
Quantique : vers une logique de marché

NOTE D'ACTION - OCTOBRE 2024




Think tank de référence en France et en Europe, l'Institut Montaigne est un espace de réflexion indépendant au service de l'intérêt général. Ses travaux prennent en compte les grands déterminants économiques, sociétaux, technologiques, environnementaux et géopolitiques afin de proposer des études et des débats sur les politiques publiques françaises et européennes. Il se situe à la confluence de la réflexion et de l'action, des idées et de la décision.

NOTE D'ACTION - Octobre 2024

Quantique : vers une logique de marché



Les notes d'action de l'Institut Montaigne identifient un enjeu spécifique et formulent des recommandations opérationnelles à destination des décideurs publics et privés.



**Note
d'éclairage**

Se situer
et rendre
intelligible notre
environnement

**Note
d'enjeux**

Poser des
constats et
identifier des
problématiques

**Note
d'action**

Formuler
des recom-
mandations
opérationnelles

**Opération
spéciale**

Sonder,
chiffrer,
expérimenter

Rapport

Analyser
et proposer
collégalement
des solutions
de long terme

*Il faut qu'une porte
soit ouverte ou fermée*

Alfred de Musset

Les technologies quantiques représentent une révolution en devenir : elles offrent pour la première fois un langage informatique capable de coder des systèmes complexes jusque-là impossibles à modéliser, et d'y associer de nouvelles logiques mathématiques. Si ces technologies n'ont pas vocation à irriguer l'ensemble des domaines scientifiques, elles marquent néanmoins un tournant décisif. En effet, elles permettent de passer d'une logique de découverte accidentelle, souvent fondée sur des approches par essai-erreur, à une capacité de prédiction systématisée sur des problématiques aujourd'hui impossibles à modéliser avec les outils classiques. **Une économie qui manquerait ce virage risquerait de se retrouver marginalisée alors que les autres puissances investissent massivement dans les technologies quantiques.**

Aujourd'hui, la France est bien positionnée tant sur le plan scientifique qu'en matière d'exportation de ses infrastructures et de son matériel quantique :

- Sur le plan scientifique, la France, grâce à l'excellence de sa recherche fondamentale et à la vitalité de son écosystème entrepreneurial, a su faire émerger quatre des six technologies quantiques les plus prometteuses : les atomes neutres, les photons intriqués, les supraconducteurs et les systèmes spin/silicium.
- Sur le plan de la commercialisation de ses infrastructures et de son matériel quantique, les acteurs français détiennent 28% des parts de marché des infrastructures quantiques mondiales, principalement concentrées sur les processeurs, rivalisant ainsi directement avec les *leaders* américains.

L'Europe dispose en outre d'avantages significatifs sur la chaîne de valeur des technologies quantiques, susceptibles de conforter son avance. Parmi ces atouts figurent notamment les émulateurs quantiques, capables de simuler le comportement de qubits sur des

machines quantiques, et ainsi d'acculturer les acteurs au développement de solutions quantiques.

Ces atouts sont pourtant menacés par deux éléments principaux :

- 1. La quasi absence d'acteurs français sur des segments de marché essentiels à la construction d'une offre quantique à vocation internationale, notamment ceux des intergiciels et des logiciels quantiques.** Aucune entreprise française n'a, à ce jour, réussi à commercialiser des outils de développement quantique, contrairement à des acteurs canadiens, autrichiens, israéliens ou encore allemands. **Sur les 85 startups spécialisées dans le logiciel quantique créées à travers le monde, seulement cinq sont françaises, et ces dernières représentent moins de 1 % des 1,6 Md \$ investis dans ce secteur au niveau mondial.**

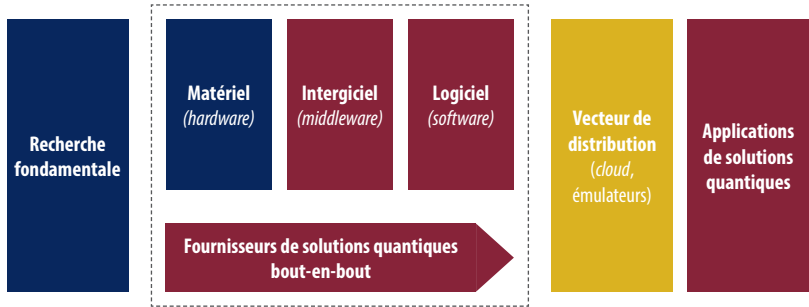
Sur le plan mondial, les montants investis par les pouvoirs publics à l'échelle internationale ont dépassé les 40 Mds \$ en 2024, avec un marché projeté entre 106 Mds \$¹ à 850 Mds \$ à horizon 2030². **En outre, les investissements des États-Unis semblent plus efficaces que ceux des européens : alors que l'Europe et les États-Unis représentent respectivement près de 30 % du marché du quantique, les États-Unis y ont seulement investi 3 Mds €, soit moins de la moitié des 7 Mds € investis par les Européens³.** Cette situation est d'autant plus regrettable que le marché du logiciel quantique, centré sur les solutions B2B (*business-to-business*), correspond précisément à un domaine où l'Europe bénéficie d'avantages comparatifs significatifs pour faire émerger des acteurs globaux intégrant l'ensemble de la chaîne de valeur.

¹ Source : Qureca, avril 2024, *Quantum Initiatives Worldwide*.

² Source : *étude du BCG de 2022 qui a été actualisée pendant l'été 2024*.

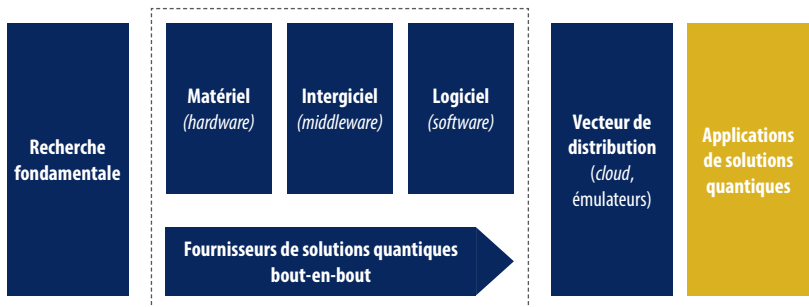
³ Source : *BCG, L'informatique quantique : la course que l'Europe ne doit pas perdre, 2022*.

Graphique n° 1 • Positionnement des acteurs français sur la chaîne de valeur quantique



- Acteurs français en position dominante
- Acteurs français présents mais insuffisamment compétitifs
- Acteurs français quasi absents du marché

Graphique n° 2 • Positionnement des acteurs américains sur la chaîne de valeur quantique



- Acteurs américains en position dominante
- Acteurs américains présents mais insuffisamment compétitifs

- 2. Des sources de financement de la stratégie nationale quantique trop rigides pour accompagner les mutations d'un marché en devenir. Lors de l'étape 1 du plan quantique, une majorité des 1,8 Md€ mobilisés** provenaient de reconductions de programmes ministériels, de co-financements industriels et de financements européens. **Seuls 650 M€ représentaient une véritable marge de manœuvre budgétaire pour les pouvoirs publics.**

Cette note propose dès lors des recommandations stratégiques et actionnables, prêtes à être mises en œuvre dans le cadre de l'étape 2 de la stratégie nationale quantique. L'objectif est de pallier ces problèmes et d'éviter de reproduire les erreurs du passé, où la France a perdu son avantage technique initial faute d'avoir su valoriser ses atouts.

Trois leviers : la consolidation de l'offre technologique française et européenne, sa rentabilisation pour qu'elle réponde à un besoin de marché, et la mise en œuvre d'une gouvernance politique qui soutiendra son développement sans le freiner.

- 1. De manière prioritaire, les pouvoirs publics doivent consolider l'offre technologique quantique française que nos acteurs ont su développer en optimisant les programmes existants, en stimulant l'investissement privé et en formant la prochaine génération d'experts.**

Cette orientation nécessite d'abord d'optimiser le programme Proqcima, géré par la Direction générale de l'Armement (DGA). Celui-ci a pour mission de retenir les deux technologies de qubits les plus prometteuses pour être passées à l'échelle dans l'industrie. Une fois ces technologies choisies, le programme pourrait prévoir de les confier à des laboratoires communs aux méthodes éprouvées, afin de gérer l'industrialisation dans un contexte d'incertitude scientifique. Il est également essentiel d'ajouter des mesures d'impact à Proqcima pour suivre l'évolution des avancées technologiques et, en fonction de celles-ci, permettre une réversibilité des choix technologiques.

Ensuite, il apparaît impératif de développer des systèmes d'interconnexion entre ordinateurs quantiques afin de garantir leur interopérabilité, une fois que les usages offrant un avantage quantique auront été définis. Cela exige une stratégie de normalisation alignée avec les réalités d'un marché où c'est l'usage des technologies qui définit les normes. En plus de renforcer la présence française au sein des instances de normalisation telles que l'IEEE, il est essentiel de s'assurer de la participation active des acteurs français et européens aux projets *open-source* majeurs, qui deviennent aujourd'hui des standards *de facto*.

