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

RÉPUBLIQUE FRANÇAISE

# RÉSEAUX DU FUTUR

## Note de synthèse / Les technologies du quantique et leur impact sur les réseaux

11 juin 2026

ISSN n°2258-3106

## La démarche « Réseaux du futur » de l'Arcep et son comité scientifique

Quels formats les réseaux du futur pourraient-ils adopter ? Quelles en seront les incidences sur le métier de régulateur de l'Arcep ? Quels pourraient être les nouveaux acteurs ou l'évolution des modèles économiques dans les secteurs régulés par l'Autorité ?

Pour alimenter ce travail prospectif et disposer d'un regard à 360° sur ces évolutions, sur un horizon de 5 à 10 ans, l'Arcep a demandé à douze personnalités qualifiées du monde académique, entrepreneurial et industriel, dans divers domaines d'expertise, de se joindre à elle dans un comité scientifique. Et pour que la réflexion soit complète, les équipes de l'Arcep échangent également avec des acteurs spécialisés de l'écosystème : opérateurs, équipementiers, acteurs d'internet, fournisseurs de service, acteurs d'internet ou encore collectivités territoriales.

L'Arcep restitue au fil de l'eau ces travaux en produisant des notes thématiques, accessibles à tous sur son site, afin d'éclairer le débat public.

**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*

**Vous pensez pouvoir contribuer à ces travaux ?**

Cette réflexion se veut « vivante », l'Arcep invite tous ceux qui le souhaitent à s'approprier ces analyses et à lui envoyer des contributions sur reseaux-du-futur@arcep.fr

**Vous souhaitez être informé des prochaines présentations de notes thématiques ?**

Demandez à être invité à com@arcep.fr.

**Où lire les autres notes thématiques ?**

A la date de publication de la présente note (mai 2025), une première note a déjà été publiée : « L'informatique au cœur des réseaux télécoms » (octobre 2024).

Les prochaines notes seront publiées sur la page dédiée à la démarche « Réseaux du futur ».

# Les technologies quantiques et leur impact sur les réseaux

## Table des matières

# 1. Introduction

La première révolution quantique, permise par le concept de dualité onde-particule et la compréhension de la structure de la matière à l'échelle microscopique, a ouvert la voie à des innovations majeures comme les semi-conducteurs, le transistor, le laser ou encore le GPS. Ces avancées ont constitué le socle technologique des télécommunications modernes en rendant possible la miniaturisation des composants électroniques, l'amélioration des systèmes de transmission et le développement des communications optiques via la fibre [1].

Aujourd'hui, cette base scientifique continue d'inspirer une nouvelle étape : la deuxième révolution quantique qui exploite directement les comportements uniques des particules[1] aux niveaux atomique et subatomique dans l'objectif de développer de nouveaux paradigmes technologiques susceptibles de transformer des secteurs stratégiques. Ces technologies se répartissent aujourd'hui en trois grandes catégories complémentaires. La première concerne **les ordinateurs quantiques**, qui exploitent les lois de la mécanique quantique pour réaliser des calculs complexes, voire insolubles, pour les ordinateurs classiques actuels. La deuxième catégorie regroupe **les communications quantiques**, dont l'objectif est de connecter différents dispositifs quantiques entre eux afin de transmettre et partager de l'information de manière sécurisée, ouvrant la voie à l'« internet quantique ». La troisième catégorie sont les **capteurs ou détecteurs quantiques** qui permettent de mesurer des quantités physiques avec une précision et une sensibilité sans précédent. Ils peuvent détecter des changements infimes dans les grandeurs physiques au-delà des capacités des capteurs classiques. Par ailleurs, l'une des principales **implications** des avancées technologiques des ordinateurs et des communications quantiques concerne **la sécurité post-quantique**, qui vise à développer de nouveaux systèmes cryptographiques capables de résister aux attaques futures des ordinateurs quantiques, afin de protéger les données sensibles et les communications.

La nouvelle ère des technologies quantique soulève désormais une question majeure : cette deuxième révolution permettra-t-elle simplement d'améliorer les réseaux existants en renforçant, par exemple, la sécurité et la performance des communications ou ouvrira-t-elle la voie à l'émergence de télécommunications entièrement nouvelles fondées sur des réseaux quantiques ?

L'objectif de cette présente note est d'explorer la transition des technologies quantiques de la recherche vers l'industrie, en établissant, d'une part, un état des lieux des avancées académiques et industrielles dans le développement des ordinateurs quantiques et des solutions associées, et en anticipant, d'autre part, les étapes et le calendrier de cette transition. Elle s'intéresse également aux applications possibles des solutions quantiques dans le domaine des infrastructures numériques en analysant les transformations possibles de l'architecture et de la performance des réseaux ainsi que les modalités de cohabitation entre informatique classique et informatique quantique.

Il est à préciser que les capteurs quantiques, les applications les plus matures des technologies quantiques[2], apparaissent relativement indépendantes des deux autres (informatique et communications quantiques y compris la cryptographie), ainsi que des enjeux de prospective sur les

[1] Les principales propriétés quantiques des particules utilisées par ces technologies : la dualité onde-particule, le principe d'incertitude, la superposition, l'intrication, le non clonage ou encore l'effet tunnel

[2] Horloges atomiques, gravimètres, magnétomètres, électromètres ou aussi détecteurs de photon

infrastructures numériques. Le champ d'application relatif aux capteurs quantiques est donc exclu de la présente note.

La note s'articule ainsi autour de quatre axes complémentaires : dans une première partie sont présentés les ordinateurs quantiques, leurs principales promesses et une feuille de route globale ainsi que les défis techniques majeurs. Ensuite, sont analysées les menaces potentielles que ces technologies font peser sur la sécurité numérique, les solutions envisagées pour y faire face et leurs implications pour les réseaux mobiles. La troisième partie est consacrée aux réseaux quantiques et au rôle stratégique des infrastructures numériques dans leur émergence et leur déploiement. Enfin, une quatrième partie se focalise sur les stratégies mises en œuvre par les acteurs industriels et les politiques publiques visant à anticiper les risques et à accélérer le développement des technologies quantiques.

# 2. L'ordinateur quantique

## 2.1. Principes de fonctionnement d'un ordinateur quantique

L'ordinateur quantique utilise principalement les deux phénomènes fondamentaux de la physique quantique que sont la superposition d'états et l'intrication :

- **La superposition** désigne la capacité d'un système quantique à être décrit comme une combinaison simultanée de plusieurs états. Elle permet à l'unité fondamentale d'information en informatique quantique, dite qubit, de se trouver dans l'état 0 ou 1 ou dans une superposition de ces deux états [2].
- **L'intrication** permet aux qubits d'être interconnectés, quelle que soit la distance qui les sépare : selon Alain Aspect, l'intrication se produit lorsque deux particules ayant interagi dans le passé puis séparées dans l'espace, forment un tout quantique inséparable qui contient plus d'informations que celle contenue dans la somme des informations de chaque particule [3].

A l'image des ordinateurs classiques, les ordinateurs quantiques sont composés d'une partie matérielle (Hardware) et une partie logicielle (Software).

**Le processeur quantique** QPU[3], le composant central de tout ordinateur quantique, intègre des bits quantiques (ou qubits) ainsi que de l'électronique de contrôle et le matériel de calcul classique. Ce dernier composant assure notamment le stockage et l'exécution des instructions, l'amplification et la gestion des signaux d'entrée et de sortie, ainsi que le traitement des données afin de distinguer les signaux utiles du bruit [4]. **Un qubit physique** peut être réalisé selon différentes approches et de façons adaptées à des tâches spécifiques, à travers la manipulation et la mesure de systèmes qui présentent un comportement quantique, tels que des circuits supraconducteurs, des photons, des électrons, des ions piégés ou des atomes [5]. Contrairement aux bits classiques qui ne peuvent prendre que les valeurs 0 ou 1, les qubits, grâce au principe de **superposition**, ne sont pas limités à un état binaire unique.

A cela, pourraient s'ajouter des systèmes de refroidissement indispensables pour certaines variantes de qubit et un ordinateur classique associé pour piloter l'ensemble.

[3] Quantum Processing Unit

La partie logicielle relie l'utilisateur ou l'algorithme au matériel quantique. Elle est formée par la pile logicielle comprenant les langages de programmation quantique, les bibliothèques, les compilateurs et les outils de simulation nécessaires au développement, à la compilation, à l'optimisation et à l'exécution des algorithmes quantiques. Un algorithme quantique consiste à décomposer un problème en une suite d'opérations élémentaires appliquées à une mémoire quantique composée de qubits. Ces opérations, que l'on appelle des portes quantiques, s'enchaînent pour former un circuit quantique dont l'exécution permet de manipuler les états quantiques (superposition, **intrication**) afin d'obtenir un résultat lors de la mesure finale [6] .

## 2.2. Les promesses de l'ordinateur quantique

Les propriétés de superposition et d'intrication confèrent aux ordinateurs quantiques le potentiel de dépasser les limites de l'informatique classique grâce à une augmentation exponentielle de la puissance de calcul et la capacité à réaliser des calculs en parallèle. Les gains en termes d'accélération varient en fonction de l'algorithme, le type et la taille de problème : par exemple, l'algorithme de Peter Shor[4] pour la factorisation de nombres entiers [7] pourrait accélérer le calcul de façon exponentielle, tandis que l'algorithme de Lov Grover [8] pour la recherche dans des bases de données non structurées offre un gain quadratique.

### L'avantage quantique

En l'absence de métrique intrinsèque standardisée pour évaluer la performance des ordinateurs quantiques, la notion d'**avantage quantique** est utilisée comme indicateur comparatif. Elle désigne la capacité **réelle** des ordinateurs quantiques à réaliser des calculs **utiles** dépassant les capacités des superordinateurs, selon des critères mesurables tels que le temps de calcul, le coût en ressources ou la précision. IBM[5] et Pascal[6] soulignent que cet avantage suppose non seulement un gain démontrable par rapport aux approches classiques, mais aussi la production de résultats corrects et vérifiables. L'avantage quantique ne se réduira pas à un niveau de performance atteint ponctuellement sur la résolution d'un problème donné mais relèvera plutôt d'un processus progressif, fondé sur des démonstrations applicatives de plus en plus convaincantes, jusqu'à sa reconnaissance par la communauté scientifique.

Pour développer cet avantage quantique, plusieurs étapes de maturité technologiques apparaissent nécessaires au développement des ordinateurs quantiques.

