arcep
autorité de régulation
des communications électroniques,
des postes et de la distribution de la presse

RÉPUBLIQUE FRANÇAISE

FUTURE NETWORKS

Briefing note / Quantum technologies and their impact on networks

11 June 2026

ISSN n°2258-3106

Arcep's 'Future Networks' initiative and its Scientific Committee

What form could future networks take and how could they affect Arcep's role as a regulator? What new players might emerge and how could business models evolve across the sectors regulated by the Authority?

To support this forward-looking work and develop a comprehensive understanding of these changes over a five- to ten-year horizon, Arcep has invited twelve distinguished experts from academia, entrepreneurship and industry, representing a range of specialist fields, to form a Scientific Committee. To ensure this reflection is as broad and well-rounded as possible, Arcep's teams also engage with specialist stakeholders across the ecosystem, including network operators, equipment manufacturers, internet companies, service providers and local authorities.

Arcep shares the findings of this work as it progresses through a series of thematic briefing notes, freely available on its website, with the aim of informing and contributing to public debate.

Jean-Luc Beylat
VP Ecosystem, Nokia

Eric Brousseau
Professeur, Université Paris-Dauphine

Giovanna Carofiglio
Senior Director, Cisco

Grazia Cecere
Professeure, Institut Mines Télécom

Amira Alloum
Directrice Ingénierie, Qualcomm France

Serge Fdida
Professeur, Sorbonne Université

Yves Gassot
Consultant indépendant

Nolwenn Germain
Présidente fondatrice, HAIDO

Isabelle Hilali
CEO fondatrice, datacraft

Christophe Bejina
DSI, Alcatel Submarine Networks

Christian Licoppe
Directeur département, Institut Polytechnique Paris

Françoise Soulié-Fogelman
Conseillière scientifique, Hub France IA

Would you like to contribute to this work?

This initiative is intended to be an ongoing and collaborative effort. Arcep invites anyone wishing to contribute to these analyses to send their contributions to reseaux-du-futur@arcep.fr

Would you like to be informed about upcoming briefing note presentations?

Please contact com@arcep.fr for an invitation.

Other briefing notes

At the time of publication of this paper (May 2025), a first briefing note has already been published: "Telecoms with an IT core" (October 2024).

Future notes will be published on the dedicated 'Future Networks' webpage.

Quantum technologies and their impact on networks

Table of contents

1. Introduction....4
2. Quantum computing....5
   - 2.1. How quantum computers operate....5
   - 2.2. The potential of quantum computers....5
   - 2.3. Quantum computing applications....7
   - 2.4. Challenges and future prospects for quantum computing....8
   - 2.5. Global roadmap....9
   - 2.6. Artificial intelligence and quantum computing: synergies and hybridisation challenges 10
   - 2.7. Cloud-based quantum computing and the first computations....11
   - 2.8. Quantum computing and the needs of the telecoms sector....12
3. Quantum computers: a threat or a revolution for communication security?....13
   - 3.1. Quantum threats for telecoms markets....14
   - 3.2. Responses to quantum threats....15
4. Quantum networks....17
   - 4.1. Technological challenges....18
   - 4.2. The role of digital infrastructures in the emergence of quantum networks....19
5. National and European quantum strategies....20
   - 5.1. Different strategic approaches by country....21
6. Legal and regulatory issues....23
   - 6.1. Security....24
   - 6.2. Cloud-based quantum computing....24
7. Conclusion....24

1. Introduction

The first quantum revolution, driven by the discovery of wave-particle duality and an understanding of the structure of matter at a microscopic scale, paved the way for major innovations including semiconductors, transistors, lasers and GPS technologies. These advances laid the technological foundations of modern telecommunications by enabling the miniaturisation of electronic components, enhancing transmission systems and fostering the development of fibre-optic communications [1].

Today, this scientific foundation is giving rise to a new phase, namely the second quantum revolution, which seeks to harness the unique behaviour of particles[1] at the atomic and subatomic levels in order to develop new technological paradigms able to transform strategic sectors. These technologies are currently divided into three complementary categories. The first is **quantum computing**, which leverages the principles of quantum mechanics to perform complex calculations that are difficult, or even impossible, for current classical computers to solve. The second category encompasses **quantum communications**, aimed at interconnecting quantum devices to enable the secure transmission and sharing of information, thereby opening the path towards a "quantum internet". The third category comprises **quantum sensors and detectors**, capable of measuring physical quantities with unprecedented levels of precision and sensitivity. These can detect minute changes in physical parameters beyond the capabilities of conventional sensors. In addition, one of the key **implications** of progress in quantum computing and quantum communications relates to **post-quantum security**, which aims to develop new cryptographic systems that are resistant to future quantum-computer attacks in order to safeguard sensitive data and communications.

The new era of quantum technologies now raises a major question: will this second revolution simply improve existing networks – for example, by enhancing the security and performance of communications – or will it lead to entirely new forms of telecommunications based on quantum networks?

This briefing note sets out to explore the transition of quantum technologies from the sphere of research into industry. It provides an overview of academic and industrial progress in the development of quantum computers and associated solutions, while also considering the likely stages and timescales of this transition. In parallel, the note examines the potential applications of quantum technologies within digital infrastructures, by analysing possible transformations in network architecture and performance, as well as the ways in which classical and quantum computing systems may coexist.

It should be noted that quantum sensors, which currently represent the most mature applications of quantum technologies,[2] remain relatively independent from the two other domains (quantum computing and quantum communications, including cryptography), as well as from broader questions concerning the future evolution of digital infrastructures. For this reason, quantum sensing applications are excluded from the scope of this note.

The note is therefore structured around four complementary themes. The first section introduces quantum computers and their potential, providing an overall roadmap and describing the major technical challenges involved. The second section analyses the potential threats these technologies

[1] The main quantum properties of particles exploited by these technologies include wave-particle duality, the uncertainty principle, superposition, entanglement, the no-cloning theorem and quantum tunnelling

[2] Atomic clocks, gravimeters, magnetometers, electrometers and photon detectors

pose to digital security, the solutions currently being developed in response, and the implications for mobile networks. The third section focuses on quantum networks and the strategic role of digital infrastructures in enabling their emergence and deployment. Lastly, the fourth section analyses the strategies adopted by industrial stakeholders and the public policies designed both to anticipate risks and to accelerate the development of quantum technologies.

2. Quantum computing

2.1. How quantum computers operate

Quantum computing is primarily based on two core phenomena of quantum physics, namely state superposition and entanglement:

- **Superposition** describes the capacity of a quantum system to exist simultaneously in several states. As a result, the fundamental unit of quantum information, known as the qubit, can exist in state 0, state 1, or a superposition of both states [2].
- **Entanglement** enables qubits to be interconnected regardless of the distance separating them. According to Alain Aspect, entanglement occurs when two particles that have interacted in the past and later become spatially separated form an inseparable quantum whole containing more information than the sum of the information carried by each individual particle [3].

As with conventional computers, quantum computers comprise both hardware and software components.

The QPU,[3] which forms the core of a quantum computer, combines quantum bits (qubits), control electronics and classical computing hardware. The classical hardware is notably responsible for storing and executing instructions, managing and amplifying input/output signals, and processing data in order to distinguish useful signals from noise [4]. **Physical qubits** can be implemented through a range of approaches adapted to specific tasks, based on the manipulation and measurement of systems displaying quantum behaviour, such as superconducting circuits, photons, electrons, trapped ions and atoms [5]. Unlike classical bits, which are limited to the values 0 or 1, qubits are not restricted to a single binary state thanks to the principle of **superposition**.

In addition, cooling systems may be required for certain qubit technologies, alongside a classical computer responsible for controlling the overall system.

The software layer acts as the interface between users or algorithms and the quantum hardware. It comprises a software stack, including quantum programming languages, libraries, compilers and the simulation tools necessary for the development, compilation, optimisation and execution of quantum algorithms. A quantum algorithm breaks a problem down into a sequence of elementary operations applied to a quantum memory composed of qubits. These operations, known as quantum gates, are assembled into quantum circuits that manipulate quantum states (superposition and **entanglement**) in order to generate a result during the final measurement process [6].