Enfin, des ajustements financiers et humains sont nécessaires pour soutenir le développement de l'informatique quantique. Étant donné que les investissements publics dans ce domaine dépassent largement les investissements privés, il est crucial d'aligner les financements publics avec les contributions privées, notamment en incitant les grands groupes industriels à acquérir des *startups* quantiques. Pour renforcer la masse salariale dédiée à la recherche quantique, des décisions stratégiques doivent être prises par les directeurs de laboratoires, telles que la création de chaires dirigées par des experts internationaux. Enfin, l'intégration de la logique non binaire (dite « non booléenne ») dans les programmes scolaires, notamment au cycle 4 en informatique, est essentielle pour préparer les élèves à modéliser les problématiques quantiques.

2. En parallèle, il est impératif de construire une offre quantique qui réponde à un besoin réel du marché, en accompagnant le développement d'acteurs compétitifs sur tous les segments de la chaîne de valeur du quantique. Bien que la France bénéficie d'une avance technologique sur le matériel quantique, la majorité des projets en cours se trouvent encore au stade de preuve de concept (POC), y compris au niveau mondial. Cela est dû au fait que peu d'acteurs français et européens se situent aujourd'hui sur les segments de l'intergiciel (*middleware*) et du logiciel (*software*) quantiques. Afin de préparer l'émergence des avantages tangibles de la technologie quantique et d'orienter les choix stratégiques des décideurs publics et privés,

l'Institut Montaigne a identifié les usages les plus prometteurs des technologies quantiques actuelles, notamment le calcul intensif, les capteurs et la communication quantique. Il est difficile de prédire précisément les domaines où les avantages quantiques se concrétiseront, mais il est certain que les technologies quantiques vont durablement transformer le marché du *High Performance Computing* (HPC). En effet, l'incertitude porte essentiellement sur le niveau de performance des futurs calculateurs quantiques et sur la montée à l'échelle des technologies habilitantes associées⁴. Néanmoins, tous les scénarios prospectifs montrent qu'il y aura *a minima* une coexistence entre des machines de type NISQ et des machines analogiques dans les centres HPC. Dans les scénarios les plus optimistes, les processus industriels seront durablement impactés, que ce soit dans le cadre d'une arrivée de processeurs de type FTQC ou d'un « saut quantique », avec des architectures modulaires permettant d'interconnecter des FTQC entre eux.

- 3. Enfin, il convient d'assurer un pilotage efficace de ces ambitions avec une gouvernance politique et scientifique qui soutienne le développement quantique sans le freiner.** Actuellement, la responsabilité politique est trop diluée, avec une exécution souvent laissée à la Coordination Nationale, seule chargée des décisions budgétaires. Ce manque de clarté dans les rôles – entre décision, exécution et évaluation – se complique davantage avec les trois comités de France 2030 (orientation, suivi, lisibilité), plaçant l'informatique quantique parmi les 30 priorités stratégiques, contrairement aux approches plus ciblées du Royaume-Uni ou des États-Unis. Sur le plan scientifique, pour une intégration efficace des technologies quantiques, il est crucial de les cartographier et de les combiner avec d'autres technologies existantes ou émergentes, afin de réduire les coûts et de faciliter la commercialisation. En 2023, le SGPI a initié avec l'Académie des Technologies une feuille de route technologique quantique

⁴ Source : [Rapport d'avril 2024 du CEA et de Futurible « Quantum 2042 : étude prospective sur les impacts du calcul quantique en 2042 »](#).

nationale, visant à partager les risques dès les phases préliminaires du développement technologique, qui va dans cette direction et gagnerait à être actualisée régulièrement.

Synthèse des propositions

Objectif 1

Affiner notre stratégie de sécurisation de la technologie quantique française pour mieux articuler la recherche fondamentale et le passage à l'échelle.

RECOMMANDATION 1

Confier à Proqcima, reconnu à l'échelle européenne comme l'acteur le plus légitime en la matière, l'identification et la sécurisation de la technologie française la mieux adaptée à une offre compétitive militaire et civile à l'échelle de l'Europe. Piloté par la direction générale de l'armement (DGA), Proqcima doit sélectionner les deux technologies françaises de qubits les plus performantes, prêtes à passer à l'échelle industrielle. Pour assurer l'efficacité de cette sélection, il est essentiel de :

- Confronter les 2 technologies françaises retenues aux technologies européennes d'égale maturité ;
- Rendre Proqcima plus dynamique en confiant les technologies à des laboratoires communs, en intégrant des mesures d'impact adaptées et en permettant à QuLoop de suivre les technologies non sélectionnées pour garantir une réversibilité en cas d'évolution de leur maturité ;
- Réserver les technologies les plus performantes pour des usages militaires et régaliens, afin de protéger les avancées françaises.

Objectif 2

Mettre en œuvre à l'échelle européenne une stratégie de normalisation intégrant des standards techniques français.

RECOMMANDATION 2

Conscient de la nécessité de prioriser les solutions tout en veillant à ne pas se faire imposer *de facto* des standards structurés par d'autres, inciter les acteurs français et européens à contribuer aux programmes *open-source* internationaux dans lesquels il y a un intérêt commercial à être contributeur.

RECOMMANDATION 3

À long-terme, et au sein des instances internationales de normalisation, dans le cadre du programme MetriQs France, définir une stratégie de normalisation à partir des acteurs et des technologies françaises et européennes en matière de normes de calcul, normes de sécurité et de compatibilité des technologies habilitantes et protocoles de communication entre infrastructures quantiques.

Objectif 3

Embarquer les investisseurs privés à hauteur des financements publics.

RECOMMANDATION 4

Mettre en place des incitations ciblées pour les grandes entreprises françaises afin d'encourager les acteurs du capital risque et du capital

croissance à investir dans le quantique, incluant des avantages fiscaux de type CIR pour les acquisitions de jeunes pousses quantiques, des indicateurs de performance valorisant ce type d'acquisitions et la création d'un fonds de capital-risque multiples entreprises (*multi corporate venture*) dédié à l'achat de startups quantiques au moment de la série B.

Objectif 4

Faire du secteur quantique un domaine d'attrait pour les jeunes talents français et internationaux.

RECOMMANDATION 5

Mettre en place des chaires quantiques dans les laboratoires de recherche fondamentale et appliquée généraux aux méthodologies éprouvées.

RECOMMANDATION 6

Intégrer des compétences fondamentales faisant appel à la logique mathématique non binaire (dite logique non booléenne) dans les programmes mathématiques révisés du cycle 4 qui seront prochainement publiés par le Conseil Supérieur de Programmes.

Objectif 5

Construire une offre quantique qui réponde à un besoin pour créer un marché rentable.

RECOMMANDATION 7

Confier à la Direction Générale des Entreprises (DGE), qui se situe au cœur de l'écosystème quantique, le soin de diffuser aux entreprises et aux investisseurs une feuille de route recensant les usages quantiques dans lesquels investir de manière à en retirer des avantages concurrentiels. Ces usages concernent prioritairement :

1. Le calcul intensif avec les applications qui font appel à de *l'explosion combinatoire et du calcul en parallèle* dans 4 secteurs prioritaires :
 - a. Chimie / pharmaceutique avec la conception automatisée de processus de synthèse et la modélisation de molécules pour détecter des pathologies de manière plus précoce ;
 - b. Industrie manufacturière / transport avec l'optimisation des routes de transport ou de la logistique avec des processus intelligents ;
 - c. Énergie / développement durable avec le pilotage des infrastructures d'énergies renouvelables, des réseaux électriques et des systèmes de stockage sensibles aux aléas climatiques ;
 - d. Finance (banque / assurance) avec l'optimisation de la gestion de portefeuille et l'analyse de corrélations de plus en plus complexes entre les différents facteurs de risque du marché.

2. Les capteurs avec les applications pour lesquels des progrès de mesure restent à faire ou pour lesquels il n'existe pas d'outils de mesure :
 - a. Dans le secteur militaire, il s'agit de s'affranchir de la dépendance au GPS dans les lieux connus et explorer des lieux encore inconnus ;
 - b. Dans le civil, il s'agit d'améliorer, avec des capteurs quantiques, les techniques d'imagerie médicale telles que les IRM et la tomographie, les techniques de détection et de modélisation de phénomènes complexes (systèmes autonomes, systèmes environnementaux, outils d'observation spatiale).

