109944. [51]

Sorensen, B. and T. Sorensen (2022), *Challenges and opportunities for securing a robust US quantum computing supply chain*, Quantum Economic Development Consortium (QED-C), https://quantumconsortium.org/quantum-computing-supply-chain-issues/ (accessed on 30 July 2024). [145]

Stanford Encyclopedia of Philosophy (2024), *Quantum Computing*, https://plato.stanford.edu/entries/qt-quantcomp/ (accessed on 3 July 2024). [174]

Taylor-Smith, K. (2020), *An Introduction to the Quantum Mechanics of Nanoparticles*, AZoQuantum, https://www.azoquantum.com/Article.aspx?ArticleID=179 (accessed on [172]

3 July 2024).

TechInformed (2023), *HSBC trials quantum cyber defence system with BT, Toshiba and AWS*, https://techinformed.com/hsbc-trials-quantum-cyber-defence-system-with-bt-toshiba-and-aws/ (accessed on 10 July 2024). [53]

Tzalenchuk, A. et al. (2022), "The expanding role of National Metrology Institutes in the quantum era", *Nature Physics*, Vol. 18/7, pp. 724-727, https://doi.org/10.1038/s41567-022-01659-z. [124]

UKRI (2023), *Commercialising quantum technologies challenge*, https://www.ukri.org/what-we-do/browse-our-areas-of-investment-and-support/commercialising-quantum-technologies-challenge/ (accessed on 18 July 2024). [115]

UNGA (2024), "International Year of Quantum Science and Technology, 2025", *Res*, No. 78/278, United Nations General Assembly, https://documents.un.org/doc/undoc/gen/n24/175/79/pdf/n2417579.pdf (accessed on 4 August 2024). [159]

University of Waterloo (2024), *What is quantum mechanics?*, https://uwaterloo.ca/institute-for-quantum-computing/quantum-mechanics (accessed on 12 July 2024). [1]

Ur Rasool, R. et al. (2023), "Quantum Computing for Healthcare: A Review", *Future Internet*, Vol. 15/3, p. 94, https://doi.org/10.3390/fi15030094. [35]

US GAO (2021), *Report to Congressional Addressees: Quantum Computing and Communications—Status and Prospects*, United States Government Accountability Office, https://www.gao.gov/assets/gao-22-104422.pdf (accessed on 18 July 2024). [119]

US GAO (2020), *Information Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks*, United States Government Accountability Office, https://www.gao.gov/assets/gao-21-171.pdf (accessed on 30 July 2024). [189]

US NSTC (2022), *Bringing Quantum Sensors to Fruition*, https://www.nsf.gov/news/news_images.jsp?cntn_id=296867&org=NSF (accessed on 2 July 2024). [4]

van Deventer, O. et al. (2022), "Towards European standards for quantum technologies", *EPJ Quantum Technology*, Vol. 9/1, p. 33, https://doi.org/10.1140/epjqt/s40507-022-00150-1. [122]

Vedral, V. (2011), *Living in a Quantum World*, Scientific American, https://www.scientificamerican.com/article/living-in-a-quantum-world/ (accessed on 2 July 2024). [169]

Venegas-Gomez, A. (2020), "The Quantum Ecosystem and Its Future Workforce", *PhotonicsViews*, Vol. 17/6, pp. 34-38, https://doi.org/10.1002/phvs.202000044. [137]

Vermaas, P. (2017), "The societal impact of the emerging quantum technologies: a renewed urgency to make quantum theory understandable", *Ethics and Information Technology*, Vol. 19/4, pp. 241-246, https://doi.org/10.1007/s10676-017-9429-1. [150]

Vermaas, P. and U. Mans (2024), "Quantum technologies and their global impact: Discussion paper", *Digital Transformation Dialogue*, UNESCO, Paris. [128]

Vuijk, G. and J. Schmalenberg (eds.) (2020), *Quantum Technologies: The Future is Quantum... and the Future is Now*. [121]