[3] Quantum Processing Unit

2.2. The potential of quantum computers

The properties of superposition and entanglement provide quantum computers with the potential to surpass the limits of classical computing by enabling exponential increases in computational power and parallel computing. The gains in terms of acceleration vary according to the algorithm, as well as the type and scale of the problem considered. For instance, Peter Shor's[4] integer factorisation algorithm [7] could exponentially accelerate computing, while Lov Grover's search algorithm for unstructured databases [8] offers a quadratic improvement in performance.

Quantum advantage

Since there is currently no universally standardised metric for assessing the performance of quantum computers, the notion of **quantum advantage** is used as a benchmark. This describes the **actual** ability of quantum computers to perform **useful** calculations that exceed the capabilities of supercomputers, based on measurable criteria such as computation time, resource requirements and accuracy. IBM[5] and Pasqal[6] emphasise that this advantage requires not only a demonstrated improvement over classical approaches, but also the production of correct and verifiable results. Quantum advantage should not be understood merely as a single breakthrough moment tied to one isolated problem, but rather as a gradual process based on increasingly convincing application-driven demonstrations, ultimately validated by the scientific community.

Several stages of technological maturity therefore appear necessary in order to consolidate this quantum advantage in the development of quantum computers.

Noisy Intermediate-Scale Quantum (NISQ)

The concept of **NISQ**, proposed by John Preskill, describes an intermediate stage in the evolution of quantum computing marked by the emergence of processors containing from several tens to several hundreds of physical qubits [9]. This generation constitutes a significant milestone as it progressively surpasses the simulation capabilities of classical supercomputers, although it remains strongly affected by noise and errors [2]. NISQ systems should therefore be viewed as a transitional phase towards fault-tolerant quantum computing, providing an experimental environment in which new algorithms, architectures and control systems can be explored in preparation for practical, robust and scalable quantum advantage.

Fault-Tolerant Quantum Computing (FTQC)

The concept of FTQC, which represents a more advanced stage of technological maturity, describes quantum computers capable of carrying out reliable and prolonged computations by correcting the intrinsic errors associated with qubits through the use of error-correction codes and robust architectures.

---

[4] According to the definition provided by the French Academy of Technologies, this refers to a quantum integer factorisation algorithm invented by Peter Shor in 1994. In theory, it could break RSA public-key encryption by decomposing large numbers into their prime factors [6].

[5] https://www.ibm.com/quantum/blog/quantum-advantage-tracker

[6] The Race to Quantum Advantage - Pasqal: https://www.pasqal.com/fr/quantum-advantage/

Widely accepted theoretical analyses suggest that a fault-tolerant quantum computer could deliver a decisive **quantum advantage** for **specific classes of problems**. In other words, tasks that would require exponential computation time on classical systems could become achievable within a reasonable timeframe on such quantum computers, while requiring fewer computational resources (reduced computation time and fewer operations). For other categories of problems, improvements could theoretically be achieved, although these appear more limited when compared with the best currently known classical algorithms [6].

2.3. Quantum computing applications

High-performance computing (HPC) refers to a field of computing based on specialised systems designed to solve complex problems requiring substantial computational resources [10].

Quantum computing is considered strategically important in many sectors where high-performance computing, partial differential equation solving, function optimisation, machine learning and predictive analytics play a decisive role.

These computational methods are primarily used in fundamental and applied research and could benefit an increasing number of industrial sectors by accelerating innovation and shortening product design, validation and time-to-market cycles. Depending on the type of problem considered, a number of sectors could derive significant advantages [11] [12]:

- **Cybersecurity and cryptography:** integer factorisation, secure key generation, cryptographic protocol analysis.
- **Defence and security:** simulation of complex systems and strategic optimisation.
- **Medicine and pharmaceuticals:** molecular modelling, chemical-reaction simulation, drug discovery.
- **Finance:** portfolio optimisation, risk management, financial market modelling.
- **Materials science and chemistry**: development of new materials, quantum simulations of molecules and chemical reactions.
- **Transport and logistics:** route and supply-chain optimisation, complex planning operations.

NISQ computers are already capable of addressing certain practical use cases, particularly when the objective is to explore specific problems without requiring perfect accuracy. This is the case, for example, in some quantum-system simulations in chemistry and materials science, as well as in fields where hybrid methods combining classical and quantum computing can deliver usable outcomes despite the presence of noise [9].

Conversely, applications demanding high reliability and fully accurate results, such as cryptanalysis using Shor's algorithm or high-precision industrial chemical simulations, will require the development of fault-tolerant quantum computers [12, 11]. As such, NISQ systems are suited to exploratory applications, prototyping and approximate optimisation, whereas FTQC is the key prerequisite for enabling large-scale cryptographic and high-impact industrial quantum applications.

In the future, these applications are expected to benefit companies of all sizes. However, at the current stage of technological development, and given the specialised expertise required, the earliest adopters of quantum computing are primarily large corporations and research institutes.

2.4. Challenges and future prospects for quantum computing

Numerous technical challenges still need to be overcome before fault-tolerant quantum computers can become a reality. Some of these challenges are linked to the phenomenon of decoherence,[7] which results from the extreme sensitivity of qubits to external disturbances such as temperature fluctuations, vibrations, acoustic waves and electromagnetic noise. This sensitivity leads to errors and reduces computational stability. In addition, the scaling-up of systems (increasing the number of qubits while maintaining their reliability) represents a major obstacle.

Beyond error correction and scalability, many other challenges remain to be addressed, notably the improvement of quantum memories, which will be necessary to enable the execution of more ambitious algorithms.

Error correction

Reducing error rates remains a major challenge for all quantum computers, regardless of the underlying technology. Errors mainly result from qubit instability and decoherence, the process by which quantum information is lost through interactions with the environment.

One of the main approaches to quantum error correction involves combining a large number of physical qubits to create a logical qubit that is more reliable and less prone to errors. The number of physical qubits needed to obtain a logical qubit depends mainly on qubit quality and the error-correction used; it can reach several thousand, or even more.

It is also necessary to improve the isolation of qubits from their environment to minimise error sources. Achieving this will demand substantial hardware advances in the design and manufacture of quantum computing components. Most quantum computers, regardless of the technology used, must operate at temperatures close to absolute zero. Photonic systems are a notable exception, as only their detectors require cryogenic cooling. These requirements result in complex and expensive infrastructure.

Finally, imperfections in control systems can also introduce further errors. This fact highlights one of the fundamental paradoxes of quantum computing: qubits must be sufficiently isolated to preserve their coherence, while remaining sufficiently controllable to enable reliable quantum operations.

At present, the most advanced quantum computers are the NISQ computers presented in Section 2.2. They experience an error every 100 to 1,000 operations and have a limited number of qubits. These machines use noise-tolerant or low-depth quantum algorithms, often combined with classical computing resources in hybrid architectures. In addition, to mitigate errors, these machines rely on statistical methods to process quantum results.

Scaling up

Challenges associated with the scalability of quantum computers are significant: it is necessary not only to increase the number of qubits successfully, but also to ensure that the theoretical acceleration provided by quantum algorithms remains significant when considering the entire computational

[7] Decoherence is the process through which a quantum system loses its quantum properties such as the superposition of states

process. More broadly, a key challenge lies in being able to control and operate large numbers of entangled quantum systems with the precision and reliability required for real-world industrial applications [13].

According to a report published by the OECD and the European Patent Office (EPO) in December 2025 [14], the quantum technology sector is evolving rapidly but is now confronting the challenges of scaling up and commercialising technologies. The industry may be entering a new stage of development, where the initial period of rapid growth gives way to more targeted development and technological maturation.

Economic challenges

The challenges associated with the development of quantum computing extend beyond technical issues and encompass economic and strategic considerations. It is difficult to currently assess the economic viability of quantum computers because the technology is still in its infancy and production volumes are limited, resulting in very high development and manufacturing costs. There is also significant uncertainty over whether large-scale, fully operational quantum computers can ultimately be built.