3. Les communications quantiques, avec la sécurisation de nos réseaux existants et l'anticipation des réseaux d'un « monde post quantique » :
 - a. Dans le secteur militaire, remplacer urgemment les algorithmes de chiffrement existants basés sur la factorisation de nombres premiers ou sur les courbes elliptiques par des algorithmes résistants aux algorithmes de Shor et veiller à empêcher la collecte de données cryptées ;
 - b. Dans le civil, favoriser le dépôt de brevets français et européens sur les distributions de clés quantiques (QKD) afin de mieux anticiper les mutations des réseaux de connectivité et résister au monopole des réseaux dits « post-quantiques » que confèrent actuellement les brevets chinois et américains.
 - c. Favoriser l'interopérabilité des clés de distribution quantique au service d'un futur réseau quantique européen terrestre et satellitaire via le projet européen EuroQCI et l'expertise des opérateurs télécom et des fournisseurs de solutions de sécurité.

RECOMMANDATION 8

Accélérer la production d'intergiciels (sur la base d'émulateurs ou de plateformes cloud existantes) pour tester des avantages quantiques en situation réelle. Pour cela, lancer un programme de partenariats public-privé, s'appuyant sur le centre HPC de *France Hybrid HPC Quantum Initiative* (HQI) financé par le PIA 4 afin de tester les usages bénéficiaires du quantique et sur l'appel à projet de Bpifrance « *Advanced Quantum Understanding: Implementing Large-Scale Applications* » (AQUILA), voué à diffuser les technologies quantiques dans les environnements industriels.

RECOMMANDATION 9

En parallèle du développement d'une offre stratégique telle que décrite dans la recommandation 7, démontrer aux acteurs financiers les avantages d'une offre quantique afin d'inciter à la création et au développement d'un écosystème applicatif dédié au quantique en Europe.

Objectif 6

Militer pour une gouvernance simple et agile adaptée à la maturité du secteur.

RECOMMANDATION 10

Passer de 6 à 2 instances de gouvernance de la stratégie quantique, l'une dédiée à la réflexion stratégique et l'autre à l'exécution opérationnelle, en confiant au Comité exécutif actuel (émanant des ministères concernés) la responsabilité totale de la stratégie quantique nationale et des financements à y allouer, et en fusionnant le Conseil Consultatif Scientifique et Technique avec le Comité Opérationnel de la stratégie nationale quantique, et l'utiliser pour renforcer la Coordination Nationale en la dotant ainsi d'un Comité d'exécution sur le modèle britannique.

RECOMMANDATION 11

Actualiser tous les deux ans la *roadmap* technologique pilotée par l'Académie des Technologies afin de permettre un ajustement des politiques technologiques dans le temps industriel.

Louise Frion

Louise Frion est **responsable de projets nouvelles technologies** à l'Institut Montaigne depuis février 2024. Louise a notamment été rapporteure du rapport *Blockchain : consolider nos atouts* et de la note *Mobiliser et former les talents du numérique* publiés en 2023. Louise a auparavant travaillé en banque d'investissement chez Lazard Londres en 2017, à la Direction générale du Trésor en 2018, au cabinet du Secrétaire d'État au Numérique en 2020 et chez Capgemini Invent en tant que consultante secteur public. Elle a par ailleurs fondé Medici&Cie, un cabinet de conseil et de formation spécialisé dans la stratégie technologique des entreprises et des administrations publiques.

Louise enseigne les technologies émergentes et leurs applications industrielles au programme MBA/EMBA de HEC Paris. Elle est diplômée du programme Grande École de l'EMLyon et d'un master II en affaires publiques de l'École Normale Supérieure et Paris 1 Panthéon Sorbonne.

« Les notes de l'Institut Montaigne reposent sur une méthodologie collégiale. Nous remercions les experts issus des secteurs publics et privés qui ont contribué à la réflexion. »

Synthèse	6
-----------------------	---

Introduction	22
---------------------------	----

1

L'ambition et les résultats de la stratégie nationale	29
--	----

1.1. Une approche incrémentale initiée par des chercheurs visionnaires	29
---	----

1.2. Une ambition politique croissante qui s'intéresse à la chaîne de valeur quantique	40
---	----

1.3. Une avance technologique réelle, mais une offre encore émergente	45
--	----

1.4. Un contexte international instructif qui motive une approche française plus offensive sur les priorités et simple sur les structures de pilotage	53
--	----

2

La nécessité de consolider l'offre technologique	56
---	----

2.1. En la sécurisant dans la lignée de Proqcima	56
---	----

2.2. En diffusant les standards français à l'échelle européenne	67
--	----

2.3. En alignant l'investissement public avec l'investissement privé	76
---	----

2.4. En attirant et en formant les bons talents	80
--	----

3	Une méthode pour porter un marché haut de gamme avec cette offre	89
	3.1. Déployer une offre quantique française	
	à vocation internationale	90
	a. Adresser prioritairement les applications de calcul intensif pour la simulation de systèmes complexes et pour optimiser des grands systèmes	91
	b. Investir dans les capteurs quantiques et la métrologie pour améliorer les outils de mesure classiques	106
	c. Anticiper les mutations qui seront générées par les communications quantiques pour la cybersécurité	109
	d. Veiller à la matérialisation effective des avantages quantiques sur ces usages	113
	3.2. Rentabiliser l'offre quantique	116
	a. Mettre des intergiciels quantiques performant à la disposition des entreprises, condition de recours aux technologies quantiques, à l'aide de partenariats choisis	117
	b. Inciter à la création et au développement d'un écosystème applicatif dédié au quantique en Europe	121
4	L'importance d'une gouvernance qui accompagne sans freiner	125
	4.1. Au niveau politique, des responsabilités trop diluées	126
	4.2. Au niveau scientifique, des partages de <i>roadmap</i> encore trop ponctuels	129

5	Plan d'action stratégique et opérationnel	132
	Objectif 1	
	Affiner notre stratégie de sécurisation de la technologie quantique française pour mieux articuler la recherche fondamentale et le passage à l'échelle	134
	Objectif 2	
	Mettre en œuvre à l'échelle européenne une stratégie de normalisation intégrant des standards techniques français	135
	Objectif 3	
	Embarquer les investisseurs privés à hauteur des financements publics	137
	Objectif 4	
	Faire du secteur quantique un domaine d'attrait pour les jeunes talents français et internationaux	138
	Objectif 5	
	Construire une offre quantique qui réponde à un besoin pour créer un marché rentable	139
	Objectif 6	
	Militer pour une gouvernance simple et agile adaptée à la maturité du secteur	145
	Annexes	149
	Remerciements	153

Le 7 juin dernier, l'année 2025 a été proclamée Année Internationale de la Science et de la Technologie Quantique (AIQ) par les Nations unies qui ont ainsi souhaité attirer l'attention du public sur les potentialités d'une nouvelle ère technologique. En 2025, nous célébrerons également le centenaire de la découverte de la mécanique quantique, une révolution silencieuse mais inéluctable qui transforme notre manière d'utiliser l'ordinateur, d'interagir et de traiter l'information.

La mécanique quantique, souvent considérée comme l'une des théories les plus complexes de la physique, est en réalité le moteur de nombreuses innovations qui façonnent notre quotidien. Contrairement à la mécanique classique, qui décrit le comportement des objets à l'échelle macroscopique, **la mécanique quantique se concentre sur l'échelle microscopique**⁵. Elle a déjà profondément influencé notre environnement, en permettant des inventions comme le GPS, le laser, ou encore le transistor. Par exemple, le GPS utilise des horloges atomiques à bord de ses satellites qui fonctionnent grâce aux transitions quantiques des atomes. Ces transitions permettent de mesurer le temps et de déterminer des positions de manière extrêmement précise et avec exactitude.

Pour fonctionner, l'ordinateur quantique utilise des qubits et non des bits, qui sont l'unité de base de l'informatique quantique. Pour comprendre, dans un ordinateur classique, les informations sont codées en bits qui sont soit dans l'état 1, soit dans l'état 0. C'est très utile pour coder le fonctionnement d'objets de manière binaire, comme l'interrupteur par exemple, qui peut être soit allumé (1), soit éteint (0), mais pas les deux en même temps (0 et 1). En généralisant, quasiment tous les média (texte, image, vidéo, son) peuvent ainsi être codés de façon binaire, avec donc de très longues séquences de bits (0 ou 1). Mais le traitement de ces séquences de bits devient rapidement extrêmement coûteux lorsqu'il

⁵ En décrivant des particules subatomiques et leurs interactions.

faut considérer toutes les combinaisons possibles de 0 et de 1 : les qubits permettent alors non seulement de gagner du temps, mais aussi de réfléchir à de nouvelles manières de coder. Par exemple, pour sortir d'un labyrinthe, un système binaire implique de tester chaque solution possible une par une, ce qui peut être très chronophage. En revanche, un système quantique permettrait de tester tous les chemins du labyrinthe simultanément et de coder les différents états associés au fil de l'eau, afin de trouver la sortie beaucoup plus rapidement.