### Noisy Intermediate-Scale Quantum (NISQ)

Le concept de **NISQ**, proposé par John Preskill, désigne une phase intermédiaire du développement du calcul quantique caractérisée par l'émergence de processeurs comportant typiquement quelques dizaines à quelques centaines de qubits physiques [9]. Cette génération marque une étape importante car elle dépasse progressivement les capacités de simulation des supercalculateurs classiques mais reste fortement contrainte par le bruit et les erreurs [2]. Le régime NISQ doit ainsi être compris comme une étape transitoire vers le calcul quantique tolérant aux fautes : un cadre expérimental permettant

[4] En reprenant la définition présentée par l'Académie des Technologies, il s'agit d'un algorithme de factorisation quantique de nombres entiers inventé par Peter Schor en 1994. Il permettrait en théorie de casser les clés publiques RSA en décomposant en nombres premiers [6].

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

[6] La course à l'avantage quantique - Pasqal : https://www.pasqal.com/fr/quantum-advantage/

d'explorer de nouveaux algorithmes, architectures et techniques de contrôle, en préparation d'un avantage quantique pratique, robuste et généralisable à grande échelle.

**L'ordinateur quantique tolérant aux fautes (Fault-Tolerant Quantum Computer, FTQC)**

Le concept de FTQC, marquant un niveau de maturité plus avancé, désigne des ordinateurs quantiques capables d'effectuer des calculs fiables et prolongés en corrigeant les erreurs intrinsèques des qubits grâce à des codes de correction d'erreurs et des architectures robustes.

Selon des analyses théoriques largement établies, un ordinateur quantique tolérant aux fautes pourrait offrir un **avantage quantique** déterminant **pour certaines classes de problèmes**. Autrement dit, un calcul nécessitant un temps exponentiel sur un ordinateur classique deviendrait réalisable en un temps raisonnable sur un ordinateur quantique de ce type tout en utilisant moins de de ressources computationnelles (temps de calcul et nombre d'opérations). Pour d'autres catégories de problèmes, des améliorations pourraient en théorie être obtenues, mais elles apparaissent plus limitées en comparaison des meilleurs algorithmes classiques connus [6].

## 2.3. Les applications du calcul quantique

On désigne par calcul intensif ou calcul haute performance (High Performance Computing – HPC) un domaine de l'informatique fondé sur l'utilisation de systèmes spécifiques destinés à résoudre des problèmes complexes et fortement exigeants en ressources de calcul [10].

Le calcul quantique est considéré comme stratégique dans de nombreux secteurs où le calcul intensif, la résolution d'équations aux dérivées partielles, l'optimisation de fonctions, l'apprentissage automatique ou l'analyse prédictive jouent un rôle déterminant.

Ces calculs sont principalement mis en œuvre dans le cadre de la recherche fondamentale et de la recherche appliquée, et sont susceptibles de bénéficier à un nombre croissant de secteurs industriels, en favorisant l'innovation et en réduisant les temps de conception, de validation et de mise sur le marché des produits. Ainsi, Selon le type de problème, différents secteurs pourraient en tirer parti [11] [12]:

- **Cybersécurité et cryptographie :** factorisation de nombres entiers, génération de clés sécurisées, analyse de protocoles cryptographiques.
- **Défense et sécurité :** simulation de systèmes complexes et optimisation stratégique.
- **Médecine et pharmaceutique :** modélisation de molécules, simulations de réactions chimiques, découverte de médicaments.
- **Finance :** optimisation de portefeuilles, gestion des risques, modélisation de marchés financiers.
- **Science des matériaux et chimie** : conception de nouveaux matériaux, simulations quantiques de molécules et de réactions.
- **Transport et logistique :** optimisation de routes et de chaînes d'approvisionnement, planification complexe.

L'utilisation d'ordinateurs NISQ permet déjà de répondre à certains cas d'usage, notamment lorsque l'objectif est de contribuer à explorer des problèmes spécifiques sans exiger une précision parfaite. C'est le cas, par exemple, de certaines tâches de simulation de systèmes quantiques en chimie ou en

science des matériaux, ou encore pour les domaines où des méthodes hybrides combinant calcul classique et quantique permettent d'obtenir des résultats exploitables malgré le bruit [9]. En revanche, pour des applications nécessitant une fiabilité élevée et des résultats strictement exacts, comme la cryptanalyse via l'algorithme de Shor ou des simulations chimiques industrielles de haute précision, le passage à l'ordinateur tolérant aux fautes devient essentiel [12, 11]. Ainsi, le NISQ est pertinent pour des usages exploratoires, de prototypage et d'optimisation approximative, tandis que le FTQC est la condition nécessaire pour débloquer à grande échelle, les applications quantiques cryptographiques et à fort impact industriel.

À l'avenir, ces applications ont vocation à bénéficier aux entreprises de toutes tailles. Toutefois, au stade actuel de développement de cette technologie, et compte tenu des compétences spécialisées à mobiliser, les premiers acteurs à se positionner comme utilisateurs du calcul quantique sont principalement des grandes entreprises ou des instituts de recherche.

## 2.4. Défis et perspectives du calcul quantique

De nombreux défis techniques sont encore à relever avant de parvenir à un ordinateur tolérant aux fautes. Une partie des défis est liée au phénomène de décohérence[7] dû à la nature des qubits extrêmement sensibles aux perturbations extérieures (température, vibrations, ondes acoustiques, bruit électromagnétique), ce qui entraîne des erreurs et limite la stabilité des calculs. De plus, la mise à l'échelle des systèmes, c'est-à-dire l'augmentation du nombre de qubits tout en conservant leur fiabilité, représente un obstacle majeur.

Outre la correction d'erreur et le passage à l'échelle, de nombreux défis restent à relever, notamment l'amélioration des mémoires quantiques sera nécessaire afin de permettre l'exécution d'algorithmes plus ambitieux.

**La correction d'erreur**

La réduction du taux d'erreur constitue un défi majeur commun à tous les ordinateurs quantiques, quelle que soit la technologie employée. La principale source d'erreurs provient de problèmes de stabilité des qubits et de décohérence, c'est-à-dire de perte d'information quantique due aux interactions avec l'environnement.

La correction d'erreurs quantiques peut reposer notamment sur la combinaison d'un grand nombre de qubits physiques afin de former un qubit logique plus fiable et moins sensible aux erreurs. Le nombre de qubits nécessaires pour obtenir un qubit logique dépend fortement de la qualité des qubits et du code de correction utilisé ; il peut atteindre plusieurs milliers, voire davantage.

Par ailleurs, il est nécessaire d'améliorer l'isolation des qubits vis-à-vis leur environnement pour réduire les sources d'erreurs. Cela implique des progrès matériels significatifs dans la conception et la fabrication des composants de l'ordinateur quantique. Quelle que soit la technologie considérée, la plupart des ordinateurs quantiques doivent fonctionner à des températures extrêmement basses, proches du zéro absolu à l'exception des technologies photoniques, pour lesquelles seuls les détecteurs nécessitent un refroidissement cryogénique. Ces contraintes exigent des infrastructures complexes et coûteuses.

[7] La décohérence est le phénomène par lequel un système quantique perd ses propriétés quantiques comme la superposition d'états

Enfin, les imperfections des systèmes de contrôle peuvent également introduire des erreurs supplémentaires. L'un des paradoxes fondamentaux de l'ordinateur quantique réside précisément dans cette tension : les qubits doivent être suffisamment isolés pour préserver leur cohérence, tout en restant suffisamment contrôlables pour permettre la réalisation d'opérations quantiques fiables.

Actuellement, les ordinateurs quantiques les plus performants sont les ordinateurs NISQ présentés dans la partie 2.2. Ils subissent des erreurs toutes les 100 à 1 000 opérations et ne disposent que d'un nombre limité de qubits. Ils utilisent des algorithmes tolérants au bruit ou à faible profondeur de circuit, généralement hybrides classiques. De plus, pour atténuer les erreurs, ces machines recourent à des méthodes statistiques pour traiter les résultats quantiques.

**Passage à l'échelle**

Les enjeux liés à la scalabilité des ordinateurs quantiques sont majeurs : il faut non seulement réussir à augmenter le nombre de qubits, mais aussi s'assurer que les accélérations théoriques apportées par les algorithmes quantiques restent significatives lorsqu'on considère l'ensemble du processus de calcul. Plus largement, un défi central consiste à parvenir à manipuler et contrôler un grand nombre de systèmes quantiques intriqués avec une précision et une fiabilité suffisantes, condition essentielle pour envisager des applications industrielles concrètes [13].

Selon un rapport de l'OCDE et de l'Office européen des brevets (OEB) publiée en décembre 2025 [14], si le paysage des technologies quantiques se développe rapidement, il est maintenant confronté à des défis de passage à l'échelle et de commercialisation des technologies. Le secteur pourrait entrer dans une nouvelle phase où l'expansion rapide qu'il a connue initialement cèderait la place à un développement plus ciblé et à la maturation des technologies.

**Enjeux économiques**

Les défis liés au développement de l'informatique quantique ne se limitent pas aux aspects techniques, mais concernent également des enjeux économiques et stratégiques. L'aspect économique des ordinateurs quantiques reste aujourd'hui difficile à évaluer, notamment parce que cette technologie est encore à un stade précoce et que la production demeure limitée, ce qui maintient des coûts de développement et de fabrication très élevés. À cela s'ajoute une forte incertitude concernant la possibilité de construire, à terme, des machines réellement capables de fonctionner à grande échelle.

La capacité de l'écosystème à déployer à grande échelle des technologies quantiques dépendra de nombreux facteurs, allant de l'investissement au développement des compétences requises en passant par la résilience des chaînes d'approvisionnement.

## 2.5. Feuille de route globale

Il est possible de définir une feuille de route identifiant à large maille les progrès à accomplir afin de passer du niveau d'exigences du NISQ aux ambitions du FTQC. Cette feuille de route, illustrée à la Figure 1, est principalement structurée autour de deux ambitions : augmentation du nombre de qubit et amélioration de la tolérance aux fautes grâce à la correction d'erreurs quantiques. Ainsi, le nombre de qubits logiques nécessaires pour que les algorithmes dédiés aux calculateurs FTQC puissent résoudre les problèmes de portée industrielle est estimé à au moins dix mille.