The successful large-scale deployment of quantum technologies will depend on a range of factors, including investment, the development of necessary skills and the resilience of supply chains.

2.5. Global roadmap

A roadmap can be defined to broadly identify the progress required to move from NISQ capabilities towards the ambitions of FTQC. As illustrated in Figure 1, this roadmap is primarily structured around two objectives: increasing the number of qubits and improving fault tolerance through quantum error correction. Accordingly, it is estimated that at least 10,000 logical qubits will be required for FTQC algorithms to address industrial-scale problems.

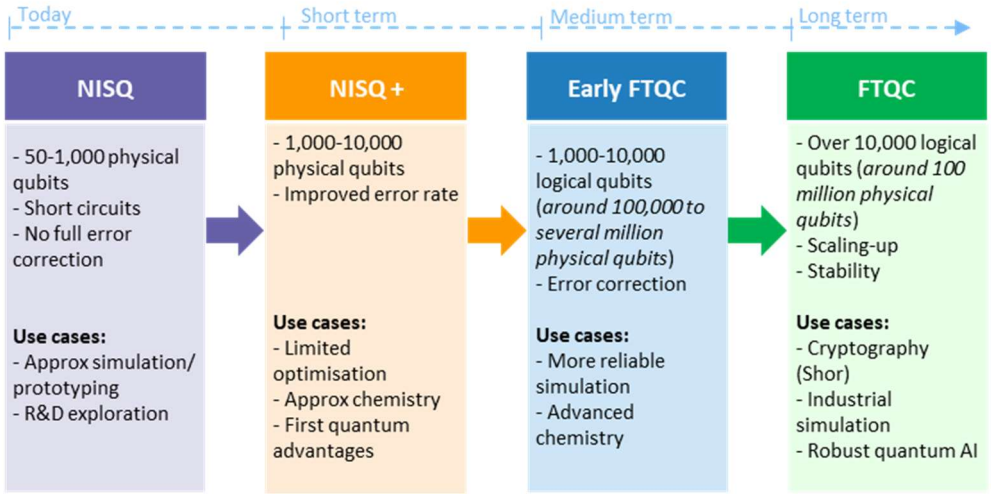

Figure 1: Roadmap towards FTQC. Source [9].

French start-ups Pasqal, C12, Alice & Bob, Quandela and Quobly, alongside major technology companies such as IBM, Google, Microsoft and Amazon, are conducting research and development activities aimed at building quantum computers capable of outperforming classical machines.

Most of these stakeholders have published roadmaps setting out their ambition to progressively increase the computing capacity of their machines until fault-tolerant quantum computing is achieved. Some provide timelines for their key milestones, while others choose not to disclose their projections. **In all cases, there is growing convergence around the emergence of FTQC by approximately 2030, followed by large-scale deployment around 2035.**

2.6. Artificial intelligence and quantum computing: synergies and hybridisation challenges

Competing approaches to complexity

As discussed earlier in this note, one of the main attractions of quantum computing is its potential to solve computational problems that exceed the capabilities of classical computing. To date, these problems have been addressed using supercomputers.

The rapid development of artificial intelligence has led to major advances in research and industry, enabling increasingly complex problems to be addressed while delivering significant gains in efficiency, performance and innovation. As a result, there is currently, and likely even more so in the future, strong complementarity and synergies between classical computing architectures (CPUs), graphics processing units (GPUs) and quantum processing units (QPUs).

According to the Academy of Technologies report, the development of artificial intelligence could also represent a form of competition for quantum computing. Advances in AI models, combined with improvements in processors such as GPUs equipped for vector and matrix operations, together with the emergence of NPUs,[8] provide powerful tools capable of solving a wide range of problems through statistical methods. These advances could therefore make it possible to solve certain calculations that were initially considered to fall exclusively within the scope of quantum computing.

AI–quantum synergies

Most stakeholders in the sector view quantum computing and artificial intelligence as complementary technologies and see significant opportunities in their combination. Quantum processors could optimise data input stages and accelerate model training by leveraging superposition and quantum parallelism, thereby enabling more efficient exploration of parameter spaces and faster performance optimisation. This approach could reduce the number of training iterations required and improve solution exploration [15]. Quantum machine learning algorithms already exist and, for certain use cases, may offer greater efficiency and lower costs than their classical counterparts.

In practice, many use cases involve a combination of problem types, some of which may be handled more efficiently by a quantum processor, while others remain better suited to classical HPC systems.

[8] Neural processing units

In this context, a hybrid approach that distributes tasks between classical and quantum computing appears particularly promising. Industry stakeholders are already working to enable seamless integration between these two types of computing.

For some major cloud service providers that are developing both AI models and quantum processors, AI could therefore play a key role in integrating quantum and classical computing by enabling seamless interaction between classical and quantum computers through cloud computing. Standardisation is expected to play a key role in ensuring interoperability between technologies and facilitating the development of hybrid ecosystems. In Europe, CEN/CENELEC has established a working group to examine these issues. The future of computing is likely to involve breaking problems down into individual tasks and assigning them to the most suitable computing resource, whether a CPU, GPU or QPU. Future computing architectures will therefore be designed by drawing on the different technological building blocks available according to the nature of the problems to be solved.

It is also worth noting that the relationship between classical and quantum computing extends beyond future hybrid approaches to solving complex problems. Artificial intelligence, which today relies primarily on classical computing, plays an important role in research enabling advances in quantum computing. AI can be used at all stages of quantum computer development,[9] from initial design through to physical system control and the implementation of error-correction techniques.

2.7. Cloud-based quantum computing and the first computations

Quantum computers are very expensive and investment remains risky. As mentioned earlier, in order to perform well, quantum computers must be highly stable and require significant isolation from the outside environment. This is why they are mainly installed in large, cloud-connected computing centres with the necessary infrastructure. These cloud computing platforms can provide the quantum processing power needed to develop algorithms, preliminary simulations and complex computations and models based on quantum technology. By harnessing the quantum expertise of cloud platforms, the need for in-house skills and expertise to access quantum computers is reduced.

Access to cloud-based quantum computers is provided by a large number of operators in the market, including the leading cloud computing companies such as Amazon, Google, Microsoft and IBM, as well as OVH and Scaleway in France. These companies offer quantum services using processing power which remains limited. The first solutions made it possible to test quantum computing using emulators and quantum computers with limited power known as NISQ computers.

Quantum computers do not aim to replace traditional computers. They are used in highly specific situations, often in combination with traditional computing.

Although the economic models which could emerge with the rise of quantum computer remain unclear, several avenues are emerging. These include:

- the commercialisation of quantum computers aimed at users with high data security requirements and the financial means and infrastructure needed to host a machine;

[9] For example, the AlphaQubit decoder, based on AI, identifies quantum computing errors with cutting-edge precision, and the AlphaTensor-Quantum method, based on deep reinforcement learning, aims to optimise logical quantum circuits in order to execute them more efficiently, i.e. with fewer operations

- the availability of computing power through quantum data centres. This is a more accessible solution aimed at the majority of users who want access to quantum computing but who are not in a position to own a quantum computer.

2.8. Quantum computing and the needs of the telecoms sector

In addition to applications in the field of cryptography, which are addressed in more detail in the following chapter, the electronic communications sector could potentially benefit from the computing power of quantum computers for specific problems requiring high computational intensity, such as network optimisation and the allocation of resources and signal processing. These issues currently involve the use of traditional algorithms, often based on heuristics or approximation methods, which can produce satisfactory solutions but which may prove to be sub-optimal as networks becoming increasingly complex.

Deployment optimisation and network management

The deployment and operation of mobile and fixed electronic communications networks involve multiple complex optimisation calculations, whether this be in terms of configuring the routing of network data flows, positioning antenna for mobile networks or rolling-out fibre optic networks. As uses develop, the density of data to be processed and the number of connected devices may continue to grow, requiring increasingly complex optimisation calculations which could call for quantum computing [16, 17].