À terme, c'est donc une révolution exponentielle, car la perspective de coder une part toujours plus importante de notre environnement dans un nouveau langage plus puissant, pourrait transformer en profondeur nos systèmes informatiques et notre rapport au monde. Pour cela, il faut produire toujours plus de qubits, dits « physiques », qui sont les unités de base, pour produire des qubits, dits « logiques », qui sont les qubits fiables protégés des erreurs en raison de leur stabilité. Les progrès en ce sens sont réguliers, et les acteurs respectent les temporalités affichées dans leurs *roadmaps*. En 2019, Google aurait momentanément atteint la suprématie quantique, soit le moment où les performances d'un ordinateur quantique dépassent intrinsèquement celles d'un ordinateur classique, avec son ordinateur Sycamore doté de 54 qubits physiques, et IBM a réalisé des avancées majeures successives, en 2021 avec son processeur Eagle à 127 qubits physiques, et en 2023 avec son processeur Osprey à 433 qubits physiques. **Concrètement, ces processeurs sont aujourd'hui utilisés pour construire des algorithmes de calcul pouvant traiter en parallèle un nombre exponentiel de données, des capteurs pouvant se passer de la dépendance au GPS, et des solutions de cryptographie plus fiables que les systèmes de clés asymétriques que nous utilisons aujourd'hui et résistants aux nouveaux algorithmes de calcul quantique.**

De leur côté, la France et l'Europe, depuis près de 5 ans, développent des ordinateurs et des capteurs quantiques mondialement reconnus. Ils ont conquis un avantage concurrentiel et une position de

leader technique sur ce marché, au même titre que les États-Unis et la Chine. En outre, la France a fait émerger trois prix Nobel en mécanique quantique en 25 ans : Claude Cohen-Tannoudji en 1997, Serge Haroche en 2012 et Alain Aspect en 2022.

Les projections du marché de la technologie quantique vont de 106 Mds \$⁶ à 850 Mds \$⁷ d'ici à 2040. Néanmoins, l'étude du BCG montre que les États-Unis ont la part de marché la plus élevée, à hauteur de 27 %, suivis du Royaume-Uni, à hauteur de 16 %, de l'Union européenne, à hauteur de 14 %, et du Canada, à hauteur de 12 % et de la Chine à hauteur de 11 %. À titre de comparaison, la France avait 3 % de part de marché, derrière l'Allemagne à 5 % et le Japon à 7 %. Cette position ne rend pas hommage au **leadership technique de la France en matière d'informatique quantique. En effet, la France a développé des expertises spécifiques sur le traitement de particules (atomes ou photons), l'efficacité des opérations associées et la correction d'erreurs dans des environnements sensibles au « bruit »**⁸. Chaque technologie développée se singularise par le fait qu'elle obtient de meilleurs résultats que les *leaders* américains, en utilisant moins de ressources de calcul, sur des composantes spécifiques. Par exemple, les « qubits de chat de Schrödinger » développés par l'entreprise Alice & Bob ont permis d'activer une méthode de correction d'erreurs plus naturelle, dites « passives », et des états intrinsèquement robustes contre certaines formes de bruit, qui permettent de consommer moins de ressources que les codes de surface utilisés par IBM (*Cf infra*). Néanmoins, le code de surface est doté d'une architecture plus simple⁹

⁶ Qureca, *Quantum Initiatives Worldwide*, avril 2024.

⁷ BCG, *Can Europe Catch Up with the US (and China) in Quantum Computing?*, 2022 (actualisé à l'été 2024)..

⁸ La notion de bruit en informatique quantique fait référence aux interférences ou perturbations non désirées qui affectent les signaux, les processus ou les données informatiques. Concrètement, cela se traduit par des données, des signaux ou des perturbations qui ne sont pas utiles et qui peuvent interférer avec les opérations en cours. En informatique quantique, on parle de « décohérence » et d'« erreurs de portes ».

⁹ L'organisation des qubits en grille bidimensionnelle permet de limiter les interactions avec les qubits voisins, ce qui fait que les seules interactions avec les voisins immédiats sont nécessaires pour corriger une erreur.

et très scalable¹⁰, ce qui peut se révéler à terme plus efficace pour passer à l'échelle l'ordinateur quantique et le rendre interopérable avec d'autres technologies.

En somme, la France a développé des avantages comparatifs pour faire mieux avec moins, mais comme trop souvent dans son histoire, elle n'a pas encore trouvé la clé pour passer à l'échelle et valoriser ces avancées sur le marché mondial. Cette clé consiste aujourd'hui à optimiser l'offre technologique française, la rentabiliser pour qu'elle réponde à un réel besoin de marché et à mettre en œuvre une gouvernance politique et scientifique qui soutiendra son développement sans la freiner.

L'informatique quantique rappelle en effet un paradoxe français en matière de nouvelles technologies : si les acteurs français savent être créatifs et ingénieux pour faire advenir des technologies de rupture et de pointe, ils le sont moins pour les commercialiser à l'échelle mondiale et prendre des parts de marché. En informatique surtout, mais aussi de manière plus large dans l'industrie, malgré des découvertes majeures, cela s'est traduit par des échecs successifs de pénétration du marché mondial ; pour n'en citer que quelques-uns : le réseau Cyclades en 1971, le langage de programmation Prolog précurseur en IA en 1972, le réseau Cyclades à commutation de paquets de 1973, le Minitel en 1982, le système expert SYMPA en 1983 pour optimiser la gestion industrielle avec des techniques d'IA, ou encore la méthode de méta-compilation¹¹ OCalm de 1996. De fait, si ces systèmes étaient très avancés sur le plan technique, ils étaient soit trop spécifiques à un marché particulier ; soit en concurrence avec des standards globaux plus simples et agiles comme Java, Python ou TCP/IP ; soit trop complexes pour être adoptés largement.

¹⁰ Pour augmenter le nombre de qubits logiques, il suffit juste d'augmenter le nombre de qubits physiques dans la grille, ce qui permet au dispositif de croître de manière régulière et prévisible. Cela correspond de plus bien aux systèmes de qubits physiques disponibles aujourd'hui.

¹¹ Ce type de méthode permet de générer du code automatiquement et d'adapter le code dynamiquement à de nouvelles situations en modifiant son comportement ou en ajoutant de nouvelles fonctionnalités.

Un exemple emblématique de génie français mal valorisé

Le réseau Cyclades¹², développé par Louis Pouzin en 1971, est aussi un exemple emblématique du potentiel français pour innover et concevoir des systèmes de pointe, sans rencontrer la demande espérée sur le marché, en raison de choix politiques mal orientés.

Cyclades était un réseau de communication novateur, basé sur la technique du datagramme pour transmettre les données. Cette innovation technologique consistait à fragmenter les informations en paquets, qui étaient ensuite envoyés de manière indépendante les uns des autres. Contrairement aux circuits virtuels qui nécessitent une connexion préalable, le datagramme offrait une approche sans connexion, permettant une transmission plus rapide et plus flexible. Il représentait une évolution naturelle du télégraphe, en introduisant une méthode de communication qui ne dépendait pas de l'ordre d'arrivée des paquets.

En 1975, Cyclades connecte 25 ordinateurs répartis en France, en Italie et au Royaume-Uni, et, l'année suivante, il devient opérationnel. Cependant, le projet a été abandonné en 1978, à la suite d'une décision politique. En particulier, les décideurs publics ont considéré que Cyclade comportait un « vice de conception » car il envoyait des données dans un ordre aléatoire. Ils n'ont pas vu que c'était en réalité la force de ce réseau, qui permettait de le rendre plus rapide et moins coûteux à mettre en œuvre. Cette technique d'envoi de données dans un ordre aléatoire a ensuite été adoptée par les Américains Vinton Cerf et Robert Kahn pour développer le protocole TCP/IP, qui constitue aujourd'hui la base de l'Internet.

¹² Cf *Comédies Françaises de Éric Reinhardt*, 2020.

Cette note formule des pistes d'action pour ne pas reproduire les mêmes erreurs avec la technologie quantique, avantage compétitif français que nous avons su développer mais qu'il nous reste encore à commercialiser et à valoriser.

Conscient des enjeux, en 2021, **l'Élysée a souhaité doter la France d'une stratégie nationale quantique** dans un cadre européen. Trois ans plus tard, **force est de constater que cette stratégie en a encore du mal à s'incarner** dans un marché mondial et que les réflexes pavloviens de focalisation sur la recherche et non sur les applications commercialisables risquent de nous priver d'un potentiel stratégique à la fois en termes de souveraineté, de croissance et de compétitivité. **Pourtant, l'élan de la v2 de la stratégie quantique a bel et bien été lancé en ce sens, mais l'enveloppe budgétaire actuelle ne permet ni de la financer à hauteur des besoins, ni de servir de catalyseur à l'investissement privé, encore insuffisant pour maintenir l'ambition de 2021.** En 2021, des experts de l'Institut Montaigne¹³ avaient déjà alerté sur le risque de saupoudrage des investissements publics annoncés et sur la nécessité de les orienter vers la demande pour permettre à l'écosystème naissant de croître.