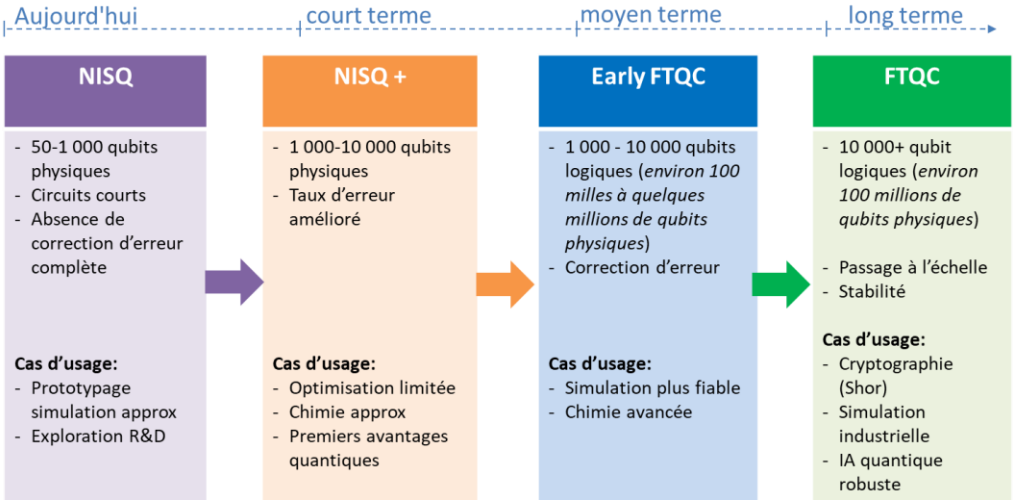


Figure 1:Feuille de route vers le FTQC. Source [9].

Les startups françaises Pasqal, C12, Alice & Bob, Quandela et Quobly, ainsi que les grands acteurs du numérique tels que IBM, Google, Microsoft ou Amazon, mènent des travaux de recherche et développement afin de mettre au point un ordinateur quantique capable de surpasser les performances des machines classiques.

La plupart de ces acteurs ont rendu publique leur feuille de route, qui affiche l'ambition d'accroître progressivement la capacité de calcul de leurs machines, jusqu'à parvenir au calcul quantique tolérant aux fautes. Certains précisent l'horizon temporel de leurs principaux jalons tandis que d'autres choisissent de ne pas communiquer leurs prévisions. **Dans tous les cas, une convergence se dessine pour situer l'émergence du FTQC à l'horizon 2030 et d'un passage à l'échelle vers 2035.**

## 2.6. Intelligence artificielle et informatique quantique : synergie et enjeux d'hybridation

**Des approches concurrentes face à la complexité**

Comme déjà évoqué dans cette note, un intérêt majeur de l'informatique quantique réside dans sa capacité potentielle à résoudre des problèmes de calcul qui dépassent les limites de l'informatique classique. Jusqu'à présent, ces problèmes de calcul sont traités par des supercalculateurs.

L'essor de l'intelligence artificielle a été à l'origine d'avancées majeures dans les domaines de la recherche et de l'industrie en permettant la résolution de problèmes plus complexes, avec des gains significatifs en termes d'efficacité, de performance et d'innovation. Il en résulte aujourd'hui et plus encore à l'avenir une forte complémentarité et d'importantes synergies entre les architectures de calcul classiques (CPU), les processeurs graphiques (GPU[8]) et les processeurs quantiques (QPU).

Selon le rapport de l'Académie des technologies, le développement de l'intelligence artificielle pourrait représenter une forme de concurrence, pour le calcul quantique. En effet, l'évolution des modèles

[8] *Graphics processing unit*

d'IA, conjuguée aux progrès des processeurs tels que les GPU dotés d'opérations vectorielles ou matricielles, ainsi qu'à l'émergence des NPU[9], fournit des outils puissants capables de traiter un très grand nombre de problèmes de manière statistique. Ces avancées pourraient ainsi permettre de résoudre certains calculs initialement envisagés comme relevant exclusivement du calcul quantique.

**Synergies IA–quantique**

La plupart des acteurs du secteur perçoivent une complémentarité et voient une réelle opportunité à l'intégration de l'informatique quantique aux modèles d'IA. Les processeurs quantiques pourraient optimiser les phases d'alimentation en données et accélérer l'entraînement des modèles en exploitant la superposition et le parallélisme quantique, qui permettent une exploration plus efficace de l'espace des paramètres et une optimisation plus rapide des performances. Cette approche peut conduire à une réduction du nombre d'itérations nécessaires à l'apprentissage et à une meilleure exploration des solutions [15]. Il existe déjà des algorithmes quantiques d'apprentissage automatique susceptibles d'être plus efficaces et moins coûteux que leurs équivalents classiques pour certains cas d'usage.

Dans la pratique, de nombreux cas d'usage combinent différents types de problèmes : certains peuvent être plus efficacement résolus par un processeur quantique, tandis que d'autres restent mieux adaptés au calcul classique HPC. Dans ce contexte, une approche de solution hybride, répartissant les tâches entre informatique classique et informatique quantique, apparaît particulièrement prometteuse. Les acteurs du secteur travaillent déjà à assurer une intégration fluide entre ces deux types de calcul.

Pour certains grands fournisseurs de services d'informatique en nuage qui développent à la fois leurs modèles d'IA et leurs processeurs quantiques, l'IA pourrait ainsi jouer un rôle clé dans l'intégration du calcul quantique et du calcul classique, en facilitant une interaction fluide entre ordinateurs classiques et quantiques via l'informatique en nuage. La normalisation est appelée à jouer un rôle clé pour garantir l'interopérabilité entre technologies et faciliter le développement d'écosystèmes hybrides. En Europe, le CEN/CENELEC a notamment mis en place un groupe de travail pour étudier ces questions. La décomposition des problèmes en taches et l'hybridation des ressources de calcul les plus adaptées à celles-ci CPU, GPU ou QPU constitue vraisemblablement l'avenir de l'informatique. Dans le futur, l'architecture de calcul sera ainsi définie, en s'appuyant sur les différentes briques technologiques disponibles les plus adaptées à la nature des problèmes à résoudre.

Il est également intéressant de noter que les liens entre l'informatique classique et l'informatique quantique ne se limitent pas à une hybridation future pour la résolution de problèmes complexes. L'intelligence artificielle qui utilise aujourd'hui essentiellement l'informatique classique, joue un rôle important dans les travaux permettant l'avancée de l'informatique quantique. Elle peut être mobilisée sur l'ensemble du développement de l'ordinateur quantique[10], depuis la phase de conception initiale jusqu'aux principes de correction d'erreurs, en passant par le contrôle des systèmes physiques.

## 2.7. L'informatique quantique en nuage et les premiers calculs

Le financement des ordinateurs quantiques est très coûteux et reste risqué pour les investisseurs. Comme évoqué précédemment, les ordinateurs quantiques nécessitent une grande stabilité et un haut

[9] *Neural processing unit*

[10] Parmi les exemples figurent le décodeur AlphaQubit, fondé sur l'IA, qui identifie les erreurs de calcul quantique avec une précision de pointe, ainsi que la méthode AlphaTensor-Quantum, basée sur l'apprentissage profond par renforcement, dont l'objectif est d'optimiser un circuit logique quantique afin de l'exécuter plus efficacement, c'est-à-dire avec un nombre réduit d'opérations.

niveau d'isolation avec l'extérieur pour être performants. C'est pourquoi ils sont principalement installés dans de grands centres de calcul qui disposent des infrastructures nécessaires et qui sont connectés en nuage. Ainsi, ces plateformes de calcul *cloud* peuvent fournir de la puissance de traitement quantique pour le développement d'algorithmes, de premières simulations, de calculs et de modélisations complexes qui s'appuient sur la technologie quantique. Cette approche réduit le besoin de compétences et d'expertise en propre pour accéder aux ordinateurs quantiques en bénéficiant de l'expertise quantique des plateformes de *cloud*.

Une multitude d'acteurs sont présents sur le marché de l'accès à des ordinateurs quantiques en nuage, dont les principales entreprises de *cloud computing* telles qu'Amazon, Google, Microsoft, et IBM ou encore OVH et Scaleway en France. Ils proposent des services quantiques, mobilisant une puissance de traitement qui reste encore limitée. Les premières offres permettent de tester le calcul quantique sur des émulateurs et des ordinateurs quantiques avec une puissance limitée (ordinateurs *NISQ*).

L'ordinateur quantique n'a pas vocation à remplacer les ordinateurs classiques : il apparait destiné à des cas d'usage bien spécifiques, et bien souvent en combinaison avec l'informatique classique.

Les modèles économiques qui pourraient émerger avec l'essor de l'informatique quantique apparaissent encore incertains, mais plusieurs pistes se dessinent :

- la commercialisation d'ordinateurs quantiques destinée aux acteurs avec des forts impératifs de sécurité des données qui disposent des moyens financiers et de l'infrastructure nécessaire pour accueillir une machine ;
- la mise à disposition de puissance de calcul via des centres de données quantiques (*quantum data centers*), il s'agit d'une solution plus accessible destinée à la plupart des utilisateurs qui souhaitent avoir accès au calcul quantique sans pour autant être en mesure de posséder un ordinateur quantique.

## 2.8. L'informatique quantique pour les besoins du secteur télécom

En complément des applications dans le domaine de la cryptographie qui seront traitées plus en détail dans le chapitre suivant, les acteurs du secteur des communications électroniques pourraient potentiellement tirer profit de la puissance de calcul des ordinateurs quantiques pour des problématiques spécifiques nécessitant une forte intensité de calcul, telles que l'optimisation de la gestion des réseaux et de l'allocation des ressources et le traitement du signal. Ces problématiques donnent lieu aujourd'hui à l'utilisation d'algorithmes classiques souvent fondés sur des heuristiques ou des méthodes d'approximation, qui permettent d'obtenir des solutions satisfaisantes mais potentiellement sous-optimales face à la complexité croissante des réseaux.

**L'optimisation des déploiements et la gestion des réseaux**

Le déploiement et l'exploitation des réseaux de communications électroniques mobiles et fixes requièrent de nombreux calculs d'optimisation complexes, ce que soit au niveau de la configuration du routage des flux de données dans le réseau, du positionnement des antennes des réseaux mobiles ou encore du déploiement des réseaux de fibres optiques. Avec le développement des usages, la densité de données à traiter et d'appareils connectés pourrait continuer à croître, appelant des calculs d'optimisation de plus en plus complexes, susceptibles de constituer un cas d'usage de l'informatique quantique [16, 17].