Radio resource allocation in mobile networks

Quantum computing may contribute towards helping resolve the notoriously difficult combinatorial problems of optimising spectrum usage. Areas that could benefit include planning and allocating radio channels, minimising interference and dynamic spectrum sharing. Quantum optimisation would be particularly useful in complex or congested environments where resource optimisation is key and where there is significant complexity.

Signal processing in mobile networks

Quantum computing and algorithms may also contribute to facilitating the design of systems that reliably and efficiently process signals at the physical layer of electronic communications. These tasks are computationally intensive and often involve compromises between performance and complexity. Progress in the design of equipment and the software used to process signals could improve performance and contribute towards optimising the coverage and quality of mobile services.

Potential applications remain very much at the exploratory stage

Work aiming to improve the performance and efficiency of networks to enable a better use of resources (radio sites, frequencies, energy) in response to greater demand while increasing the flow and reducing communication latency is being carried out by academic and private research teams [18, 17, 16]. Vodafone, for example, has been working with ORCA Computing, which is developing a photonic quantum computer, to optimise the design, planning and deployment of its mobile and fixed networks. The operator hopes to optimise fibre optic cable routing, reduce the total length of the fibres needed and optimise the position of mobile base stations, thus reducing the amount of civil engineering work required. Ultimately, Vodafone also wants to use quantum computing to model its international infrastructures such as underwater cables and “direct-to-device” satellite services [19].

According to those we interviewed, the telecoms sector does not appear to be an immediate priority for algorithmic research in quantum computing. Others believe that quantum computers will only provide real added value to telecoms networks when they become both scalable and fault tolerant.

Initially, operations could access quantum power through cloud-based computing centres to resolve optimisation problems, using a hybrid approach combining traditional and quantum computing.

In the long term, with a fully functional fault-tolerant quantum computer (FTQC), more complex optimisation problems in the telecoms network could potentially be resolved, such as dynamically adjusting data flow routing, a task which currently remains beyond the scope of traditional computers.

However, the quantum advantage remains difficult to measure and must be viewed in light of the effectiveness of existing classical heuristics, which already provide an adequate response to the majority of common use cases.

3. Quantum computers: a threat or a revolution for communication security?

The emergence of quantum computing represents a major issue for communication security. A sufficiently powerful quantum computer capable of using Shor's algorithm [7] or Grover's algorithm [20] could break traditional cryptography systems [21], such as RSA [22], which are very widely used and, consequently, could infringe upon the confidentiality of communications and the stored information upon which they depend.

The threat horizon is difficult to estimate. It is estimated that it would take eight hours to break RSA-2048 with around 20 million physical qubits [23] or one week with one million physical qubits [24].

Security protocols, particularly those used in electronic communications, are designed to be used for long periods of time and generally involve mechanisms enabling the key size to be increased or parameters to be adjusted as the security level reduces. However, the quantum threat could impose more far-reaching changes not only involving increasing the key size but potentially replacing primitive cryptography entirely and adapting the protocols to support them [26].

Two main approaches are emerging in response to this risk:

- The physical approach with **quantum key distribution (QKD)**, which can generate and distribute symmetrical cryptographic keys using dedicated quantum channels (fibre optic or satellite). This approach is based on the principles of the theory of quantum information in order to guarantee theoretical information security during key generation.
- The algorithmic approach using **post-quantum cryptography**, based on new mathematical paradigms which are supposedly resistant to quantum attacks (such as those based on Euclidean networks).

Against this backdrop, the French National Agency for the Security of Information Systems (ANSSI) now encourages all companies to incorporate the quantum threat into their risk analysis and to envisage adopting post-quantum cryptography (PQC) to secure relevant cryptographic products [25].

3.1. Quantum threats for telecoms markets

Store now, decrypt later

The emergence of quantum computing capacities which could compromise asymmetric cryptographic algorithms brings with it a major risk of delayed compromise of the confidentiality of electronic communications. Malicious actors could attempt to intercept and store data flows or protected data now in order to decrypt them later when the relevant quantum capacities are available.

This scenario significantly modifies the measurement of risk over time. Communications which are considered as secure today could be exploitable tomorrow, despite the fact that the data in question should remain confidential for long periods of time [27].

When it comes to securing exchanges through telecommunications networks, the data and exchanges protected by TLS[10]/IPSec[11] [28] and by the mechanism of certificates (such as itinerant interfaces), including subscriber data, authentication credentials, private keys and certificate chains, could be exposed to such a threat [29, 30].

The erosion of confidence-building mechanisms

ANSSI has stressed an acute risk of the falsification of signatures and identity theft, which would affect the authentication and integrity of exchanges when such signatures are required (with subtleties depending on the use case and the requirement for long-term validity of signatures [29].

When it comes to mobile telephone networks, this risk concerns the use of X.509 certificates[12] [28], certificate chains and private keys in mutual authentication and the integrity/authentication of certain exchanges (such as between itinerant partners), insofar as the use of a cryptanalytic quantum computer on these components could enable identity theft and falsification/tampering[13] [31].

Hybrid threats and transition risks in complex environments

Quantum threats not only arise in the form of attacks based exclusively on the use of quantum computing. They can also arise in hybrid scenarios, which combine traditional attack techniques with the gradual weakening of cryptographic mechanisms.

Traditional vulnerabilities could thus be exploited alongside a breakdown in cryptographic trust, increasing the probability of complex attacks and ripple effects, for example through the compression of update chains, ID systems or supply chain dependencies.

3.2. Responses to quantum threats

Post-quantum cryptography

[10] TLS (Transport Layer Security) is one of the most widespread network flow protection solutions

[11] IPsec is a secure communication protocol suite which protects network flows

[12] International Telecoms Union (ITU) standard X.509, which defines the format of public key infrastructure (PKI) certificates

[13] “Data tampering” refers to the unauthorised modification, erasure or manipulation of data

Post-quantum cryptography (PQC) covers algorithms designed to remain safe against attacks using quantum computing power. In contrast to traditional schemes such as RSA or ECC, the security of which is based on factorisation or the discrete logarithm, PQC algorithms use mathematical problems for which no effective quantum algorithm is currently known. This design makes them resistant to known quantum attacks, because the accelerations that current quantum algorithms (Shor, Grover) provide cannot effectively break these problems under their recommended parameters.

In the United States, the National Institute of Standards and Technology (NIST) has already normalised post-quantum public key encryption algorithms such as ML-KEM which is used to exchange keys [32]. These advances do not involve any major material change for computing infrastructures and traditional telecoms, although they may require greater software resources.

However, the integration of PQC into existing protocols is complex, involving the integration of new algorithms, modifications to protocols such as TLS or SSH and the adaptation of software stacks, which are likely to introduce new vulnerabilities.

Within 3GPP, reflections on the transition towards PQC as part of the latest 5G evolutions (Releases 19-20) are under way, mainly in the form of technical studies and impact analyses. At this stage, work has not yet been translated into compulsory normative integration within the existing 5G specifications, in contrast to preliminary discussions on Release 21, associated with the first specifications for 6G. The normative integration of security mechanisms which are resistant to quantum threats, notably PQC, is principally envisaged in the context of Release 21 and the specifications associated with 6G which will be natively “quantum safe”.

Quantum Key Distribution

QKD is a technique which enables the generation of a symmetrical key between two parties using the physical properties of quantum mechanics, notably the fact that any measurement of a quantum state disrupts that state and can, therefore, be detected. In practice, it depends on two distinct channels:

- A dedicated quantum channel (fibre optic or free space optics) to transmit the quantum states which enable the key to be encoded,
- A traditional channel authenticated for signal exchanges, error correction and integrity verification.

QKD does not itself quantify the data, it only distributes the symmetrical keys which are then used by traditional algorithms (such as AES). It is, therefore, a key distribution mechanism and not an end-to-end quantification solution. According to the position shared by many European cybersecurity agencies, QKD remains at a pre-operational stage [33]. It requires dedicated physical infrastructures, which are costly and difficult to roll-out, presents significant constraints in terms of distance and optical attenuation, and depends on material components which are still not widely standardised. Moreover, it does not eliminate the need for traditional cryptographic mechanisms for data authentication and protection [33]. Consequently, QKD can only currently be envisaged for very specific point-to-point connections in controlled environments and is not a generic solution for security large-scale communications, in contrast to software-based PQC.