À titre de comparaison, notre approche de l'IA est un bon repère des possibles. Les Américains ont investi prioritairement dans les infrastructures de transport et de traitement (suivis rapidement par les Chinois) et ont ensuite capitalisé sur elles pour construire leurs briques techniques aux fins de conquête commerciale, avec une approche « de bout en bout ». Les Français, ne maîtrisant pas les composants et systèmes d'infrastructure, sont aujourd'hui dépendants de partenariats commerciaux. Ainsi, une entreprise comme Mistral, à la pointe de l'innovation, doit composer avec un partenaire américain, en l'occurrence Nvidia pour l'infrastructure de traitement.

¹³ Florian Carrière et Théophile Lenoir, *Informatique quantique : construire un écosystème pour le futur*, Institut Montaigne, 2021.

Dans les infrastructures quantiques, la France et quelques pays européens ont un avantage comparatif technologique – de la même manière que les *hyperscalers* américains dans les années 2000 pour le *cloud computing*.

Notre maîtrise des infrastructures quantiques nous donne la possibilité de façonner le marché, de construire nos propres barrières à l'entrée et de nous positionner au meilleur niveau mondial – à condition, bien sûr, de **ne pas rester confiné à un exercice de recherche et de développement, mais bien de nous inscrire dans une stratégie d'industrialisation et un modèle économique vertueux et pérenne.**

Afin de pouvoir valoriser et développer plus encore notre technologie quantique, d'en faire véritablement un champion mondial – ce que notre excellence technologique justifie, l'Institut Montaigne a souhaité retenir des erreurs passées un certain nombre de points d'attention à traiter impérativement et sans délai. Ils concernent prioritairement :

- **la sécurisation de la technologie** et sa transformation en une offre compétitive;
- **les enjeux de normalisation** européenne à partir de standards techniques;
- **la question des financements privés** en complément des investissements publics existants;
- **la formation, l'attractivité et la rétention des talents** pour maintenir et exploiter tout le potentiel de notre avance technologique;
- **le façonnage d'un marché d'offre rentable**, gage de compétitivité et de développement pragmatique;
- **la nécessité d'une gouvernance adaptée à la maturité du secteur.**

L'Année Internationale de la Science et de la Technologie Quantique sera une occasion unique de sensibiliser le public et les décideurs à ces nouvelles réalités. La révolution quantique est en marche. Allons au bout de nos ambitions, et donnons-nous les moyens d'en saisir les opportunités!

1 L'ambition et les résultats de la stratégie nationale

1.1 UNE APPROCHE INCRÉMENTALE INITIÉE PAR DES CHERCHEURS VISIONNAIRES

L'informatique quantique investit le champ de l'infiniment petit pour repousser les limites actuelles du calcul, de la sécurité de l'information, et de nos capacités à simuler des problèmes complexes. Ses bases théoriques ont été formulées dans les **années 1980 par Richard Feynman¹⁴ et David Deutsch¹⁵** qui ont démontré la possibilité de concevoir des systèmes quantiques pour simuler des systèmes complexes et exécuter des calculs hors de la portée de nos capacités actuelles. En **1994, Peter Shor** a développé un algorithme capable de trouver rapidement les facteurs premiers d'un nombre, en utilisant un temps de calcul qui augmente raisonnablement avec la taille du nombre, et non de manière extrêmement rapide comme on le pensait auparavant. Or, la robustesse des systèmes cryptographiques actuels repose sur l'hypothèse selon laquelle trouver ces facteurs premiers prendrait énormément de temps, un temps dit « exponentiel ». Cette découverte a donc montré qu'un jour l'informatique quantique pourrait briser nos systèmes de sécurité actuels. De fait, la robustesse des systèmes de cryptographie à clé publique comme le Rivest-Shamir-Adleman (RSA)¹⁶ reposent aujourd'hui sur notre difficulté à factoriser des grands nombres dans un temps réduit¹⁷. En

¹⁴ Prix nobel de physique en 1965, il a élaboré la première théorie de la fission nucléaire avec Niels Bohr dans les années 1930, et reste un des pionniers de la théorie des trous noirs en relativité générale et de la cosmologie quantique.

¹⁵ À l'origine de l'algorithme de Deutsch qui montre que les ordinateurs quantiques peuvent surpasser les ordinateurs classiques sur certains types de problèmes.

¹⁶ Systèmes de chiffrement utilisant une clé publique pour chiffrer les données et une clé privée pour les déchiffrer. Dans un tel système, la clé publique est constituée de deux grands nombres premiers multipliés ensemble pour former un produit appelé « module ». La clé privée est dérivée de ces nombres premiers. Pour déchiffrer un message, il faut donc retrouver ces deux nombres premiers à partir du module, qui est complexe si les nombres sont très grands.

2001, les laboratoires de recherche d'IBM et de Stanford ont réalisé les premières démonstrations expérimentales de l'algorithme de Shor, ce qui a marqué une étape importante dans la validation pratique de la théorie de Feynman et Deutsch.

Par le traitement simultané de toutes les réponses possibles à un problème donné, ces chercheurs ont eu l'intuition géniale que des calculs en parallèle pourraient permettre de résoudre plus rapidement des problèmes complexes (dits non-polynomiaux (NP)¹⁸) ou dont la complexité croît de manière exponentielle (dit non-polynomiaux (NP) complets¹⁹). Plus de 300 problèmes NP complets sont recensés à ce stade. Il est important de noter que l'informatique quantique n'a toutefois pas le potentiel de résoudre tous les problèmes, en particulier ceux qui reposent sur de la force brute²⁰. Néanmoins, les perspectives offertes sur les problèmes NP et NP complets sont porteuses pour résoudre des problèmes d'optimisation ou d'algèbre linéaire plus rapidement.

D'autres scientifiques ont ensuite prouvé que l'infiniment petit était une échelle exploitable pour modéliser et résoudre plus précisément des problèmes réels. En 1982, le physicien français et prix Nobel Alain Aspect a réalisé une série d'expériences qui ont montré de manière incontestable que les prédictions de la mécanique quantique sont correctes, soit une validation expérimentale de la possibilité d'exploiter des phénomènes infiniment petits. Ainsi, des particules intriquées, comme des photons, peuvent rester connectées instantanément même à grande distance l'une de l'autre. Cela confirme empiriquement la violation des inégalités de Bell, et confirme l'hypothèse de Bohr sur la non-localité de

¹⁷ Cf le rapport de Florian Carrière et Théophile Lenoir, *Informatique quantique : construire un écosystème pour le futur* (Institut Montaigne, 2021), sur la sécurité et l'informatique quantique.

¹⁸ Par exemple, le fait de vérifier qu'une séquence d'ADN se retrouve bien dans plusieurs gènes.

¹⁹ Par exemple, le fait de remplir son sac ou son coffre de manière optimale pour respecter une contrainte de temps, sans avoir à tester toutes les solutions possibles.

²⁰ Soit le fait de tester une à une toutes les combinaisons possibles pour arriver à résoudre un problème, comme la répartition exacte des nombres premiers (hypothèse de Riemann).

particules intriqués (*détaillées dans l'encadré infra*). Les **inégalités de Bell de 1964** étaient considérées comme le principal obstacle à la matérialisation de la mécanique quantique, car elles établissent des contraintes pour toute théorie basée sur des hypothèses de localité²¹ et de réalisme²² incompatibles avec les corrélations observées en mécanique quantique. Alain Aspect et ses équipes ont réalisé des expériences avec des photons intriqués en mesurant leur polarisation à des angles variés pour tester empiriquement les limites des inégalités de Bell. Les résultats obtenus ont montré des corrélations plus fortes que celles autorisées par les inégalités de Bell, violant ainsi ces inégalités de manière incontestable.

Aux origines de la mécanique quantique

La mécanique quantique trouve son origine dans un débat philosophique entre Albert Einstein et Niels Bohr sur la notion de localité. En 1925, Einstein, Podolsky et Rosen ont formulé le paradoxe dit EPR, qui remettait en question la nature de la réalité et de la mesure en physique quantique. Ils se sont demandés si des particules liées entre elles (ou intriquées) pouvaient instantanément s'influencer l'une l'autre, même à distance, et donc, si une information pouvait se propager plus rapidement que la vitesse de la lumière. Pour Einstein, tout phénomène est forcément « local », c'est-à-dire lié à la position des molécules dans l'espace, conformément aux principes de la relativité restreinte²³. Une telle possibilité impliquerait donc l'existence de « variables cachées », encore inconnues des physiciens. Pour Bohr, il n'y a

²¹ *Les interactions ne peuvent pas se propager plus rapidement que la vitesse de la lumière.*

²² *Les propriétés des objets existent indépendamment de leur mesure.*

²³ *Selon cette théorie, un objet n'est influencé uniquement par son environnement immédiat, ce qui signifie que les interactions ne se produisent qu'entre objets voisins dans l'espace. Ces interactions doivent se limiter à la vitesse de la lumière ou moins.*

toutefois pas forcément de médiation entre l'espace et le temps (« non-localité »). Deux particules intriquées peuvent ainsi maintenir une corrélation instantanée indépendamment de la distance qui les sépare. Si la non-localité ne viole pas nécessairement la relativité restreinte, elle remet en question le lien de corrélation entre l'espace et le temps pour décrire notre espace-temps. Ainsi l'espace-temps pourrait être envisagé comme un réseau de corrélations dites quantiques, plutôt que comme une collection de points indépendants. Cela suggère qu'il pourrait exister des dimensions autres que le spatio-temporel, des réalités parallèles ou des niveaux d'existence que nous ne pouvons même pas concevoir avec notre compréhension actuelle.