**L’allocation des ressources radio des réseaux mobiles**

L’informatique quantique pourrait être pertinente pour aider à résoudre les problèmes combinatoires notoirement difficiles impliqués dans l'optimisation de l’usage du spectre. La planification et les affectations de canaux radio, la minimisation des interférences ainsi que le partage dynamique des fréquences radio pourraient en bénéficier. L’optimisation quantique serait notamment utile dans des environnements complexes ou congestionnés où l’optimisation des ressources est clé et sa complexité importante.

**Le traitement du signal dans les réseaux mobiles**

L'informatique et les algorithmes quantiques pourraient également contribuer à faciliter la conception des systèmes assurant de manière fiable et efficace le traitement du signal sur la couche physique des communications électroniques. Ces tâches sont intensives en calcul et impliquent souvent des compromis entre performance et complexité. Des avancées portant sur la conception du matériel et des logiciels utilisés pour le traitement du signal pourraient permettre d’en améliorer les performances, contribuant ainsi à optimiser la couverture et la qualité de service mobile.

**Des perspectives d’application qui restent très exploratoires à ce stade**

Des travaux visant à améliorer la performance et l’efficacité des réseaux pour permettre une meilleure utilisation des ressources (sites radio, fréquences, énergie) pour répondre à la demande de trafic accrue tout en augmentant le débit et en réduisant la latence des communications sont menés par des équipes de recherche académiques et privées [18, 17, 16]. Vodafone, par exemple, s’est associé avec la société ORCA Computing qui développe un ordinateur quantique photonique pour optimiser la conception, la planification et le déploiement de ses réseaux mobile et fixe. L’opérateur espère notamment optimiser le routage dans les fibres optiques pour réduire la longueur totale des fibres à déployer et optimiser l'emplacement des stations de base mobiles pour minimiser les travaux de génie civil. A terme, Vodafone souhaite également modéliser à l’aide de l’informatique quantique ses infrastructures internationales comme les câbles sous-marins ou les services satellites « direct to device » [19].

Selon les acteurs interrogés, il ressort que le secteur des télécoms ne semble pas être une priorité immédiate de la recherche algorithmique de l’informatique quantique. Certains acteurs estiment que les ordinateurs quantiques ne fourniront une réelle valeur ajoutée aux réseaux télécoms que lorsqu’ils deviendront à la fois évolutifs et tolérants aux erreurs.

En effet, dans un premier temps les opérateurs pourraient accéder à la puissance quantique via des centres de calculs en nuage pour résoudre les problèmes d’optimisation via une approche hybride, combinant informatique classiques et quantiques.

Sur le long terme, avec un ordinateur quantique pleinement fonctionnel (FTQC), il pourrait être envisagé de résoudre des problèmes d’optimisation plus complexes dans les réseaux télécoms, tels que l’ajustement dynamique du routage des flux de données, une tâche qui reste aujourd’hui hors de portée des calculateurs classiques.

Pour autant, l'avantage quantique reste encore difficile à mesurer, celui-ci devra être mis en perspective avec l'efficacité des heuristiques classiques existantes, qui répondent déjà de manière adéquate à la majorité des cas d'usage courants.

# 3. L'ordinateur quantique : menace ou révolution pour la sécurité des communications ?

L'émergence de l'informatique quantique représente un enjeu majeur pour la sécurité des communications. Un ordinateur quantique suffisamment puissant et capable d'utiliser l'algorithme de Shor [7] ou l'algorithme de recherche de Grover [20] pourrait casser les systèmes de cryptographie classiques [21], qui sont très largement utilisés, tels que RSA [22], et par conséquent, la confidentialité des communications et des informations stockées qui en dépendent.

L'horizon de la menace est difficile à estimer, les estimations pour casser RSA-2048 sont de 8h avec environ 20 millions de qubits physiques [23] ou 1 semaine avec 1 million de qubits physiques [24].

Les protocoles de sécurité notamment ceux utilisés pour les communications électroniques, sont conçus pour être utilisés sur de longues durées et intègrent généralement des mécanismes permettant d'augmenter les tailles de clés ou d'ajuster les paramètres lorsque le niveau de sécurité diminue. Toutefois, la menace quantique pourrait imposer des changements plus profonds : il ne s'agirait plus seulement d'augmenter des tailles de clés, mais potentiellement de remplacer entièrement les primitives cryptographiques et d'adapter les protocoles pour les supporter [26].

Deux approches principales émergent face à ce risque :

- L'approche physique avec la **quantum key distribution (QKD)** qui permet de générer et de distribuer des clés cryptographiques symétriques au moyen de canaux quantiques dédiés (fibre optique ou satellite). Cette méthode s'appuie sur les principes de la théorie de l'information quantique afin de garantir une sécurité informationnelle théorique lors de l'établissement des clés.
- L'approche algorithmique avec la **cryptographie post-quantique** qui repose sur de nouveaux paradigmes mathématiques supposés résistants aux attaques quantiques (par exemple basés sur les réseaux euclidiens).

Dans ce contexte, l'Agence nationale de la sécurité des systèmes d'information (ANSSI), encourage toutes les entreprises à inclure dès à présent la menace quantique dans leur analyse de risque et d'envisager l'adoption de solutions de cryptographie post-quantique (PQC) pour sécuriser les produits cryptographiques concernés [25].

## 3.1. Les menaces du quantique sur les réseaux télécoms

**Intercepter aujourd'hui pour déchiffrer demain (« store now, decrypt later »)**

L'émergence de capacités de calcul quantique susceptibles de compromettre les algorithmes cryptographiques asymétriques introduit un risque majeur de compromission différée de la confidentialité des communications électroniques. Des acteurs malveillants pourraient tenter d'intercepter et de conserver, dès aujourd'hui, des flux chiffrés ou des données protégées afin de les déchiffrer ultérieurement lorsque des capacités quantiques pertinentes seront disponibles.

Ce scénario modifie profondément l'appréciation du risque dans le temps : des communications considérées comme sécurisées aujourd'hui pourraient devenir exploitables demain, alors que les données concernées ont vocation à rester confidentielles sur de longues périodes [27].

S'agissant de la sécurisation des échanges sur les réseaux de télécommunications, les données et échanges protégés par TLS[11]/IPSec[12] [28] et par des mécanismes à certificats (ex : interfaces d'itinérance), incluant notamment des données d'abonnés, du matériel d'authentification, des clés privées et des chaines de certificats, pourraient être exposés à une telle menace [29, 30].

**Fragilisation des mécanismes d'établissement de la confiance**

L'agence nationale de la sécurité des systèmes d'information (ANSSI) souligne notamment un risque accru de falsification de signatures et d'usurpation d'identité, qui affecterait l'authentification et l'intégrité des échanges lorsque ces signatures sont requises (avec des nuances selon le cas d'usage et l'exigence de validité à long terme des signatures) [29].

S'agissant des réseaux de téléphonie mobile, ce risque concernerait l'utilisation des certificats X.509[13] [28], des chaines de certificats et des clés privées dans l'authentification mutuelle et l'intégrité/authentification de certains échanges (ex : entre partenaires d'itinérance), dans la mesure où l'utilisation d'un ordinateur quantique cryptanalytique sur ces composants pourrait permettre des attaques d'usurpation d'identité et de falsification/tampering[14] [31].

**Menaces hybrides et risque de transition dans des environnements complexes**

Les menaces liées au quantique ne se manifestent pas uniquement sous la forme d'attaques reposant uniquement sur le recours à l'informatique quantique. Elles pourraient également s'inscrire dans des scénarios hybrides, combinant des techniques d'attaque conventionnelles avec l'affaiblissement progressif des mécanismes cryptographiques.

Des vulnérabilités classiques pourraient ainsi être exploitées en parallèle d'une rupture de la confiance cryptographique, augmentant la probabilité d'attaques complexes et d'effets en cascade, par exemple via la compromission de chaînes de mise à jour, de systèmes d'identité ou de dépendances de la chaîne d'approvisionnement.

## 3.2. Les solutions face aux menaces quantiques

**Cryptographie post-quantique (PQC)**

La cryptographie post-quantique (PQC) regroupe un ensemble d'algorithmes conçus pour rester sûrs face à des attaquants disposant d'une puissance de calcul quantique. Contrairement aux schémas classiques comme RSA ou ECC, dont la sécurité repose sur la factorisation ou le logarithme discret, les algorithmes PQC s'appuient sur des problèmes mathématiques pour lesquels aucun algorithme quantique efficace n'est connu à ce jour. Cette conception les rend résistants aux attaques quantiques connues, car les accélérations offertes par les algorithmes quantiques actuels (Shor, Grover) ne permettent pas de casser efficacement ces problèmes sous leurs paramètres recommandés.

[11] TLS (Transport Layer Security) est une des solutions les plus répandues pour la protection des flux réseau

[12] IPsec est une suite de protocoles de communication sécurisée permettant la protection des flux réseau

[13] Norme X.509 définie par l'Union internationale des télécommunications (UIT) qui définit le format des certificats d'infrastructure à clé publique (PKI)

[14] Le tampering des données est la modification, la suppression ou la manipulation non autorisée de données,

L'institut de standard américain NIST[15] a déjà normalisé des algorithmes post-quantique de chiffrement à clé publique (PKC) tel que le ML-KEM utilisé pour l'échange de clés [32]. Ces évolutions n'impliquent pas de changement matériel majeur pour les infrastructures informatiques et télécoms classiques, bien qu'elles puissent requérir davantage de ressources logicielles.

Cependant, l'intégration de la PQC dans les protocoles existants est complexe. Elle implique l'intégration de nouveaux algorithmes, des modifications au sein des protocoles comme TLS ou SSH et des adaptations des piles logicielles, ce qui est susceptible d'introduire de nouvelles vulnérabilités.

Au sein du 3GPP, les réflexions relatives à la transition vers la cryptographie post-quantique ont été engagées dans le cadre des dernières évolutions de la 5G (Releases 19–20), principalement sous la forme d'études techniques et d'analyses d'impact. À ce stade, ces travaux ne se traduisent pas encore par une intégration normative obligatoire dans les spécifications 5G existantes au contraire des discussions préparatoires à la Release 21, associées aux premières spécifications 6G. L'intégration normative de mécanismes de sécurité résistants aux menaces du quantique, notamment la cryptographie post quantique est principalement envisagée dans le cadre de la Release 21 et des spécifications associées à la 6G qui sera nativement « *quantum safe* ».