Hybrid solutions

Faced with the threat that quantum computing poses to current encryption mechanisms, hybridisation consist of combining several security mechanisms based on different mechanisms to avoid being

dependent on any single one. The objective is to strengthen the overall robustness of communications, to limit the risks linked to computing capacities and to enable a controlled transition to post-quantum security. By taking a hybrid approach, keys emerging from several mechanisms are combined to produce a unique final key, guaranteeing that security is preserved as long as any one of the underlying mechanisms remains secure.

The combination of traditional cryptographic mechanisms with post-quantum algorithms is the first step in hybridisation. When a secure communication is established, traditional tried-and-tested algorithms are used in combination with algorithms which are resistant to quantum computing to negotiate the encryption keys. This approach increases protection against future threats.

In contrast, integrating PQC into existing protocols increases software complexity and requires particularly attention to be paid to the quality and maturity of implementation, in order to avoid the introduction of new vulnerabilities. For example, working groups are currently studying the hybridisation of known protocols such as TLS with post-quantum methods such as ML-KEM. The first feedback from this IETF research indicates that this hybridisation has an impact on the size of the public keys communicated and can lead to a duplication of shared keys and to a non-negligible possibility of failure during the handshake.[14]

More advanced hybridisation could consist of combining traditional mechanisms, post-quantum mechanisms and the quantum distribution of keys [34]. In this case, key exchanges would be carried out on the traditional network using traditional and post-quantum algorithms such as a quantum channel which can generate additional keys with physical security guarantees. This approach makes it possible to diversify cryptographic methods based on different mathematical hypotheses (traditional and PQC), as well as mechanisms based on the laws of physics using QKD. The keys from these various sources are then combined to produce a unique final key. It does, however, involve significant complexity in terms of integration, exploitation and cost, which means it is reserved for the most sensitive uses.

ANSSI and the European[15] and US standards bodies recommend preparing for the migration of telecoms networks' security protocols, particularly Public Key Interfaces (PKIs), towards hybrid solutions combining traditional cryptography and PQC in a structured way. This involves the uses of public key cryptography (including updating software and third products), planning for gradual migration and taking into account the supplier/partner chain [29] [35] [36]. The GSMA guidelines highlight the practical constraints of deployment in the networks (existing infrastructures, supplier dependency, support for third-party tools and the need for interoperability tests on multi-vendor products when new mechanisms and protocols are introduced) [31].

4. Quantum networks

Quantum networks or the quantum internet provide the infrastructure and communication protocols required to interconnect distributed quantum systems [37] enabling the communication of quantum bits. These networks work on principles similar to traditional networks but use totally different physical

[14] An automatic negotiation process which establishes the parameters of communication between two entities before communication begins

[15] ETSI : European Telecommunications Standards Institute

mechanisms, based on the laws of quantum mechanics, particularly the entanglement and superposition of quantum states.

In contrast to traditional networks, quantum networks initially only respond to highly specific use cases, targeting niche applications with high added value in fields such as scientific research, defence, cybersecurity and finance [37]:

- **Improving communication security**: quantum networks could establish quantum cryptographic systems such as the distribution of quantum keys (QKD) presented in Section 3.2.
- **Multiplying computing power:** the deployment of network-connected quantum computing nodes could make it possible to construct a distributed computing system which is much more powerful than any single device. This type of network could share quantum data between distant nodes, essential to coordinating complex distributed computations and encouraging the emergence of distributed quantum computations. Problems requiring millions of qubits would be difficult to resolve using a single quantum computer, while the use of a modular infrastructure connecting several processors could be a more viable approach in the short term.
- **Transmitting information from advanced quantum sensors** to enable the lossless transmission of ultra-precise measurements generated by quantum sensors (for example, for the synchronisation of atomic clocks) towards quantum computing centres. Quantum networks would also make it possible to preserve quantum correlations between several distant sensors, opening the way to even more precise interferometry or distributed detection.

The first prototypes aim to integrate quantum networks into traditional networks, based on existing infrastructures, particularly fibre optic networks and satellite connections. Several studies and experiments show that quantum technologies, particularly QKD, can co-exist with traditional signals in the same existing fibre optic cables, which would allow a large part of the existing telecoms infrastructure to be reused. In practical terms, this often involves the use of multiplexing and filters to reduce interference between quantum signals and traditional signals [38] [39].

Satellites represent another major possibility for upscaling quantum networks. Current projects envisage that satellites could distribute entangled photons or quantum keys between different terrestrial stations, making it possible to interconnect quantum networks spread over large distances or between continents.

It should be noted that the capacity of a quantum network to transmit information will remain limited, as its primary function is to carry quantum states associated with data transmission, while the data itself continues to travel via the traditional network. Thus, much as quantum computers do not aim to replace traditional computers, quantum networks will not replace existing infrastructures but will complement them.

4.1. Technological challenges

The construction of quantum networks, while still at an embryonic stage, appears to be complicated given the technical limitations principally linked to the difficulty of quantum measurement and the particular fragility of entanglement [37].

Long distance transmission

One of the main barriers concerns the transmission of quantum bits over long distances. The physical properties of quantum information, in particular entanglement, are extremely sensitive to disruptions

and degrade rapidly during propagation in environments such as fibre optics. This fragility leads to a gradual loss of coherence, making reliable distribution of quantum states difficult over long distances without specific mechanisms.

The use of traditional repeaters and amplifiers to restore and strengthen the signal is impossible in quantum mechanics due to the non-cloning theorem, which prohibits the perfect copying of a quantum state without destroying it. Quantum repeaters are being developed to overcome this obstacle. These are quantum mechanisms which are based on the creation of entangled states on short segments and entanglement swapping[16] making it possible to progressively extend correlations over long distances, without cloning or directly quantifying the quantum state being transmitted. These mechanisms can thus make it possible to overcome the limits of a single direct connection. Their design, however, remains complex and costly, notably because it requires the integration of reliable quantum memories.

The French national quantum strategy has identified the French startup Welinq, which emerged from pioneering work carried out by the French National Centre for Scientific Research **(**CNRS) and Sorbonne University, as having significant potential to lift this technological barrier, as a result of the solutions that it has developed.

A complementary solution would be to incorporate satellite-based quantum communications, which benefit from much more reliable attenuations in free space than terrestrial fibre optics. The use of satellites in low Earth orbit has already made it possible to distribute pairs of entangled protons over distances exceeding several hundreds of kilometres. However, this type of solution also presents challenges, particularly the short duration of visibility between a satellite and terrestrial stations, atmospheric states and the need for a constellation of satellites to ensure continuous coverage [40].

Collaboration currently under way between Welinq, Qphox and the Sorbonne University Meet-Q project aims to integrate quantum processors and optical quantum network technologies. The aim of this project is to make it possible to connect quantum processors to quantum storage technologies and quantum repeaters, which are essential for the interconnection and transmission of quantum information. Advances in this field could open the way for the development of quantum data centres, capable of carrying out rapid, reliable and large-scale computations. This collaboration could, therefore, play a key role in the definition of essential technological interfaces and the development of quantum networks.

The scientific community has highlighted several other challenges:

- Cost and resource-efficiency: developing economically viable components while maintaining high performance is a major challenge for large-scale adoption;
- Interoperability: ensuring compatibility between different quantum technologies and between quantum networks and traditional networks. Using specific algorithms, it may be possible to develop hybrid interfaces ensuring the compatibility and interconnection between

[16] Entanglement swapping is a quantum operation which makes it possible to prolong the entanglement of two distant qubits using an intermediary qubit entangled with each of them.

traditional and quantum networks. Standardisation work could contribute towards ensuring compatibility as well as the definition of universal communication protocols.