Le débat entre Albert Einstein et Niels Bohr renvoie à deux grandes notions techniques essentielles pour comprendre la mécanique quantique : la superposition et l'intrication.

- **La superposition est à considérer à l'échelle d'une seule unité de base de l'informatique quantique, soit une abstraction mathématique qui permet de représenter l'information pour ensuite la stocker et la traiter dans le système (en l'occurrence le qubit, Cf *infra*)** : elle permet à une unité d'information d'exister simultanément dans une combinaison linéaire de deux états. Une particule peut être en même temps « ici » et « là », ou plus largement une de ses propriétés (le spin notamment, qui est une propriété intrinsèque des particules quantiques qui détermine leur comportement dans un champ magnétique) peut prendre plusieurs valeurs « en même temps » avec une certaine probabilité. En revanche, dès qu'on mesure la position (ou le spin) du qubit, cette superposition disparaît : il se met dans un état final (on parle alors de « décohérence quantique », ou de « réduction du paquet d'ondes »).

- **L'intrication est à considérer à l'échelle de plusieurs unités de base de l'informatique quantique, soit plusieurs qubits** : c'est un principe par lequel deux ou plusieurs unités d'information ne peuvent être décrites indépendamment de l'état des autres unités d'information, même si elles sont situées à grande distance les unes des autres. Concrètement, cela signifie que si l'on agit sur l'un des qubits, l'autre va être modifié instantanément, et exactement de la même façon : il s'agit donc d'une propriété très contre-intuitive, qu'Einstein lui-même n'a jamais vraiment acceptée (il pensait que des variables cachées expliquaient ce comportement). Les expériences scientifiques conduites ultérieurement ont confirmé que l'intrication quantique est réelle et exploitable. Pour tester empiriquement l'existence de « variables cachées locales », John Bell a mis au point des inégalités en 1964, qui sont des contraintes mathématiques devant être respectées pour expliquer les comportements d'intrication basés sur des variables cachées locales. Le prix Nobel 2022 français Alain Aspect et ses équipes ont ensuite réalisé plusieurs expériences pour tester ces inégalités sur des particules intriquées²⁴. Les résultats ont montré des corrélations qui violaient les inégalités de Bell confirmant ainsi la réalité physique de l'intrication des particules, et ouvrant la voie à de nombreuses manières d'exploiter la technologie quantique.

Pour qu'un système quantique fonctionne dans un environnement réel, le défi clé est de maintenir la superposition et l'intrication quantique le plus longtemps possible, pour pouvoir tester le système.

²³ L'expérience consistait à changer l'orientation d'appareils de mesure – les polariseurs – pendant que les photons se déplacent depuis leur source. Cela implique de changer les orientations en quelques nanosecondes, ce qui pose d'importants défis scientifiques. Comme l'état du polariseur est décidé au cours de l'expérience, il n'est pas possible que les photons communiquent entre eux tout du long, ce qui remettrait en question ce principe d'intrication.

Plusieurs difficultés se posent aujourd’hui :

- Les situations de **décohérence** qui font perdre aux qubits leur état de superposition en raison de leur interaction avec l’environnement (fluctuations électromagnétiques, vibrations mécaniques, températures trop élevées, etc.), témoignant de la fragilité intrinsèque des états quantiques, qui doivent être complètement isolés de leur environnement pour être manipulés ;
- Le **bruit thermique, électromagnétique** ou **de fond** peut perturber les qubits physiques, car ils ne peuvent pas être copiés pour redondance²⁵, mais nécessitent des techniques spécifiques pour corriger et détecter les erreurs sans perturber l’état quantique (codes de stabilisateur, opérations correctives, etc.) ;
- Des **erreurs de contrôle** peuvent survenir lors de la manipulation de qubits, en raison d’un manque de précision dans l’application des portes quantiques, qui permettent d’effectuer des opérations en qubits, et d’erreurs de synchronisation entre calculs quantiques ;
- Des **interactions non désirées entre qubits** pendant les opérations peuvent aussi survenir, car les qubits doivent être couplés pour réaliser des opérations quantiques, et les interactions croisées sont difficiles à contrôler et éliminer.

Une fois ces barrières levées, il est possible de créer des **qubits logiques** qui sont **stables** et créés à partir de plusieurs **qubits physiques corrigés d’erreurs**. Le nombre de qubits physiques nécessaires pour réaliser un qubit logique dépend fortement de la technique de correction d’erreurs utilisée et du niveau de correction souhaité contre les erreurs. Le **code de surface** utilisé par IBM et Google nécessite 100 à 1 000 qubits physiques pour chaque qubit logique, tandis que les **cat qubits**²⁶ utilisés par Alice & Bob permettent de n’utiliser que 20 à 50 qubits physiques pour chaque qubit logique en adaptant les codes de surface pour faciliter la correction

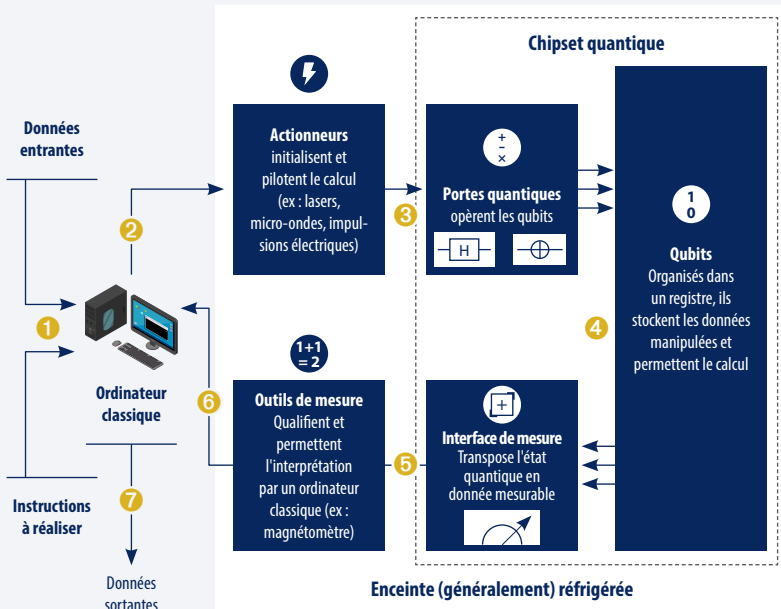
²⁵ En raison du théorème de non clonage, formulé par William Wootters et Wojciech Zurek en 1982, qui interdit la copie exacte d’états quantiques inconnus.

²⁶ Qubits basés sur des états de chats de Schrodinger qui exploitent des états de superposition cohérents les uns avec les autres.

d'erreurs localisée (par des structures en treillis où chaque qubit participe à la détection d'erreur de qubits adjacents). Des entreprises comme IBM, Google et D-Wave sont en mesure de proposer des ordinateurs quantiques dans leur cloud aujourd'hui en utilisant les codes surface.

Schéma de principe d'un ordinateur quantique

Ce schéma vise à montrer comment l'informatique quantique complète l'informatique classique, car il a besoin aussi de composantes de l'informatique traditionnelle pour fonctionner.



Source : Étude Wavestone x France Digitale, 2019, « L'Informatique quantique : prêt pour le grand saut ? ».

Comprendre les portes quantiques

Les portes quantiques sont des opérations qui modifient l'état des qubits de manière déterministe et réversible, en utilisant des matrices unitaires, garantes de la réversibilité de l'opération. Ce sont les interfaces entre les qubits et les technologies habilitantes, qui permettent à ces qubits d'être transposés à l'échelle macroscopique. Sur le plan mathématique, elles peuvent être simples (Hadamard, Pauli) ou multi qubits (CNOT, Toffoli). Le caractère réversible de la porte est fondamental pour garantir la conservation de l'état quantique tout au long de l'opération. Ce sont les briques fondamentales qui permettent de construire des circuits quantiques complexes, tels que l'algorithme de Shor pour la factorisation ou l'algorithme de Grover pour la recherche non structurée. Contrairement aux portes classiques, les portes quantiques permettent de faire du calcul en parallèle de manière massive en exploitant les spécificités de l'informatique quantique.