**Quantum Key Distribution (QKD)**

La distribution quantique de clés (QKD) est une technique permettant d'établir une clé symétrique entre deux parties en exploitant des propriétés physiques de la mécanique quantique, notamment le fait que toute mesure d'un état quantique le perturbe et peut donc être détectée. En pratique, elle repose sur deux canaux distincts :

- Un canal quantique dédié (fibre optique ou liaison optique libre) pour la transmission des états quantiques qui permettent d'encoder la clé,
- Un canal classique authentifié pour les échanges de signalisation, la correction d'erreurs et la vérification d'intégrité.

La QKD ne chiffre pas les données elle-même : elle sert uniquement à distribuer des clés symétriques ensuite utilisées par des algorithmes classiques (par exemple AES). Il s'agit donc d'un mécanisme de distribution de clés et non d'une solution de chiffrement de bout en bout. Selon la position commune de plusieurs agences européennes de cybersécurité, la QKD reste aujourd'hui à un stade pré-opérationnel [33]. Elle nécessite des infrastructures physiques dédiées, coûteuses et difficiles à déployer, présente de fortes contraintes de distance et d'atténuation optique, et dépend de composants matériels encore peu normalisés. De plus, elle n'élimine pas le besoin de mécanismes cryptographiques classiques pour l'authentification et la protection des données [33]. En conséquence, la QKD ne peut être envisagée, à ce stade, que pour des liaisons point à point très spécifiques, dans des environnements contrôlés, et ne constitue pas une solution générique pour la sécurisation des communications à grande échelle, contrairement à la cryptographie post-quantique logicielle.

**Solutions Hybrides**

Face à la menace que représente le calcul quantique pour les mécanismes de chiffrement actuels, l'hybridation consiste à combiner plusieurs mécanismes de sécurité reposant sur des mécanismes

[15] NIST : National Institute of Standards and Technology

différents, afin de ne pas dépendre d'un seul. L'objectif est de renforcer la robustesse globale des communications, de limiter les risques liés à l'évolution des capacités de calcul, et de permettre une transition maîtrisée vers la sécurité post-quantique. Dans une approche hybride, les clés issues de plusieurs mécanismes sont combinées pour produire une clé finale unique, garantissant que la sécurité est préservée tant qu'au moins l'un des mécanismes sous-jacents reste sûr.

La combinaison de mécanismes cryptographiques classiques avec des algorithmes post-quantiques constitue la première étape de l'hybridation. Lors de l'établissement d'une communication sécurisée, des algorithmes classiques éprouvés sont utilisés conjointement avec des algorithmes résistants au calcul quantique pour négocier les clés de chiffrement. Cette approche permet de renforcer la protection face aux menaces futures.

En contrepartie, l'intégration de la PQC dans des protocoles déjà déployés accroît la complexité logicielle et nécessite une attention particulière à la qualité et à la maturité des implémentations afin d'éviter l'introduction de nouvelles vulnérabilités. Par exemple, des groupes de travail sont en cours pour étudier l'hybridation de protocoles connus tel que TLS avec des méthodes post-quantique tel que ML-KEM. Les premiers retours de ces travaux de l'IETF indiquent que cela impacte la taille des clés publiques transmises, peut provoquer une duplication des clés partagées, et qu'il existe une possibilité non nulle d'échec lors du *handshake*[16].

Une hybridation plus avancée pourrait consister à associer les mécanismes classiques, post-quantiques et la distribution quantique de clés [34]. Dans ce cas, des échanges de clés sont réalisés sur le réseau classique à l'aide d'algorithmes traditionnels et post-quantiques, tandis qu'un canal quantique permet de générer des clés supplémentaires bénéficiant de garanties physiques de sécurité. Cette approche permet de diversifier les méthodes cryptographiques reposant sur des hypothèses mathématiques différentes (cryptographie classique et post-quantique), ainsi que des mécanismes fondés sur les lois de la physique grâce à la QKD. Les clés issues de ces différentes sources sont ensuite combinées pour produire une clé finale unique. Elle s'accompagne toutefois d'une complexité importante en termes d'intégration, d'exploitation et de coûts, ce qui la réserverai aux usages les plus sensibles.

Il est recommandé par l'ANSSI et par les instituts de standards européen[17] et américain de préparer la migration des protocoles de sécurité des réseaux télécoms notamment les PKI, vers des solutions hybrides combinant cryptographie classique et cryptographie post-quantique de façon structurée : inventorier les usages de la cryptographie à clé publique (y compris mises à jour logicielles et produits tiers), planifier une migration progressive, et prendre en compte la chaine de fournisseurs/partenaires [29] [35] [36]. Les lignes directrices de la GSMA mettent en avant des contraintes pratiques de déploiement dans les réseaux (infrastructures existantes, dépendances à des fournisseurs, support des outils tiers, et besoins de tests d'interopérabilité sur des produits multi-vendeurs lors de l'introduction de nouveaux mécanismes/protocoles) [31].

## 4. Les réseaux quantiques

Les réseaux ou l'internet quantiques représentent l'infrastructure et les protocoles de communication nécessaires à l'interconnexion de dispositifs quantiques répartis [37] permettant la communication de bits quantiques. Ces réseaux reposent sur des principes analogues à ceux des réseaux classiques, mais

[16] Processus automatisé de négociation qui établit les paramètres d'une communication entre deux entités avant que la communication commence

[17] ETSI : European Telecommunications Standards Institute

mettent en œuvre des mécanismes physiques totalement différents, fondés sur les lois de la mécanique quantique, notamment l'intrication et la superposition des états quantiques.

A la différence des réseaux classiques, les réseaux quantiques ne répondraient, dans un premier temps, qu'à des cas usages très spécifiques, ciblant des applications de niche à forte valeur ajoutée, dans des domaines comme la recherche scientifique, la défense, la cybersécurité ou la finance [37] :

- **Le renforcement de la sécurité des communications :** les réseaux quantiques pourraient permettre de mettre en place les systèmes de cryptographie quantique comme la distribution de clés quantiques (QKD), présentée en partie 3.2.
- **La multiplication de la puissance de calcul :** le déploiement de nœuds de calcul quantique interconnectés via un réseau pourrait permettre de construire un système de calcul distribué beaucoup plus puissant que ce qu'un seul appareil pourrait faire. Ce type de réseau pourrait partager des états quantiques entre des nœuds distants, ce qui est essentiel pour coordonner des calculs complexes répartis favorisant l'émergence du calcul quantique distribué. En effet, la résolution de problèmes nécessitant des millions de qubits pourrait être difficilement réalisable sur un seul ordinateur quantique, alors que le recours à une infrastructure modulaire reliant plusieurs processeurs pourrait être une approche plus viable à court terme.
- **La transmission d'informations issues de capteurs quantiques avancés** pour permettre l'acheminement sans dégradation de mesures ultra précises générées par les capteurs quantiques (par exemple, pour la synchronisation d'horloges atomiques) vers des centres de calcul quantique. Les réseaux quantiques permettraient aussi de préserver des corrélations quantiques entre plusieurs capteurs distants, ouvrant la voie à une interférométrie ou détection distribuée encore plus précise.

Les premiers prototypes visent à intégrer les réseaux quantiques aux réseaux classiques, en s'appuyant sur les infrastructures existantes, notamment les réseaux de fibres optiques et les liaisons satellitaires. En effet, plusieurs études et expérimentations montrent que les technologies quantiques, notamment la distribution de clés quantiques (QKD), peuvent coexister avec les signaux classiques dans les mêmes fibres optiques existantes, ce qui permet de réutiliser une grande partie de l'infrastructure télécoms déjà en place. En pratique, cela implique souvent l'utilisation de techniques de multiplexage et de filtres pour réduire les interférences entre les signaux quantiques et les signaux classiques [38] [39].

La composante satellitaire est également une piste majeure pour étendre les réseaux quantiques à grande échelle. Des projets actuels envisagent que les satellites puissent distribuer des photons intriqués ou des clés quantiques entre différentes stations terrestres, permettant d'interconnecter des réseaux quantiques répartis sur de très grandes distances ou entre continents.

Il convient de souligner que la capacité de transfert d'information d'un réseau quantique demeurera limitée, sa fonction principale étant de transporter des états quantiques associés à la transmission de données qui continueront à circuler, quant à elles, sur le réseau classique. Ainsi, de même que les ordinateurs quantiques n'ont pas vocation à remplacer les ordinateurs classiques, les réseaux quantiques ne remplaceront pas les infrastructures existantes, mais les compléteront.

## 4.1. Les défis technologiques

La construction de réseaux quantiques, encore en stade embryonnaire, s'avère compliquée face à des limitations techniques principalement liés à la difficulté de la mesure quantique ou la fragilité particulière de l'intrication [37].

**La transmission à longue distance**

L'un des principaux verrous concerne la transmission des bits quantiques sur de longues distances. En effet, les propriétés physiques de l'information quantique, en particulier l'intrication, sont extrêmement sensibles aux perturbations et se dégradent rapidement lors de la propagation dans des milieux comme les fibres optiques. Cette fragilité provoque une perte progressive de cohérence, rendant difficile la distribution fiable d'états quantiques sur de grandes distances sans dispositifs spécifiques.

L'utilisation de répéteurs et d'amplificateurs classiques pour restaurer et renforcer le signal est impossible en mécanique quantique en raison du théorème de non-clonage, qui interdit de copier parfaitement un état quantique sans le détruire. Pour contourner cet obstacle des répéteurs quantiques sont en cours de développement. Il s'agit de dispositifs quantiques qui reposent sur la création d'états intriqués sur des segments courts et sur des opérations d'échange d'intrication[18] permettant d'étendre progressivement ces corrélations sur de plus longues distances, sans cloner ni mesurer directement l'état quantique transmis. Ces dispositifs permettent ainsi de dépasser les limites d'une liaison directe unique. Leur conception demeure toutefois complexe et coûteuse car elle requiert notamment l'intégration de mémoires quantiques fiables.

La stratégie nationale quantique identifie la startups française Welinq, issue de travaux pionniers menés au CNRS et à la Sorbonne, comme un acteur à fort potentiel susceptible de lever ce verrou technologique grâce aux solutions qu'elle développe.