The International Telecommunications Union Standardization Sector (ITU-T) has published a new standard, **Y.3800**, that lays a foundation for networks using **QKD**, crucial for securing quantum communications. The standard describes the **conceptual structures**, **basic functions** and architecture of QKD networks. The Y.3800 standard helps design, deploy and use QKD networks, but remains at **the base architecture stage**.

The European Telecommunications Standards Institute (ETSI) launched the Technical Committee on Quantum Technologies (TC QT) with over 90 participants. The initiative aims to advance standardised quantum technologies, particularly in product development, and contribute to a sustainable future globally by mapping the quantum ecosystem and creating a **Quantum Technologies Radar**.

In response to these challenges, quantum networks will be developed in stages [37]. Scientists propose a roadmap starting with the deployment of a pre-quantum network capable of sending qubits between two nodes and ending with a quantum network capable of offering distributed computing services. According to the researchers' estimated trajectory, the roadmap will include intermediate stages such as adding quantum memory and quantum repeaters [41]. The early version of quantum networks will be able to provide immediate benefits over classical systems such as communication security (and QKD) and ultra-precise synchronisation. The last-stage network will play a long-term role, particularly by connecting quantum processors together, thus enabling distributed quantum computing.

4.2. The role of digital infrastructures in the emergence of quantum networks

Development of the first terrestrial quantum networks that can fulfil QKD requirements should be able to use existing fibre-optic networks. Experimental deployment of quantum networks has shown that classical fibre-optics networks can transmit quantum data such as QKD keys.

Furthermore, the coexistence of classical and quantum links on the same fibre has advantages such as reduced infrastructure costs, simplified deployment and operational flexibility. This hybrid approach has piqued the interest of research teams. It has been shown that QKD can theoretically share a channel with classical communications [42]. Nevertheless, hybrid networks raise scalability issues. Quantum properties have very different design constraints compared to classical networks. According to some research, hybrid networks are an intermediate step towards a full quantum internet [43].

In contrast, classical telecommunications satellites do not appear to be intrinsically compatible with QKD, which would require specific satellites equipped with laser communication systems.

In partnership with some Member States and the European Space Agency, the European Commission is working on designing, developing and deploying a secure quantum network to cover the entire European Union including its overseas territories. The EuroQCI network will be part of IRIS^2 (the third EU flagship satellite constellation) and will consist of a terrestrial component using fibre-optic communication networks to link strategic sites on the European continent and a space-based component using satellites to produce a pan-European quantum communication infrastructure.

Industrial collaborations, such as those initiated by SpeQtral and Thales Alenia Space and those between SES and the European Space Agency (ESA), are already experimenting with satellite quantum communication through joint testing of orbit and ground stations.

Outside of France, experiments are underway to prove the feasibility of QKD on fibre optics. These experiments include the quantum network deployed by Cisco Systems and the Qunnect startup, which transmits signals through fibre-optic cables between Brooklyn and Manhattan in New York [44] as well as the first large-scale Chinese network covering 3,700 km, which can perform parallel communication between 20 users [45].

5. National and European quantum strategies

An international quantum technology race began several years ago. Quantum mechanics is considered to represent a major sovereignty issue due to its civil and military impacts. In this context, several countries have implemented national strategies and policies to develop their national ecosystems and stimulate developments in this fast-growing area. According to an OECD report published in December 2025[17], an estimated US$55.7 billion has been invested in quantum science and technology by governments, mainly of developed countries, since 2013. However, the OECD urges caution in interpreting these amounts because government announcements cite the total allocated budget for such programmes, which can include pre-existing or private funding. The global market for quantum technologies could reach US$106 billion by 2040, according to a 2023 report by McKinsey. In November 2025, 18 OECD Member countries and the European Union adopted official strategies to coordinate their already allocated funds, programmes and initiatives. Public funding seems essential given the lengthy and uncertain time spans for quantum technology development, which are major risks for private investors. This includes funding for public research, research and development support for private companies, the launch of public procurement contracts and equity. Strategies are coordinated by governments through one or more ministries with the support of public agencies specialised in implementing specific programmes.

These strategies usually involve international cooperation. However, international cooperation and collaboration are hampered by current geopolitical tensions, a focus on national security and strategic self-sufficiency, especially regarding dual-use applications, and restrictions on technology transfer. These security concerns could lead to more compartmentalised and closed national ecosystems, to the detriment of international scientific research. Yet such cooperation can help reduce duplication, increase the impact of public and private investments, benefit from economies of scale and create greater incentives to invest in research and development. These considerations could lead governments to find a balance between opening up their quantum technology ecosystems, which promotes collaboration and innovation, and the need to prevent abuse and misappropriation. According to the OECD, the quantum landscape is developing towards selective collaborations between trusted countries, as shown by the increasing number of bilateral agreements on quantum technologies, to the detriment of more global agreements. Even between partner countries, collaboration is faltering. For example, between 2018 and 2022, collaboration between the United States and EU Member States decreased in intensity by 15% in the area of quantum technology, reflecting a broader downward trend around the world.

17 https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/12/an-overview-of-national-strategies-and-policies-for-quantum-technologies_33a0b249/5e55e7ab-en.pdf

The constraints of supply chains for critical materials and components, the concentration of investments and technological protectionism can also exacerbate divisions between developing countries and developed countries, increasing the "quantum divide" [14].

5.1. Different strategic approaches by country

The strategies of China and the United States

According to some analysts, citing figures unsupported by official statistics, China has allocated public funds exceeding US$15 billion to compensate for the deficit in its private sector, which is less developed than that of the United States and, to a lesser extent, Europe[18]. For years China has been focussing on quantum communication, testing and deploying QKD communication networks. Of note, China has developed the world's longest quantum communication network between Beijing and Shanghai, a distance of 2,000 km, and in 2016 established the first satellite quantum link with Austria. Since then, the country has formed satellite links with South Africa and Russia.[19] The country is also investing in quantum computers,[20] with recent announcements of major progress in quantum computing using superconducting and photonic architectures.[21] The approach taken by China remains closed and national, with limited international collaborations through research publications and limited sharing of its developments, reflecting a strategic approach aiming to develop a competitive advantage in communications.

The United States appears to be one of the main funders of research into quantum computing. Generally, technological developments seem to be at a relatively exploratory stage, but with potential applications in many sectors, whereas China seems to be focussing on the more immediate applications of quantum communications. The US government's annual budget allocated to research and development has been around US$1 billion since 2022 and benefits major players such as IBM, which currently leads the field.[22] IBM developed its first quantum computer in 2019 and in 2023 it launched Condor, the world's first quantum processor to exceed 1,000 qubits. The company aims to develop a 100,000-qubit commercial quantum computer by 2033. In addition, US startups receive significant private investment. According to a 2023 McKinsey report, private investments in the US are the largest in the world, at over US$2.3 billion, more than five times investments in the EU (US$405 million). This situation results from the amount of available capital and an investment culture which is deeply attached to risk-taking for innovation.

Focus on the European strategy

The Quantum Europe Strategy, adopted by the European Commission in July [46], marks a key step towards positioning the EU as a global leader in the quantum sector by 2030. This initiative recognises that Europe excels in scientific research and has an active startup ecosystem but struggles to translate

[18] https://itif.org/publications/2024/09/09/how-innovative-is-china-in-quantum/

[19] https://thequantuminsider.com/2025/03/14/china-established-quantum-secure-communication-links-with-south-africa/

[20] The superconducting computer Tianyan-504, launched in December 2024, has a 504-qubit Xiaohong chip

[21] https://www.cullen-international.com/news/2026/05/Global-trends-in-quantum-technology.html

[22] The US quantum strategy, launched in 2018, aims to ensure continued US leadership. It comprises six policy areas: science, workforce, industry, infrastructure, economic security and international cooperation and includes several projects in the areas of communication, computers and sensors. It is supported by national defence legislation and the CHIPS and Science Act of 2022. It is coordinated by several federal agencies, including the National Institute of Standards and Technology, the National Science Foundation and the Department of Energy.

this potential into market opportunities **due to the fragmentation of initiatives and a lack of investment compared to the United States and China**

The strategy is based on five main areas: research and innovation, quantum infrastructures, strengthening the European quantum ecosystem, quantum technologies for space and defence and developing quantum skills. Its flagship measures include the creation of a research, technology and innovation programme to align the efforts of EU and Member States to support basic research and develop industrial applications, the implementation of a facility to design a quantum processor and **six quantum pilot lines, the launch of a pilot facility for the European Quantum Internet**, the expansion of quantum competence clusters[23] and the creation of a European Quantum Skills Academy. The strategy also plans to develop a Quantum Technology Roadmap in Space together with the ESA and will participate in a defence technology roadmap.