Waters, R. (2024), *Quantum computing breakthroughs draw investment back to sector*, Financial Times, https://www.ft.com/content/d0b486ab-ed6c-46f0-b7b6-66cc60780efe (accessed on 3 July 2024). [18]

West, M. et al. (2023), "Towards quantum enhanced adversarial robustness in machine learning", *Nature Machine Intelligence*, Vol. 5/6, pp. 581-589, https://doi.org/10.1038/s42256-023-00661-1. [106]

White House (2022), *National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems*, https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/ (accessed on 26 September 2024). [91]

White House OSTP (2022), *Quantum Information Science and Technology Workforce Development National Strategic Plan: A Report by the Subcommittee on Quantum Information Science Committee on Science of the National Science & Technology Council*, https://www.quantum.gov/wp-content/uploads/2022/02/QIST-Natl-Workforce-Plan.pdf (accessed on 8 August 2024). [134]

White House OSTP (2021), *The Role of International Talent in Quantum Information Science: A report by the Subcommittee on Economic and Security Implications of Quantum Science of the National Science and Technology Council*, https://www.quantum.gov/wp-content/uploads/2021/10/2021_NSTC_ESIX_INTL_TALENT_QIS.pdf (accessed on 8 August 2024). [141]

World Economic Forum (2022), *State of Quantum Computing: Building a Quantum Economy*, https://www3.weforum.org/docs/WEF_State_of_Quantum_Computing_2022.pdf (accessed on 2 July 2024). [170]

Zeguendry, A., Z. Jarir and M. Quafafou (2023), "Quantum Machine Learning: A Review and Case Studies", *Entropy*, Vol. 25/2, p. 287, https://doi.org/10.3390/e25020287. [74]

Zhang, Z. and Q. Zhuang (2020), "Distributed Quantum Sensing", *Quantum Science and Technology*, Vol. 6/4, https://doi.org/10.1088/2058-9565/abd4c3. [21]

Zhao, M. et al. (2023), "Quantum Sensing of Thermoelectric Power in Low-Dimensional Materials", *Advanced Materials*, Vol. 35/27, p. 2106871, https://doi.org/10.1002/ADMA.202106871. [38]

Zhong, H. et al. (2020), "Quantum computational advantage using photons", *Science*, Vol. 370/6523, pp. 1460-1463, https://doi.org/10.1126/science.abe8770. [184]

Notes

[1] Particles of less than 100 nanometres in size tend to be governed by quantum effects (Taylor-Smith, 2020[172]). For reference, a sheet of paper is about 100 000 nanometres thick. Many biological molecules, such as viruses and proteins, are in the range of tens to hundreds of nanometres.

[2] Quantum effects are most typically observed at these scales because, at larger scales, objects have more complex interactions with their surroundings, causing such effects to disappear. Quantum effects, however, have been demonstrated to persist at larger scales, i.e. in molecules and specific materials, even at room temperature. They are suspected to operate in migratory birds and in photosynthesis (Vedral, 2011[169]) and recent research has discovered they play a role in brain activity (Fore, 2024[190]).

[3] Classical information and communications technologies are those that gather, process and transmit information using classical bits.

[4] Quantum sensing has its roots in metrology, where quantum devices have been used to more accurately measure units or fundamental constants, redefining the world's measurement system (Tzalenchuk et al., 2022[124]). For example, atomic clocks use transitions between energy levels in atoms to define the second as a unit of time with extraordinary precision. The international metre standard defined in 1889 by a platinum-iridium bar at the International Bureau of Weights and Measures in Sèvres, France, remained in use until 1960, when it was more precisely redefined using quantum sensing devices. Since May 2019, all physical units have been redefined based on fundamental constants of nature, largely enabled by advances in quantum measurement techniques (Tzalenchuk et al., 2022[124]).

[5] Atomic clocks are essential in providing precise timing signals to GPS satellites, which in turn allow GPS receivers on Earth to accurately calculate their position, velocity and time. Without atomic clocks, the accuracy required for GPS to function reliably across various applications would not be achievable.