Une autre solution complémentaire serait l'intégration de communications quantiques s'appuyant sur des satellites, qui profitent d'atténuations beaucoup plus faibles dans l'espace libre que dans les fibres optiques terrestres. L'utilisation de satellites en orbite terrestre basse a déjà permis de distribuer des paires de photons intriqués sur des distances dépassant plusieurs centaines de kilomètres. Cependant, ce type de solution comporte aussi des défis, notamment la courte durée de visibilité entre un satellite et des stations terrestres, les effets atmosphériques, et la nécessité d'une constellation de satellites pour assurer une couverture continue [40].

Une collaboration en cours entre Welinq, Qphox et la Sorbonne Meet-Q, vise à intégrer des processeurs quantiques et des technologies de réseaux quantiques optiques. L'objectif de ce projet est de permettre de relier des processeurs quantiques à des technologies de stockage quantique et à de répéteurs quantiques, qui sont essentiels pour l'interconnexion et la transmission de l'information quantique. Des avancées dans ce domaine pourraient ouvrir la voie au développement de centres de données quantiques, capables d'effectuer des calculs rapides, fiables et à grande échelle. Cette collaboration pourrait donc jouer un rôle clé dans la définition d'interfaces technologiques essentielles et dans le développement de réseaux quantiques.

[18] L'échange d'intrication est une opération quantique qui permet de prolonger l'intrication entre deux qubits distants en utilisant un qubit intermédiaire intriqué avec chacun d'eux

La communauté scientifique met en évidence plusieurs autres défis :

- Le coût et l'efficacité des ressources : développer des composants économiquement viables tout en maintenant des performances élevées constitue un défi majeur pour une adoption à grande échelle ;
- L'interopérabilité : assurer la compatibilité entre différentes technologies quantiques et entre les réseaux quantiques et les réseaux classiques. Grâce à des algorithmes spécifiques, il pourrait être possible de développer des interfaces hybrides assurant la compatibilité et l'interconnexion entre réseaux classiques et réseaux quantiques. Des travaux de normalisation pourraient contribuer à assurer la compatibilité de ces ainsi que la définition de protocoles de communication universels.

Le secteur de normalisation de l'Union internationale des télécommunications (ITU-T) a publié une recommandation appelée **Y.3800**, qui pose des bases pour les réseaux prenant en charge la **distribution de clés quantiques (QKD)**, un élément clé des communications quantiques sécurisées. Ce standard décrit notamment la **structure conceptuelle**, les **fonctionnalités fondamentales** et l'architecture de réseaux quantiques QKD. Cette norme aide à concevoir, déployer et exploiter des réseaux QKD, mais reste **au stade des architectures de base** pour l'instant.

L'institut des standards de télécommunications européen (ETSI[19]) a lancé un comité technique sur les technologies quantique (TC QT) avec plus de 90 participants visant à faire progresser le développement de technologies quantiques standardisées, en particulier dans le domaine de la conception de produits, et à contribuer à un avenir durable à l'échelle mondiale grâce à la cartographie de l'écosystème quantique et à la création d'un **Radar des technologies quantiques**.

Face à ces défis, les réseaux quantiques seront développés par étapes successives [37]. Les scientifiques proposent une feuille de route qui commence par le déploiement d'un réseau pré-quantique capable de transmettre des qubit entre deux nœuds et qui se termine par un réseau quantique capable d'offrir des services de calcul distribué. Selon la trajectoire estimée par ces chercheurs, des étapes intermédiaires de la feuille de route incluront l'ajout de mémoire quantique et l'intégration de répéteurs quantiques [41]. La version jeune des réseaux quantiques sera capable d'offrir des avantages immédiats aux systèmes classiques telles que la sécurité de la communication (ou aussi la QKD), et la synchronisation ultra précise. Le dernier, quant à lui, interviendra sur le long terme notamment pour connecter les processeurs quantiques permettant ainsi le calcul quantique distribué.

## 4.2. Le rôle des infrastructures numériques dans l'émergence des réseaux quantiques

Le développement des premiers réseaux quantiques terrestres qui viendraient répondre à des besoins de la QKD devrait pouvoir s'appuyer sur les réseaux en fibre optiques existants. En effet, des déploiements expérimentaux de réseaux quantiques ont démontré la capacité des réseaux fibres classiques à transmettre des données quantiques notamment pour l'envoi des clés QKD.

[19]The European Telecommunications Standards Institute

En outre, la coexistence de liens quantiques et classiques sur une même fibre offre, des avantages**,** tels que la réduction des coûts d'infrastructure, la simplification du déploiement et la flexibilité opérationnelle. Cette approche d'hybridation suscite l'intérêt d'équipes de recherche. Il a été démontré que la QKD peut théoriquement coexister avec des communications classiques en co-canal [42]. Toutefois, l'hybridation soulève des problématiques liés à la scalabilité. En effet, les caractéristiques quantiques imposent des contraintes de conception très différentes des réseaux classiques. Selon certains travaux de recherche, les réseaux hybrides représentent une étape intermédiaire vers un internet quantique complet [43].

A l'inverse, les satellites de télécommunication classiques n'apparaissent pas intrinsèquement compatibles avec la QKD. Des satellites spécifiques embarquant des dispositifs de communication par laser seraient nécessaires.

La Commission européenne, en partenariat avec certains Etats membres et l'Agence spatiale européenne travaille à la conception, au développement et au déploiement d'un réseau de communication quantique sécurisé couvrant l'ensemble de l'Union européenne, y compris ses territoires d'outre-mer : EuroQCI. Ce réseau fera partie d'IRIS² et sera composé, d'une part, d'un segment terrestre reposant sur des réseaux de communications en fibre optique reliant des sites stratégiques à l'échelle du continent européen et, d'autre part, d'une composante spatiale basée sur des satellites pour créer une infrastructure de communication quantique paneuropéenne.

Des collaborations industrielles, telles que celle initiée par SpeQtral et Thales Alenia Space, ou celle entre SES et l'agence européenne de l'espace (ESA), expérimentent déjà des communications quantiques par satellite, avec des tests conjoints entre orbite et stations sol.

A l'échelle internationale, des expérimentations sont en cours pour démontrer la faisabilité de la QKD sur la fibre. Parmi ceux-ci figurent notamment, le réseau quantique déployé par Cisco Systems et la start-up Qunnect qui transmet des signaux via des câbles en fibre optique entre Brooklyn et Manhattan, à New York [44] ou aussi le premier réseau à grande échelle chinois couvrant 3 700 km et permettant des communications parallèles entre 20 utilisateurs [45].

## 5. Stratégies quantiques nationales et européennes

Une course aux technologies quantiques est lancée depuis plusieurs années à l'échelle internationale. Le quantique est considéré comme un enjeu de souveraineté majeure au regard de ses impacts civils et militaires. Dans ce contexte, plusieurs Etats ont mis en place des stratégies et des politiques nationales afin de développer leurs écosystèmes nationaux et de stimuler les développements dans ce domaine en rapide évolution. Selon l'OCDE, dans un rapport de décembre 2025[20], on estimait à 55,7 milliards de dollars américains les fonds engagés dans la science et la technologie quantiques par les gouvernements du monde entier depuis 2013, principalement par les pays développés. L'organisation invite toutefois à interpréter ces montants avec prudence car les annonces gouvernementales intègrent le budget total prévu dans les programmes, pouvant inclure notamment des financements préexistants, ainsi des financements privés. Le marché mondial des technologies quantiques devrait atteindre 106 milliards d'ici 2040 selon un rapport de McKinsey de 2023. En novembre 2025, 18 pays

[20] 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

membres de l'OCDE, ainsi que l'Union européenne, avaient adopté des stratégies officielles permettant notamment de coordonner les financements déjà engagés et les différents programmes et initiatives. Les financements publics apparaissent nécessaires étant donné les délais longs et incertains de développement de la technologie, qui représente des risques importants pour les investisseurs privés. Ils concernent la recherche publique, du soutien à la recherche et développement des entreprises privées, le lancement de marchés publics ou encore le financement par capitaux propres. Les stratégies sont généralement coordonnées au niveau gouvernemental par l'intermédiaire d'un ou plusieurs ministères, avec le soutien d'agences publiques spécialisées dans la mise en œuvre des programmes spécifiques.

Ces stratégies comportent généralement une dimension relative à la coopération internationale. Cependant, les tensions géopolitiques actuelles, l'accent mis sur la sécurité nationale et l'autonomie stratégique notamment vis-à-vis des applications à double usage, et les restrictions en matière de transfert de technologies freinent la coopération et la collaboration supranationale. Ces préoccupations en matière de sécurité pourraient conduire à des écosystèmes plus cloisonnés et fermés à l'échelle de chaque pays, au détriment de la recherche scientifique internationale. Or, cette coopération peut contribuer à réduire les doublons, à amplifier l'impact des investissements publics et privés, bénéficier des économies d'échelle et créer des incitations plus fortes à investir dans la recherche et développement. Ces enjeux peuvent amener les gouvernements de trouver un équilibre entre l'ouverture des écosystèmes technologiques quantiques, qui favorise la collaboration et l'innovation, et la nécessité de prévenir les abus et les détournements. Selon l'OCDE, le paysage quantique évolue vers une collaboration sélective entre pays de confiance comme l'illustre le nombre croissant d'accords bilatéraux en matière de technologies quantiques au détriment d'accords plus globaux. Même entre pays partenaires, la collaboration s'étiole. A titre d'exemple, entre les Etats-Unis et les membres de l'UE, l'intensité de cette collaboration a diminué de 15% entre 2018 et 2022 dans le domaine des technologies quantiques, cette baisse reflétant une tendance mondiale plus large.

Les contraintes de la chaîne d'approvisionnement en matériaux et composants critiques, la concentration des investissements et le protectionnisme technologique pourraient également exacerber les divisions entre les pays en développement et les pays développés et accentuer « la fracture quantique » [14].