This strategy is complementary to the "Quantum Technologies Flagship" launched in 2018, a large-scale research initiative funded by the EU and other public agencies with a budget of €1 billion over ten years, bringing together research institutes and businesses. The project funds commercial projects in the three main areas of quantum technology (computing, communication and sensing) as well as basic research, training and international cooperation. Since 2021 the programme has published an annual report on the "23 Key Performance Indicators for Quantum Technologies in Europe" and their progress towards the goals set for 2030 in six areas: the ecosystem, quantum communication, quantum computing, quantum simulation, quantum sensing and metrology, and education.

In the area of quantum communication, the EuroQCI project mentioned in section **4** is one of the main pillars of the EU cybersecurity strategy, aiming to secure communications and data for critical infrastructures and government institutions. The Commission will rely on technological advances permitted by the Quantum Technologies Flagship. In this framework, national terrestrial projects have been funded with the aim of testing various technologies and protocols and adapting them to the specific needs of each country. Nationally, the France QCI project led by Orange will use existing infrastructures in the Paris and Nice regions to test quantum technologies, including QKD, and incorporate them into existing telecoms networks. A quantum network will also be established in Toulouse for the French Civil Aviation Authority.

Furthermore, the Commission aims to publish a "Quantum Act" in 2026, the main goal of which will be to support and encourage – through public and private investment – the sovereign and secure development of quantum technologies in the EU by promoting a unified ecosystem that is funded and coordinated at a European level.

Focus on French initiatives in the context of France 2030

The "France 2030" investment plan aims to make up for the lag in French industry, invest massively in innovative technology and support the green transition. In this context, quantum technologies have been identified as key to achieving the goals that have been set.

In 2021 France announced the launch of a national strategy for quantum technologies,[24] with a budget of €1.8 billion over four years, of which €1 billion is funded by the state. It has five strategic goals:

- Develop quantum technologies and the uses of quantum computing

[23] Quantum competence clusters are regional centres providing shared infrastructure and services while connecting stakeholders in research and industry. These centres are located in a few European regions including around Paris, Munich and Barcelona. The European Commission aims to invest in building new centres and strengthening the links between them.

[24] https://quantique.france2030.gouv.fr/

- Gain expertise in quantum sensing technologies
- Develop and distribute post-quantum cryptography
- Develop quantum communication technologies
- Gain expertise in quantum enabling technologies

According to the government, this strategy has led to a number of initiatives including the creation of around twenty startups, fundraising over €600 million, and an estimated 20% share of the global market in some segments.

Furthermore, in 2024 the Ministry of Armed Forces launched the Proqcima programme, in partnership with the French General Secretariat for Investment (SGPI). This programme aims to build at least two prototypes of French-designed universal quantum computers by 2032. With a budget of €500 million, the programme has signed framework agreements with five startups (Alice & Bob, C12, Pasqal, Quandela and Quobly) to identify and develop solutions to design such computers. Proqcima is an innovative partnership structured in the form of a phased competition between participants, leading to a gradual selection of the best-performing companies.

6. Legal and regulatory issues

The development of quantum computing raises major regulatory issues in terms of sovereignty, security and access.

6.1. Security

The question of cryptography standards that might be imposed or recommended could raise several issues, specifically those related to selection criteria for solutions, their adoption timetable, their modes of deployment and the potential risks of divergence between standards to be authorised and those preferred by private stakeholders. Furthermore, constraints caused by compliance with security standards could limit the breadth of technical solutions that companies can potentially consider, raising operational issues for companies.

As an example, the potential incompatibility between older communications standards and new post-quantum security requirements could influence the medium-term strategic decisions by telecoms companies to maintain or withdraw certain generations of networks. Some of the specifications currently being created, particularly for 6G, apparently already include native integration of “quantum-safe” security mechanisms. However, previous generations are based on classical cryptographic primitives, which could gradually lose their ability to comply with stronger cybersecurity requirements, thus accelerating their regulatory and economic obsolescence.

6.2. Cloud-based quantum computing

Access to the power of quantum computing via cloud computing services could raise major regulatory issues, particularly in terms of the sovereignty, competition and governance of strategic technologies, as highlighted by the OECD in its recent work on quantum technology policies [47]. The OECD draws attention to the risk of market concentration benefiting a limited number of dominant stakeholders, which can create a strategic dependency and intensify inequalities in accessing these advanced infrastructures. In addition, it emphasises the importance of standardisation and interoperability in order to prevent “vendor lock-in”, guaranteeing fair and open competition.

Finally, the use of delocalised platforms to access quantum computers via the cloud could also raise questions about digital sovereignty and data security, especially when processing occurs in regions outside users' jurisdictions.

In this context, the emergence of cloud services such as "Quantum as a Service" (QaaS), which enables remote access to quantum computing capacity via the cloud, could raise the question of whether it is necessary to adapt the regulatory framework (particularly the regulation of data processing services based on data regulations) for quantum computing, enabling equal access to and effective competition between quantum computing services.

7. Conclusion

The design and use of quantum computers is still in the research phase and many challenges remain before entering the industrial phase. In addition to the need to find an economic model for stakeholders, it will also be necessary to develop relevant algorithms for each use case, adapt the skills of engineers and experts in the private sector and research laboratories, allow companies to access computing centres with quantum computers and supercomputers and promote the development of supply and demand in France and Europe.

In the short term, the first uses of quantum computers will probably be in sectors other than telecommunications. Their high cost, complex infrastructures required and uncertainty about their immediate added value currently discourage stakeholders in the sector. Nonetheless, in the longer term, telecoms networks could access quantum computing resources via quantum cloud platforms, enabling some specialised processing to be performed externally for the design and configuration of network usage systems and equipment.

The most immediate issue for telecommunications is to anticipate the threats of quantum computers, which risk weakening the cryptographic schemes currently used in networks. Therefore, mobile infrastructures will need to gradually migrate to quantum-safe solutions that can withstand the threats of quantum technology by incorporating ANSSI recommendations, which encourage planning and preparing for this transition to ensure resilience in communication.

Telecommunications will play a key role in the deployment of future quantum infrastructures, particularly via hybrid networks that combine classical fibre optics and satellite channels. The first concrete application of quantum networks fills a need to secure communications; nevertheless, quantum networks around the world are still at the experimental stage and will be developed in stages, with each generation enabling the emergence of increasingly ambitious new applications, all the way to distributed quantum computing. This will involve a progressive development toward hybrid architectures that combine classical infrastructures and quantum links.

It is still too early to predict the exact extent to which quantum technologies will transform the telecoms sector. Changes could remain limited to strengthening and securing existing infrastructures or they could gradually open a pathway to new communication architectures and improved performance as systems and algorithms are developed. In any case, the road to these possibilities is bounded by experimental stages and technological challenges which will define the speed and nature of this revolution. The development of standards and the definition of a coherent national and European strategy will determine the direction these developments will take.

Additionally, national and European strategies will play a key role in accelerating the development of currently embryonic solutions. They will enable coordination of the various ecosystem stakeholders, promote links between solution providers and users and, most importantly, make essential funding available to guarantee stakeholders' economic sustainability until they reach sufficient technological

maturity. These initiatives are therefore of major strategic significance and contribute towards maintaining sovereignty in this area.

Finally, the development of a quantum computer using cloud computing infrastructures is likely to raise questions about infrastructure development and adjustment of security standards, namely for data stored in the cloud. In particular, the economic structure of access to cloud computing power and its interaction with the ecosystem of cloud stakeholders, could lead to a risk of dependence or circumvention of security and resilience requirements applying to cloud computing service providers.