[6] Section 1.3 of (Stanford Encyclopedia of Philosophy, 2024[174]) provides a historical overview of the development of quantum algorithms.

[7] See (BSI, 2018[175]) for an assessment of various quantum computing platforms.

[8] In particular, the no-cloning theorem states that it is impossible to create an exact copy of an unknown quantum state.

[9] A survey of quantum simulators and their applications in science is available at (Altman et al., 2021[176]).

[10] Innovative methods in credit scoring can raise concerns around data privacy, fairness and the explainability of the models (Bruno, 2023[48]).

[11] EuroQCI will be an integral part of IRIS², the new EU space-based secure communication system. See https://defence-industry-space.ec.europa.eu/eu-space/iris2-secure-connectivity_en.

[12] Specifically, asymmetric cryptography, also known as public-key cryptography, which uses a pair of keys: a public key that anyone can access and a private key that is kept secret. The public key encrypts data, and the private key decrypts it. This system eliminates the need to share private keys, thus reducing the risk of interception during key exchange (OECD, 2024[23]). Discrete logarithms are another type of maths problem used by existing cryptographic systems, which are also exposed to quantum attacks (Battarbee et al., 2024[194]).

[13] For example, QKD solutions do not inherently verify the identity of the source sending the quantum signals (OECD, 2024[23]). Currently, the sender and receiver need to rely on either asymmetric cryptography or preinstalled keys to achieve such authentication.

[14] Privacy-enhancing technologies (PETs) include digital technologies, approaches and tools that enable data processing and analysis while safeguarding the confidentiality and, in some cases, the integrity and availability of the data (OECD, 2023[186]). PETs thereby protect the privacy of data subjects and the commercial interests of data controllers.

[15] Cryptographic methods use random numbers to generate strong encryption keys. Classical random number generators rely on algorithms and initial seed values, making them predictable and, therefore, vulnerable. In contrast, quantum random number generators are devices that use quantum effects to create truly random numbers (Mannalatha, Mishra and Pathak, 2023[101]). Quantum random number generators are a mature technology with commercial products already available. They offer a higher level of security and have valuable applications in cybersecurity and financial transactions, among other areas.

[16] A cryptographic method allowing certain computations to be performed on encrypted data without the need to decrypt it first, and without requiring access to the secret key. The result of such computations is also delivered in encrypted form for the user to privately decrypt (OECD, 2024[23]).

[17] GPS is commonly used as a network time reference (Alghamdi and Schukat, 2021[104]).

[18] See (Zhong et al., 2020[184]).

[19] For a review of research and technology organisations and their funding, governance and policy context, see (Larrue and Strauka, 2022[183]).

[20] The cost of participating in standards negotiations is often prohibitive, and the lengthy process of creating international standards is impractical for many SMEs due to the significant time and resource commitments required (RHC, 2024[47]).

[21] See the Committee's proposed roadmap for the standardisation of quantum technologies (CEN/CENELEC, 2023[188]).

[22] A survey of technician job postings in the United States quantum industry showed that 28% of postings did not require any level of education (QED-C, 2023[192]).

[23] Market concentration issues are, however, not limited to quantum computing; other quantum technologies may pose similar risks. For example, access to atomic clocks could give certain firms in the financial sector an unfair advantage (RHC, 2024[47]).

[24] The list of G77 Member States is available at https://www.g77.org/doc/members.html.

[25] One expert in the GFTech focus group cited USD 70 000 for 12 hours of a quantum computer.

Annex A. Quantum computing in depth

The quantum advantage is rooted in the difference between bits and qubits

A classical computer with N bits can represent and process data in 2^N states. For example. a single bit has two states (0 or 1), two bits have four possible states (00, 01, 10, 11) and three bits have eight states (000, 001, 010, 011, 100, 101, 110, 111). With 77 bits, a classical computer can technically represent an immense number of states, i.e. 2^{77} or about 151 sextillion states. However, bits can only be in one state at a time. Cycling through all these combinations, even at a rapid rate like 63 billion operations per second (typical for modern PCs), would require approximately 76 000 years. Today's most powerful supercomputers could do it in almost two days at a rate of a quintillion operations per second.