## 5.1. Axes de stratégies nationales différents selon les pays

**Stratégies de la Chine et des Etats-Unis**

Selon certains analystes, ces chiffres n'étant pas étayés par des statistiques officielles, la Chine aurait pris des engagements de financement public dépassant les 15 milliards de dollars américains, compensant le déficit de son secteur privé moins développé qu'aux Etats-Unis ou, dans une moindre mesure, qu'en Europe[21]. Le pays met l'accent depuis des années sur le domaine des communications quantiques, testant et déployant des réseaux de communication à distribution de clés quantiques (QKD). La Chine a notamment développé le plus long réseau de communication quantique au monde entre Pékin et Shangaï, soit une distance de 2000 km et établi la première connexion quantique par satellite en 2016 avec l'Autriche. Depuis lors, le pays a mis en place des liaisons par satellite vers l'Afrique du Sud et la Russie[22]. Le pays investit également dans les ordinateurs quantiques[23], avec des annonces récentes d'avancées majeures dans le calcul quantique utilisant des architectures

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

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

[23] L'ordinateur supraconducteur Tianyan-504, lancé en décembre 2024, est équipé d'une puce « Xiaohong » de 504 qubits

supraconductrices et photoniques[24]. L'approche de la Chine reste nationale et fermée avec une collaboration internationale limitée dans les publications de recherche et limite le partage de ses développements, reflétant ainsi une approche stratégique visant à développer un avantage concurrentiel dans les communications.

Les États-Unis apparaissent comme l'un des principaux financeurs des travaux dans le domaine de l'informatique quantique. De façon générale, les développements technologiques paraissent se situer à un stade plus exploratoire mais avec de potentielles applications dans de nombreux secteurs alors que la Chine semble se concentrer sur les applications les plus immédiates des communications quantiques. Le budget annuel du gouvernement américain alloué à la recherche et développement s'élève à environ 1 milliard de dollars depuis 2022 et bénéficie aux grands acteurs comme IBM, leader du domaine[25]. L'entreprise, qui a développé son premier ordinateur quantique en 2019, a lancé, en 2023, le processeur quantique Condor, le premier au monde à dépasser les 1 000 Qubits et prévoit de développer un ordinateur quantique commercial de 100 000 qubits d'ici 2033. En outre, les start-ups américaines bénéficient d'importants investissements privés. Selon un rapport de McKinsey de 2023, les investissements privés américains sont en tête du classement mondial avec plus de 2,3 milliards de dollars, surpassant notamment ceux de l'UE de plus de cinq fois (405 millions de dollars). Cette situation résulte de l'ampleur des capitaux disponibles et d'une culture d'investissement profondément attachée à la prise de risques qui favorisent l'innovation.

**Focus sur la stratégie européenne**

La stratégie « Quantum Europe », présentée par la Commission européenne en juillet 2025 [46], marque une étape clé pour faire de l'Union européenne un leader mondial du secteur quantique d'ici à 2030. Cette initiative s'inscrit dans un contexte où l'Europe possède une excellence reconnue dans la recherche scientifique et un écosystème dynamique de start-up, mais peine à transformer ce potentiel en succès économique **en raison notamment de la fragmentation des initiatives et d'un déficit d'investissements face aux États-Unis et à la Chine**.

La stratégie est structurée autour de cinq axes majeurs : la recherche et innovation, les infrastructures quantiques, le renforcement de l'écosystème européen, les technologies quantiques pour l'espace et la défense, et enfin le développement des compétences spécifiques. Parmi les mesures phares figurent la création d'un programme de recherche , de technologie et d'innovation pour harmoniser les efforts de l'UE et des Etats-membres pour soutenir la recherche fondamentale et le développement d'applications industrielles, la mise en place d'une installation de conception de processeur quantique et **six lignes pilotes de processeurs quantiques**, **lancement d'une installation pilote pour l'Internet quantique européen**, l'extension du nombre de pôles de compétences[26], et la création d'une Académie européenne des compétences quantiques. La stratégie prévoit aussi une feuille de route

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

[25] La stratégie américaine du quantique lancée en 2018 a pour objectif d'assurer le maintien du leadership américain. Elle contient six domaines politiques : la science, la main-d'œuvre, l'industrie, les infrastructures, la sécurité économique et la coopération internationale et couvre, à travers plusieurs projets dans les domaines des communications, des ordinateurs et des capteurs quantiques. Elle est soutenue par les lois sur l'autorisation de la défense nationale et la loi CHIPS et Science de 2022. Elle est coordonnée par plusieurs agences fédérales dont le National Institute of Standards and Technology, la National Science Foundation et le Department of Energy.

[26] *Quantum competence clusters,* en anglais. Il s'agit de centres régionaux qui fournissent des infrastructures et des services partagés, tout en mettant en relation les acteurs de la recherche et de l'industrie. On retrouve ces centres dans quelques régions européennes telles que la région métropolitaine de Paris, de Munich ou Barcelone entre outres. La Commission européenne souhaite donc investir dans la création des nouveaux centres et dans le renforcement des liens entre eux.

quantique dans le spatial en collaboration avec l'ESA et la participation à la feuille de route technologique pour l'armement.

Cette stratégie vient en complément du « Quantum Technologies Flagship » lancé en 2018. Il s'agit d'une initiative de recherche à grande échelle dotée d'un budget d'un milliard d'euros sur 10 ans financé par l'UE ainsi que d'autres financeurs publics, qui rassemble des instituts de recherche et des entreprises. Le projet finance aussi bien des projets à vocation commerciale dans les trois grands domaines des technologies quantiques (informatique, communication et détection) que la recherche fondamentale ou encore des activités d'éducation et de coopération internationale. Depuis 2021, le programme publie annuellement « 23 indicateurs de performance clés pour les technologies quantiques en Europe » et leur progression pour atteindre les objectifs fixés pour 2030 dans 6 domaines : l'écosystème, la communication quantique, l'informatique quantique, la simulation quantique, la détection et la métrologie quantiques et l'éducation.

Dans le domaine des communications quantiques, le projet euroQCI, mentionné dans la partie **4**, constitue l'un des principaux piliers de la stratégie de cybersécurité de l'UE visant à sécuriser les communications et les données des infrastructures critiques et des institutions gouvernementales. La Commission s'appuiera sur les avancées technologiques permises par le *Quantum Technologies Flagship*. Dans ce cadre, des projets nationaux sur le segment terrestre ont été financés avec l'objectif est de tester différentes technologies et protocoles et en les adaptant aux besoins spécifiques de chaque pays. Au niveau national, le projet France QCI, piloté par Orange, s'appuiera sur les infrastructures existantes dans les régions de Paris et de Nice pour tester les technologiques quantiques dont la QKD et les intégrer dans des réseaux télécom existants. Un réseau quantique sera également mis en œuvre à Toulouse pour la Direction générale de l'aviation civile française.

Par ailleurs, la commission envisage de publier en 2026 un « Quantum Act ». Son objectif principal sera d'encadrer et de stimuler – par des investissements publics et privés – le développement souverain et sécurisé des technologies quantiques dans l'UE, en favorisant un écosystème unifié, financé et coordonné à l'échelle européenne.

**Focus sur les initiatives françaises dans le cadre de France 2030**

Le plan d'investissement France 2030 vise à rattraper le retard industriel français, à investir massivement dans les technologies innovantes et à soutenir la transition écologique. Dans ce cadre, les technologies quantiques ont été identifiées comme stratégiques pour atteindre les objectifs fixés.

En 2021, la France a annoncé le lancement de la stratégie nationale pour les technologies quantiques[27], dotée d'un budget de 1,8 Md€ sur quatre ans, dont 1 Md€ financé par l'État. Cette stratégie s'articule autour de cinq objectifs stratégiques :

- Développer les technologies et les usages du calcul quantique
- Maîtriser les technologies de capteurs quantiques
- Développer et diffuser la cryptographie post-quantique
- Développer les technologies de communications quantiques
- Maîtriser les technologies habilitantes du quantique

Selon le gouvernement, parmi les réalisations permises par cette stratégie à ce stade figurent la création d'une vingtaine de start-up, des levées de fonds supérieures à 600 M€, ainsi qu'une part estimée à 20 % du marché mondial dans certains segments.

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

Par ailleurs, en 2024, le ministère des Armées, en partenariat avec le Secrétariat général pour l'investissement (SGPI), a lancé le programme Proqcima. Celui-ci vise à disposer, d'ici 2032, d'au moins deux prototypes d'ordinateurs quantiques universels de conception française. Doté de 500 M€, ce programme a conduit à la signature d'accords-cadres avec cinq start-up (Alice & Bob, C12, Pasqal, Quandela et Quobly) afin d'identifier et de développer des solutions pour la conception de ces ordinateurs. Proqcima est structuré sous la forme d'un partenariat d'innovation organisant une mise en concurrence progressive des entreprises participantes, avec une sélection graduelle des acteurs les plus performants.

# 6. Enjeux réglementaires et de régulation

Le développement de l'informatique quantique soulève des défis majeurs de régulation en termes de souveraineté, sécurité et d'accès.

## 6.1. La sécurité

La question des standards de cryptographie appelés à être imposés ou recommandés pourrait soulever plusieurs enjeux, tenant notamment aux critères de sélection des solutions, à leur calendrier d'adoption, aux modalités de leur déploiement ainsi qu'aux aux possibles risques de divergence entre les standards ayant vocation à être autorisés et ceux privilégiés par certains acteurs privés. Par ailleurs, les contraintes induites par le respect des référentiels de sécurité pourraient limiter l'étendue des solutions techniques susceptibles d'être retenues par les opérateurs et soulever des enjeux opérationnels pour ces acteurs.

A titre d'exemple, une éventuelle incompatibilité des standards de communication les plus anciens avec les nouvelles exigences de sécurité post quantique pourrait influencer, à moyen terme, les choix stratégiques des opérateurs télécoms quant au maintien ou au retrait de certaines générations de réseaux. Si certaines spécifications en cours d'élaboration notamment dans le cadre de la 6G paraissent d'ores-et-déjà s'orienter vers l'intégration native de mécanismes de sécurité « *quantum-safe* », les générations antérieures, reposant sur des primitives cryptographiques classiques, pourraient devenir progressivement moins conformes à des exigences de cybersécurité renforcées. Cela pourrait accélérer leur obsolescence réglementaire et économique.

## 6.2. L'informatique quantique en nuage

L'accès à la puissance de calcul quantique via des services d'informatique en nuage (*cloud*) pourrait soulever des enjeux réglementaires importants, notamment en matière de souveraineté, de concurrence et de gouvernance des technologies stratégiques, comme le souligne l'OCDE dans ses travaux récents sur les politiques des technologies quantiques [47]. L'Organisation met ainsi en évidence le risque d'une concentration du marché au profit d'un nombre restreint d'acteurs dominants, susceptible d'engendrer une dépendance stratégique et d'accentuer les inégalités d'accès à ces infrastructures avancées. En outre, l'OCDE insiste sur l'importance de la normalisation et de l'interopérabilité afin de prévenir les situations de verrouillage technologique (« *vendor lock-in* ») et de garantir une concurrence ouverte et équitable.