Appendix I – Interviews

Interviews

A series of interviews formed the basis of our considerations on quantum technologies. Nevertheless, the positions we express in this note do not necessarily reflect the views of the individuals we met nor the institutions with which they are affiliated.

We interviewed the following:

- Google
- Welinq
- Pasqal
- Alice & Bob
- ANSSI
- CNRS/Sorbonne Université
- INRIA
- Nokia
- Ericsson
- Huawei
- Orange
- Microsoft
- OVH Cloud
- C12
- VeriQloud
- OCDE
- DGE
- Académie des Technologies
- Commission européenne (DG CNECT)

Appendix II – Key references

[1] T Ghose, "Science history: Invention of the transistor ushers in the computing era — Oct. 3, 1950," *LIVESCIENCE,* 2025.

[2] MA Nielsen, IL Chuang, "Quantum computation and quantum information," *Cambridge University Press,* 2010.

[3] A Aspect, "Si Einstein avait su", Odile Jacob, 2025.

[4] IBM, "QPU," [Online]. Available: https://www.ibm.com/fr-fr/think/topics/qpu.

[5] IBM, "Quantum Computing," [Online]. Available: https://www.ibm.com/fr-fr/think/topics/quantum-computing.

[6] Académie des Technologies, "État de l'art de l'ordinateur quantique tolérant aux fautes, questions et défis," 2025.

[7] PW Shor, "Algorithms for quantum computation: discrete logarithms and factoring," *Proceedings 35th annual symposium on foundations of computer science,* 1994.

[8] LK Grover, "A fast quantum mechanical algorithm for database search," *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing,* 1996.

[9] J Preskill, "Quantum Computing in the NISQ era and beyond," *Quantum*, vol. 2, 2018.

[10] GENCI, "Calcul haute performance, intelligence artificielle et calcul quantique," GENCI, [Online]. Available: https://www.genci.fr/connaitre-genci/calcul-haute-performance-intelligence-artificielle-et-calcul-quantique.

[11] V Raseena, "Quantum computing: foundations, algorithms, and emerging applications," *Frontiers in Quantum Science and Technology,* 2025.

[12] MA Nielsen, IL Chuang, "Quantum computation and quantum information," *Cambridge university press,* 2010.

[13] O Ezratty, "Understanding Quantum Technologies," 2024.

[14] OECD, "Mapping the global quantum ecosystem," 2025.

[15] H-Y Huang et al., "Quantum advantage in learning from experiments," *American Association for the Advancement of Science (AAAS),* 2022.

[16] F Phillipson, "Quantum computing in telecommunication—a survey," *Mathematics,* 2023.

[17] Ericsson, "Exploring the potential advantages of quantum computing in telecommunication networks," 2025.

[18] POSTQUANTUM, "Quantum Use Cases in Telecom," 2025 Fevrier 2025. [Online]. Available: https://postquantum.com/quantum-computing/use-cases-telecom/.

[19] Vodafone, "Vodafone partners with ORCA Computing to model future networks in minutes using quantum technology," 10 Juin 2025. [Online]. Available: https://www.vodafone.com/news/newsroom/technology/vodafone-partners-with-orca-computing-to-model-future-networks-in-minutes-using-quantum-technology.

[20] LK Grover, "Fast quantum mechanical algorithm for database search," *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing,* 1996.

[21] L Chen et al., "Report on post-quantum cryptography," *US Department of Commerce, National Institute of Standards and Technology,* 2016.

[22] RL Rivest, A Shamir & L Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM,* vol. 21, 1978.

[23] C Gidney C, M Ekerå, "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits," *Quantum,* 2021.
[24] C Chevignard, PA Fouque & A Schrottenloher, "Reducing the number of qubits in quantum factoring," *Annual International Cryptology Conference,* 2025.
[25] ANSSI, "Avis de l'ANSSI sur la migration vers la cryptographie post-quantique (Suivi 2023)", 2023.
[26] M Campagna et al., "Quantum Safe Cryptography and Security: An introduction, benefits, enablers and challenges," *European Telecommunications Standards Institute,* 2015.
[27] D Joseph et al., "Transitioning organizations to post-quantum cryptography," *Nature,* 2022.
[28] ETSI, "White Paper No. 8 - Quantum Safe Cryptography and Security," 2015.
[29] ANSSI, "Avis de l'ANSSI sur la migration vers la cryptographie post-quantique," 2022.
[30] GSMA, "Post Quantum Cryptography for 5G Roaming use case v1.0," 2024.
[31] GSMA, "PQ.03 Post Quantum Cryptography - Guidelines for Telecom Use Cases v2.0," 2024.
[32] NIST, "Module-Lattice-Based Key-Encapsulation Mechanism Standard, U.S. Department of Commerce," 2024. [Online].
[33] B. -. F. O. f. I. S. N. N. C. S. C. S. N. C. S. A. ANSSI - French Cybersecurity Agency, "Position Paper on Quantum Key Distribution," 2023.
[34] GSMA, "GSM Association Non-Confidential," 2024.
[35] NIST, "Migration to Post-Quantum Cryptography," 2022.
[36] ETSI, "TR 103 619 V1.1.1 Migration strategies and recommendations to Quantum Safe schemes," 2019.
[37] F Dupuy, "L'internet quantique : l'intrication au cœur du réseau de demain", Dunod, 2024.
[38] B-X Wang et al., "Long-distance transmission of quantum key distribution coexisting with classical optical communication over a weakly-coupled few-mode fiber," *Optics express,* vol. 28, no. 19, 2020.
[39] MJ Clark et al., "Coexistence of entanglement-based quantum channels with DWDM classical channels over hollow core fibre in a four node quantum communication network," *npj Quantum Information,* vol. 11, no. 11, p. 181, 2025.
[40] J Meister, P Kleinpaß & D Orsucci, "Simulation of satellite and optical link dynamics in a quantum repeater constellation," *EPJ Quantum Technology,* vol. 12, no. 11, 2025.
[41] S DiAdamo et al., "Packet switching in quantum networks: A path to the quantum internet," *Physical Review Research,* 2022.
[42] Y Mao et al., "Integrating quantum key distribution with classical communications in backbone fiber network," *Optics express,* 2018.
[43] JM Lukens, NA Peters & B Qi, "Hybrid classical-quantum communication networks," *Progress in Quantum Electronics,* 2025.
[44] Cisco, "Quantum Networking: How Cisco is Accelerating Practical Quantum Computing," [Online]. Available: https://blogs.cisco.com/news/quantum-networking-how-cisco-is-accelerating-practical-quantum-computing?dtid=osscdc000283&linkclickid=srch.
[45] Y Zheng et al., "Large-scale quantum communication networks with integrated photonics," *Nature,* 2026.
[46] European Commission, "Quantum Europe Strategy: Quantum Europe in a Changing World," 2025.
[47] OECD, "The National Academies of Sciences in Quantum Computing: Progress and Prospects," 2025.
[48] PW Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," 1997.

[49] D Gottesman, "Stabilizer Codes and Quantum Error Correction," 1997.
[50] Ericsson, "Ericsson Technology Review: Exploring the potential advantages of quantum computing in telecommunication networks," 2025.
[51] NIST, "Versatile quantum-enabled telecom receiver," 2 March 2023. [Online]. Available: https://postquantum.com/quantum-computing/use-cases-telecom/.
[52] NIST, "practical-quantum-enhanced-receivers-classical-communication," 20 April 2021. [Online]. Available: https://www.nist.gov/publications/practical-quantum-enhanced-receivers-classical-communication.
[53] NIST, "Quantum Matchmaking: New NIST System Detects Ultra-Faint Communications Signals Using the Principles of Quantum Physics," September 2020. [Online]. Available: https://www.nist.gov/news-events/news/2020/09/quantum-matchmaking-new-nist-system-detects-ultra-faint-communications.
[54] ETSI, "TR 103 619 V1.1.1 - Migration strategies and recommendations to Quantum Safe schemes," 2019.