In contrast, quantum computers can process these combinations simultaneously thanks to the quantum properties of qubits. In a state of superposition, qubits embody information as probabilities of being 0 or 1. In theory, this capability allows quantum computers to achieve dramatic speedups in solving problems considered challenging or impossible for classical computers. A quantum computer with 300 qubits that performs as intended would have 2^{300} possible configurations, more than the number of particles in the known universe (Charley, 2022[162]).

When qubits are measured, they irreversibly collapse to a specific state (0 or 1), losing their quantum properties and the information they hold. As the information is encoded in probabilities, multiple measurements are needed to extract information from quantum computers (QuEra, 2023[163]). After an operation, while classical bits will always be 0 or 1, qubits may be 0 sometimes and 1 other times. Multiple measurements are therefore needed to reveal the probability defined by the quantum state (e.g. obtaining "1" 70% of the time and "0" 30% of the time).

Quantum computing algorithms

Table 7 lists various quantum algorithms, their computation types, sample applications and potential speedups over classical computing algorithms. The performance of "heuristic" algorithms like the Quantum Approximate Optimisation Algorithm (QAOA) and quantum machine learning, which aim to provide approximate solutions when exact ones are impractically time-consuming or complex, is not understood in a rigorous or theoretical way. As an OECD GFTech focus group expert explains, such algorithms are not susceptible to mathematical proofs that allow for the precise calculation of speedup gains. For this reason, it remains possible that such algorithms do not see significant quantum advantage. Their performance will only be learned by running them at progressively larger scales as quantum computing capacity increases. However, the quest for quantum advantages in algorithms might be misguided because it focuses too narrowly on very specific problems already tackled using classical algorithms. This narrow set of problems does not reflect the broader applicability and practical utility of quantum computing (Schuld and Killoran, 2022[164]).

Table 7. Selected quantum algorithms and their speedup over classical algorithms

Algorithm	Type of computation	Sample applications	Speedup[1]
Shor	Integer factorisation	Cryptanalysis	Super-polynomial
Hamiltonian	Simulation of quantum phenomena	Chemical dynamics, condensed matter physics, open quantum systems, etc.	Super-polynomial
Ramesh and Vinay[2]	Pattern matching	Genomic sequence matching. Optimising quantum circuits.	Super-polynomial in some cases
Grover	Search	Search in large, unstructured databases. Many optimisation problems can be framed as search problems	Polynomial
Harrow, Hassidim and Lloyd (HHL)	Solving linear equations	Financial portfolio optimisation, supply chain management, machine learning, power-grid management, fluid dynamics, aerodynamics and thermodynamics simulations.	Polynomial
Adiabatic	Optimisation	Financial portfolio optimisation, traffic congestion management, energy grid management and quantum chemistry.	Polynomial
Quantum Approximate Optimisation Algorithm (QAOA)	Optimisation	Travelling Salesman Problem, Social Network Analysis, data clustering, protein folding, energy grid management.	Unknown
Quantum machine learning	Data classification and training of AI	Reinforcement learning	Unknown

Notes:
[1] Speedup refers to how much faster a quantum computer can solve a problem compared to a classical computer. A polynomial speedup means that a quantum algorithm can solve a problem relatively faster than a classical algorithm, but the improvement is moderate. For example, if a classical computer takes 10 hours to solve a problem, a quantum computer with a polynomial speedup might solve the same problem in 1 hour. A super-polynomial speedup represents a dramatic improvement. If a classical computer would take 100 years to solve a problem, a quantum computer with super-polynomial speedup might solve it in just a few minutes. For some algorithms, the anticipated speedup is unknown because they are designed to work well in practice but lack mathematical proofs demonstrating that they are faster than the best classical algorithms.
[2] This is a hybrid quantum-classical algorithm that combines Grover with a classical computing algorithm.
Source: Adapted from (Montanaro, 2016[165]; Jordan, 2024[166]).