Si la France n'a pas les moyens d'explorer autant de technologies de qubits que les États-Unis, la France est toutefois en avance sur 4 des 6 technologies quantiques les plus prometteuses. En particulier, les atomes froids pour Pasqal, les photons intriqués pour Quandela, les supraconducteurs pour Alice&Bob, le silicium / spin pour Quobly et C12. Concrètement, cela se matérialise aujourd'hui par des processeurs quantiques dans des laboratoires²⁷, qui sont pour l'instant aussi gros, voire plus gros, que les premiers ordinateurs du début des années 1990. Pour fonctionner, les qubits ont besoin d'être contrôlés par un ensemble de technologies dites « habilitantes » comme le laser, les lentilles, les miroirs

²⁷ À l'Institut d'Optique de Palaiseau pour Pasqal, au Centre de nanosciences et de nanotechnologies de Palaiseau pour Quandela, au Laboratoire de physique de l'ENS pour Alice&Bob, au CEA-LETI pour Quobly et au laboratoire Coulomb de Montpellier pour C12.

ou encore la cryogénie. Ce matériel n'est exploitable que s'il est contrôlé par un « logiciel embarqué », qui correspond au système d'exploitation du processeur quantique.

Tableau n° 1 • Technologies explorées pour produire des qubits et habilitantes associées utilisées par les acteurs quantiques français

Acteur	Technologie de qubit	Technologie habilitante
Pasqal	<p>Atomes froids (ou atomes neutres piégés) : atomes ayant été refroidis à une température proche du zéro absolu, utilisés pour les simulateurs quantiques. Ils permettent de construire des particules toutes identiques entre elles, soit des « atomes neutres », dont les interactions peuvent ainsi prendre plusieurs formes.</p> <p>Les atomes sont composés d'autant d'électrons que de protons.</p>	<ul style="list-style-type: none"> • Système de refroidissement laser pour atteindre la température de zéro absolu. • Réseaux optiques pour piéger. • Technique de contrôle laser pour manipuler les atomes. • Systèmes ultra vides pour minimiser les interactions indésirables avec l'environnement.
Quandela	<p>Photons intriqués : systèmes qui permettent de maintenir des qubits stables, par le biais de composants optiques (faisceaux diviseurs, miroirs, modulateurs de phase, ou encore rotateurs de polarisation), de lasers et autres sources de lumière spécifiques. Ce dispositif est facilement intégrable sur des puces de semi-conducteurs, et donc adapté pour des applications de télécommunication quantique, car facilement transmissible sur longue distance via de la fibre optique.</p> <p>Ils n'exigent pas de systèmes de réfrigération à basse température.</p>	<ul style="list-style-type: none"> • Sources de photons uniques, comme des boîtes quantiques²⁸ ou des cristaux non linéaires. • Circuits optiques intégrés pour manipuler les photons. • Détecteurs de photons sensibles.

²⁸ En lien avec les travaux des Nobels de chimie Alexei Ekimov, Louis Brus et Mounqi Bawendi sur les « quantum dots », une des rares manifestations macroscopique de la mécanique quantique. Elles permettent d'obtenir une gamme colorimétrique beaucoup plus riche, pour servir la recherche biomédicale, améliorer la performance des lasers, etc.

Acteur	Technologie de qubit	Technologie habilitante
Alice & Bob	<p>Supraconducteurs : contrairement aux pièges à ions qui utilisent des lasers, les systèmes supraconducteurs utilisent des courants et des champs électromagnétiques micro-ondes pour manipuler les qubits.</p> <p>Ils peuvent être miniaturisés et intégrés dans des puces, similaires à la technologie des semi-conducteurs, et nécessitent aussi des températures proches du zéro absolu.</p>	<ul style="list-style-type: none"> • Réfrigérateurs cryogénique à dilution pour atteindre des températures très basses. • Techniques de nanofabrication pour fabriquer les circuits de supraconducteurs. • Électronique de contrôle à très basse température pour manipuler les qubits.
Qobly	<p>Qubits de spin en silicium : le silicium est un élément chimique abondant, le deuxième après l'oxygène. Il est moins sujet au « bruit quantique » que d'autres matériaux, ce qui peut potentiellement conduire à des temps de cohérence plus longs pour les qubits.</p> <p>De plus, l'utilisation du silicium est attrayante pour intégrer la technologie quantique avec les technologies de semi-conducteurs existantes et éventuellement permettre une plus grande scalabilité, car elle pourrait utiliser les techniques de fabrication à grande échelle de l'industrie des semi-conducteurs.</p>	<ul style="list-style-type: none"> • Techniques de fabrication de semi-conducteurs conventionnelles. • Systèmes ultra-vides pour minimiser les défauts de surface et améliorer la cohérence des spins.
C12	<p>Spin d'électrons : souvent pratiqué sur des nanostructures en silicium (<i>Cf. supra</i>), il s'agit d'un mouvement angulaire mécanique basé sur la rotation d'une masse (en l'occurrence le silicium), pour réaliser des états quantiques (superposés ou intriqués). Les spins des électrons sont manipulés à l'aide de champs magnétiques ou électriques, qui permettent de contrôler les états quantiques.</p> <p>La lecture de l'état d'un qubit de spin se fait en mesurant le spin de l'électron, souvent par des techniques qui exploitent la résonance magnétique.</p>	<ul style="list-style-type: none"> • Techniques de fabrication de nanotube de carbone de haute pureté. • Système de lecture de spins utilisant des champs magnétiques et micro-ondes. • Réfrigération cryogénique pour maintenir les conditions de spin cohérentes. • Systèmes ultra vides pour améliorer la pureté et la stabilité des nanotubes de carbone.

Autres technologies de qubits utilisées par des acteurs internationaux

Les ions piégés : cette approche utilise des ions chargés comme qubits, soit des particules atomiques ou moléculaires. Concrètement, les ions sont maintenus en suspension dans un vide et isolés par des champs électromagnétiques, d'où le terme de « pièges à ions ». Pour manipuler ce type d'états quantiques, il faut des lasers spécifiques, qui frappent les ions pour les maintenir « entrelacés » le plus longtemps possible. Cela exige des techniques d'isolation sophistiquées pour minimiser les interactions entre les ions et les molécules d'air, et parfois de la cryogénie à titre expérimental (technologie utilisée par IonQ).

L'ordinateur topologique : ordinateurs fonctionnant avec « anyons », soit des particules qui gardent en mémoire tout échange de position ou mouvement au cours du temps. Cela permet de créer des qubits très stables et plus résistants aux erreurs (technologie utilisée par Amazon et Google).

Aujourd'hui, environ 70 ordinateurs quantiques sont opérationnels dans le monde²⁹. Le principal défi technologique des technologies de fabrication de qubits peut s'appréhender comme deux faces du problème de la cohérence d'un système quantique : d'une part, il faut pouvoir enchaîner un maximum d'opérations complexes avec un faible taux d'erreurs, et d'autre part, il faut maintenir l'intrication le plus longtemps possible en isolant les qubits un maximum. En somme, il s'agit de fabriquer un maximum de qubits physiques sans bruit thermique (à l'origine des erreurs) et décohérence (à l'origine du caractère non exploitable des qubits).

²⁹ Gouvernement.

Pour résoudre ce problème, les acteurs doivent passer deux fois à l'échelle :

- 1. Verticalement avec des systèmes de correction d'erreurs de qubits actifs³⁰;**
- 2. Horizontalement avec des systèmes d'interconnexion entre ordinateurs quantiques pour garantir leur interopérabilité une fois que les usages seront débloqués et identifiés³¹.**

1.2. UNE AMBITION POLITIQUE CROISSANTE QUI S'INTÉRESSE À LA CHAÎNE DE VALEUR QUANTIQUE

Ces découvertes ont eu un écho majeur dans les programmes d'investissement publics sur la scène mondiale. Les montants investis par les pouvoirs publics ont dépassé les 40 Mds \$ en 2024 avec un marché projeté entre 106 Mds \$³² à 850 Mds \$³³, les gains recouvrant à la fois de nouveaux marchés et des optimisations opérationnelles.

Dès 2016, la Commission européenne publiait un *Quantum Manifesto*³⁴, qui s'est ensuite concrétisé en 2018 par l'initiative *Quantum Flagship Technologies*³⁵ dotée de 1 Md€ sur 10 ans. Déjà, l'objectif était de « soutenir la transformation de la recherche européenne en applications commerciales ». Cet objectif a été réaffirmé en 2019 par le Rapport Forteza, Hertaman, Kerenidis³⁶ qui soutenait que « cette révolution (...) ne peut se

³⁰ Comme par exemple le Orion Alpha Device de Pasqal composé de 3 millions de portes logiques opérationnelles (il en faut 200 millions pour atteindre le pallier des 128 qubits logiques).