Enfin, le recours à des plateformes d'accès délocalisées à des calculateurs quantiques via l*e cloud* pourrait poser également des questions de souveraineté numérique et de sécurité des données, notamment lorsque les traitements sont effectués dans des juridictions différentes de celles des utilisateurs.

Dans ce contexte, l'émergence de services *cloud* tels que le « *Quantum Computing-as-a-Service* », qui permettent l'accès à distance aux capacités de calculs quantiques via le *cloud*, pourrait interroger sur la nécessité d'adapter le cadre réglementaire (en particulier la régulation des services de traitement de données issue du règlement sur les données) aux services quantiques, afin notamment de permettre un accès équitable et une concurrence effective entre services d'informatique quantique.

## 7. Conclusion

La conception et l'utilisation d'ordinateurs quantiques est encore dans une phase de recherche et de nombreux défis sont encore à relever avant un passage au stade industriel. Outre la nécessité de trouver un modèle économique pour les acteurs, il sera nécessaire de développer les algorithmes pertinents selon les cas d'usage, d'adapter les compétences des ingénieurs et experts dans les entreprises et dans les laboratoires de recherche, de permettre aux entreprises d'avoir accès aux centres de calcul regroupant ordinateurs quantiques et supercalculateurs et de favoriser le développement de l'offre et la demande en France et en Europe.

A court terme, les premiers cas d'usage des ordinateurs quantiques concerneront probablement d'autres secteurs que celui des télécommunications. Leur coût élevé, la complexité des infrastructures nécessaires et l'incertitude quant à la valeur ajoutée immédiate freinent encore l'intérêt des acteurs du secteur. Toutefois, à plus long terme, les réseaux télécoms pourraient accéder à des ressources de calcul quantique via des plateformes cloud quantiques, permettant d'externaliser certains traitements spécialisés intervenant dans la conception et la configuration des équipements et systèmes permettant d'assurer l'exploitation des réseaux.

Par ailleurs, l'enjeu le plus immédiat pour les télécommunications concerne l'anticipation des menaces des ordinateurs quantiques qui risqueront de fragiliser les schémas cryptographiques actuellement utilisés dans les réseaux. Ainsi, les infrastructures mobiles devront progressivement migrer vers des solutions résistantes aux menaces du quantique, dites *quantum safe*, en intégrant les recommandations de l'ANSSI qui encourage l'anticipation et la préparation de cette transition afin d'assurer la résilience des communications.

Les télécommunications joueront un rôle clé dans le déploiement des futures infrastructures quantiques, en particulier via les réseaux hybrides combinant fibres optiques classiques et canaux satellitaires. La première application concrète des réseaux quantiques répond à un besoin de sécurisation des communications ; toutefois, les réseaux quantiques restent globalement à un stade expérimental et vont se développer par étapes successives, chaque génération permettant l'émergence de nouvelles applications plus ambitieuses allant jusqu'au calcul quantique distribué. Ceci impliquera une évolution progressive vers des architectures hybrides combinant infrastructures classiques et liens quantiques.

Il est encore trop tôt pour prédire avec certitude l'ampleur exacte des transformations qu'apporteront les technologies quantiques au secteur télécom. Elles pourraient se limiter à renforcer et sécuriser les infrastructures existantes, ou bien ouvrir progressivement la voie à de nouvelles architectures de communication et à des performances améliorées, à mesure que les systèmes et algorithmes se développent. Dans tous les cas, la route vers ces perspectives reste jalonnée d'étapes expérimentales et de défis technologiques qui définiront le rythme et la nature de cette révolution. Le développement de standards et la définition d'une stratégie nationale et européenne cohérentes joueront un rôle clé pour orienter ces évolutions.

De plus, les stratégies nationales et européennes joueront un rôle déterminant dans l'accélération du développement des solutions encore embryonnaires. Elles permettront notamment de coordonner les différents acteurs de l'écosystème, de faciliter la mise en relation entre fournisseurs de solutions et

utilisateurs, et surtout de mobiliser les financements nécessaires pour garantir la soutenabilité économique des acteurs jusqu'à l'atteinte d'une maturité technologique suffisante. Ces initiatives revêtent ainsi une dimension stratégique majeure, en contribuant à préserver la souveraineté sur ce domaine.

Enfin le développement de l'ordinateur quantique, ayant vocation à s'appuyer largement sur des infrastructures d'informatique en nuage est susceptible de soulever des questions concernant le développement des infrastructures et les normes de sécurité adaptées notamment pour les données stockées dans le cloud. En particulier, la structuration économique de l'offre d'accès à la puissance de calcul via le cloud et son interaction avec l'écosystème des acteurs du cloud pourrait entrainer un risque de dépendance ou de contournement des exigences de sécurité et de résilience applicables aux fournisseurs de services d'informatique en nuage.

# Annexe I – Entretiens

**Entretiens**

Un cycle d'entretien a nourri notre réflexion sur les technologies quantiques. Pour autant, les positions prises dans cette note ne reflètent pas nécessairement les points de vue des personnes rencontrées ni des institutions auxquelles elles appartiennent.

Ont notamment été reçus en entretien :

- 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)
- CNRS

## Annexe II – Principaux éléments bibliographiques


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

[2] M. A. a. C. I. L. Nielsen, «Quantum computation and quantum information,» *Cambridge university press,* 2010.

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

[4] IBM, «QPU,» [En ligne]. Available: https://www.ibm.com/fr-fr/think/topics/qpu.

[5] IBM, «Quantum Computing,» [En ligne]. Available: https://www.ibm.com/fr-fr/think/topics/quantum-computing.

[6] A. d. Technologies, «État de l'art de l'ordinateur quantique tolérant aux fautes, questions et défis,» 2025.

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

[8] L. K. 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,» vol. 2, 2018.

[10] GENCI, «Calcul haute performance, intelligence artificielle et calcul quantique,» GENCI, [En ligne]. 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] M. A. a. C. I. L. Nielsen, «Quantum computation and quantum information,» *ambridge university press,* 2010.

[13] O. Ezratty, « Understanding Quantum Technologies,» 2024.

[14] OCDE, «Mapping the global quantum ecosystem,» 2025.

[15] H.-Y. a. B. M. a. C. J. a. C. S. a. L. J. a. M. M. a. N. H. a. B. R. a. K. R. a. P. J. a. M. J. R. Huang, «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. [En ligne]. 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. [En ligne]. Available: https://www.vodafone.com/news/newsroom/technology/vodafone-partners-with-orca-computing-to-model-future-networks-in-minutes-using-quantum-technology.

[20] L. K. Grover, « fast quantum mechanical algorithm for database search,» *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing,* 1996.

[21] L. a. C. L. a. J. S. a. L. Y.-K. a. M. D. a. P. R. a. P. R. A. a. S.-T. D. Chen, «Report on post-quantum cryptography,» *US Department of Commerce, National Institute of Standards and Technology,* 2016.

[22] R. L. a. S. A. a. A. L. Rivest, «A method for obtaining digital signatures and public-key cryptosystems,» *Communications of the ACM,* vol. 21, 1978.

[23] H. t. f. 2. b. R. i. i. 8. h. u. 2. m. n. qubits, «How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits,» *Quantum,* 2021.

[24] C. a. F. P.-A. a. S. A. chevignard, «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. a. C. L. a. D. O. a. D. J. a. F. J. a. G. N. a. H. D. a. J. T. a. L. N. a. M. M. a. o. Campagna, «Quantum Safe Cryptography and Security: An introduction, benefits, enablers and challenges,» *European Telecommunications Standards Institute,* 2015.

[27] D. a. M. R. a. M. M. a. T. J. a. P. F. D. a. L. O. a. L. S. a. H. J. a. V. P. a. H. R. Joseph, «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. [En ligne].

[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. a. M. Y. a. S. L. a. Z. L. a. L. X.-B. a. G. D. a. G. Y. a. L. J. a. T. Y.-L. a. T. S.-B. a. o. Wang, «Long-distance transmission of quantum key distribution coexisting with classical optical communication over a weakly-coupled few-mode fiber,» *Optics express,* vol. 28, n° %19, 2020.

[39] M. J. a. A. O. a. B. S. a. J. G. T. a. S. H. a. P. P. a. P. F. a. K. G. T. a. R. J. a. N. R. a. o. Clark, «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, n° %11, p. 181, 2025.

[40] J. a. K. P. a. O. D. Meister, «Simulation of satellite and optical link dynamics in a quantum repeater constellation,» *EPJ Quantum Technology,* vol. 12, n° %11, 2025.

[41] S. a. Q. B. a. M. G. a. K. R. a. S. A. DiAdamo, «Packet switching in quantum networks: A path to the quantum internet,» *Physical Review Research,* 2022.

[42] Y. a. W. B.-X. a. Z. C. a. W. G. a. W. R. a. W. H. a. Z. F. a. N. J. a. C. Q. a. Z. Y. a. o. Mao, «Integrating quantum key distribution with classical communications in backbone fiber network,» *Optics express,* 2018.

[43] J. M. a. P. N. A. a. Q. B. Lukens, «Hybrid classical-quantum communication networks,» *Progress in Quantum Electronics,* 2025.

[44] Cisco, «Quantum Networking: How Cisco is Accelerating Practical Quantum Computing,» [En ligne]. Available: https://blogs.cisco.com/news/quantum-networking-how-cisco-is-accelerating-practical-quantum-computing?dtid=osscdc000283&linkclickid=srch.

[45] Y. W. H. J. X. e. a. Zheng, « Large-scale quantum communication networks with integrated photonics,» *Nature,* 2026.

[46] Commission européenne , «Quantum Europe Strategy: Quantum Europe in a Changing World,» 2025.

[47] OECD, «la National Academies of Sciences dans Quantum Computing: Progress and Prospects,» 2025.

[48] P. W. 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 Mars 2023. [En ligne]. Available: https://postquantum.com/quantum-computing/use-cases-telecom/.

[52] NIST, «practical-quantum-enhanced-receivers-classical-communication,» 20 Avril 2021. [En ligne]. 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,» septembre 2020. [En ligne]. 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.