³¹ Comme par exemple Welling, qui permet de connecter les ordinateurs quantiques sur toute la pile logicielle pour augmenter la performance d'ensemble du « système ».

³² Qureca, Quantum Initiatives Worldwide, avril 2024.

³³ BCG, Can Europe Catch Up with the US (and China) in Quantum Computing?, 2022 (actualisé à l'été 2024).

³⁴ Quantum Europe Conference, Quantum Manifesto, 2016.

³⁵ Commission européenne, The EU'S Quantum Technologies Flagship, 2022.

³⁶ Paula Forteza (dir.), Quantique : le virage technologique que la France ne ratera pas, 2019.

passer d'industriels réalisant des investissements importants et testant ces nouvelles innovations ». La même année, la National Academy of Sciences, Engineering and Medicine des États-Unis insistait sur le potentiel transformateur des applications commerciales de l'informatique quantique³⁷ dans son rapport Quantum Computing Progress and Prospect³⁸.

En France, le président de la République a donc présenté une stratégie nationale quantique dotée de 1,8 milliard d'euros en 2021 à l'Université Paris-Saclay dans une approche de partenariat public-privé pour « bâtir un destin et un avenir sur notre territoire ». Cette stratégie est, depuis, portée par Neil Abroug, ancien directeur du programme ICT et nanosciences du CEA. **Deux axes majeurs ont structuré le discours du 21 janvier 2021³⁹ : la souveraineté et l'anticipation des ruptures technologiques.** Sur la souveraineté, l'ambition était de sécuriser toutes les composantes de la chaîne de valeur quantique (recherche, technologie, industrie). Sur l'anticipation des ruptures technologiques, il s'agissait de s'assurer de notre résilience face aux crises futures en ayant innové au bon moment, comme sur l'IA, les risques sanitaires, et les risques climatiques. Ainsi, la maîtrise de nos technologies quantiques s'incarnait dans un programme de R&D intégré de la recherche fondamentale à l'industrialisation (i) et dans le renforcement de l'écosystème d'innovation français dans son environnement européen en attirant les meilleurs talents (ii). *In fine*, cette stratégie visait avant tout à garder la maîtrise des composantes essentielles de la chaîne de valeur quantique. Par conséquent, les technologies quantiques avaient été incluses dans le décret IEF⁴⁰ en tant qu'actifs stratégiques à part entière⁴¹.

³⁷ *Optimisation, finance, chimie, cryptographie, intelligence artificielle, entre autres.*

³⁸ *National Academies of Sciences, Engineering, and Medicine, Quantum computing, 2019.*

³⁹ *Emmanuel Macron, Présentation de la stratégie nationale sur les technologies quantiques, 2021*

⁴⁰ *Direction générale du Trésor, Les secteurs d'activités dans lesquels les investissements sont soumis à autorisation préalable, 2023.*

⁴¹ *Ce qui signifie qu'elles font partie d'un secteur d'activité dans lequel les investissements sont soumis à une procédure d'autorisation préalable, car ils se rattachent directement à la protection de la Défense nationale.*

L'objectif de la phase 1 du plan quantique français était ainsi de construire une filière industrielle de technologies quantiques pour prendre des parts de marché à l'international, créer des emplois directs et positionner le quantique dans les exportations françaises. Elle reposait ainsi sur deux piliers : la technologie avec des calculateurs quantiques bruités de taille intermédiaire (NISQ), et la prise de positions stratégiques dans la chaîne de valeur, avec la construction d'un ordinateur quantique tolérant aux défauts (FTQC). En effet, il est apparu que les avancées technologiques étaient encore loin de la réalisation d'ordinateurs quantiques tolérants aux erreurs, et qu'il fallait des systèmes alternatifs pour tester les solutions quantiques dans des environnements réels. Un grand défi avait par conséquent été lancé en France en 2021 pour implémenter la correction d'erreur et passer à l'échelle le nombre de qubits physiques, en cheminant vers la construction d'un FTQC. Les performances sont toutefois conditionnées à notre capacité à développer des qubits avec des taux d'erreur très bas, à implémenter la correction d'erreur à grande échelle, et à mettre au point des systèmes de contrôle et d'interconnexion de qubits évolutifs, robustes et fiables.

Point sur la différence entre le NISQ et le FTQC

Le NISQ (*Noisy intermediate scale quantum*) et le FTQC (*fault-tolerant quantum computing*, anciennement LSQ pour *large scale quantum*) font référence à deux catégories d'ordinateurs quantiques. Leur différence réside dans leur capacité à exécuter des calculs quantiques de manière efficace et dans la qualité de leurs qubits.

- Le NISQ se rapporte aux ordinateurs quantiques actuels, qui ont un nombre limité de qubits (quelques dizaines), avec une fidélité relativement basse (qubits bruyants et sujets à des erreurs) et une correction d'erreurs limitée.

- Le FTQC se rapporte à la génération future d'ordinateurs quantiques qui auront un grand nombre de qubits physiques pour fabriquer le plus de qubits logiques possibles (fourchette entre 10 et 10 000, qui sera amenée à évoluer selon les résultats de la recherche fondamentale⁴²) (plusieurs milliers / millions), un faible taux d'erreur et une pleine implémentation technique de la correction d'erreurs, pour résoudre tout type de calcul adapté à la mécanique quantique.

Cette stratégie a ensuite été déclinée en 6 objectifs visant à sécuriser toutes les composantes d'une filière industrielle autonome et compétitive :

1. l'usage des simulateurs d'ordinateurs quantiques grâce aux supercalculateurs et aux ordinateurs hybrides de type NISQ (calculateurs bruités de taille intermédiaire);
2. le développement de l'ordinateur quantique universel en capitalisant sur les atouts de notre recherche en microélectronique;
3. les technologies des capteurs quantiques pour étendre la technologie sur toute la chaîne de valeur industrielle;
4. l'offre de cryptographie post-quantique pour conserver notre avance en développant des composants à l'état de l'art mondial;
5. les technologies habilitantes dont la cryogénie et le laser pour assurer notre approvisionnement en ressources clés;
6. la structuration d'un écosystème avec les bons talents, en doublant le vivier de spécialistes.

⁴² Avec les qubits de chat, Alice & Bob a montré qu'il était possible de faire un qubit logique avec 30 qubits physiques, alors que jusqu'à il y a encore 2-3 ans il en fallait entre 1 000 et 10 000. Il y a encore de la place pour la recherche fondamentale dans ce domaine. De plus, le nombre de qubits physiques nécessaires varie en fonction des applications et de la complexité du problème à traiter.

La spécificité de l'étape 1 du plan quantique résidait dans le fait que les 1,8 Md€ de financements annoncés n'étaient pas uniquement composés d'argent public. Ce plan était composé de trois sources de financement distinctes : 1 Md€ au titre de la reconduction de programmes ministériels au titre de 350 M€, de France 2030 et du plan d'investissement d'avenir (PIA) 4 au titre de 650 M€, près de 550 M€ de cofinancements industriels et près de 250 M€ de financements européens. Les financements industriels et européens ont déjà été débloqués et alloués. **Dès lors, la véritable marge de manœuvre budgétaire publique était de 650 M€, dont environ 600 M€ ont d'ores et déjà été engagés. Il reste donc près de 50 M€ de marge de manœuvre effective jusqu'à fin 2024.**

Trois composantes majeures se sont ainsi matérialisées avec le plan quantique : des capteurs, des ordinateurs et une chaîne d'approvisionnement robuste avec des technologies habilitantes. Désormais, ces composantes doivent permettre de créer un marché intérieur européen. En particulier, nos startups et industriels n'ont pour l'heure pas touché de financements significatifs. L'enveloppe (non définitive) de 400 M€ sur 8 ans du programme Proqcima⁴³ est bienvenue, mais insuffisante pour combler le manque de financements privés, d'autant plus que seulement 80 M€ des 400 M€ de l'enveloppe ont été sécurisés à ce stade. Toutefois, les ordres de grandeur sont de 1 à 10 entre les financements publics et les financements privés en France (*Cf infra*), et de 1 à 2 entre les financements publics français et les financements publics des autres pays *leaders* sur ce type de programme (qui avoisinent plutôt le milliard de dollars). En parallèle, si les investissements d'acteurs privés ont permis de réaliser **des premières démonstrations sur des cas d'usage précis, les partenariats public-privé ont peiné à se concrétiser, notamment sur le financement.** C'est pourquoi, dans son discours du 7 décembre 2023⁴⁴,

⁴³ *L'Usine digitale, La DGA lance un programme avec 5 start-ups françaises pour s'équiper en calculateurs quantiques, 2024.*

⁴⁴ *Emmanuel Macron, Déclaration sur la recherche française, 7 décembre 2023.*

le président de la République a insisté sur la mise en place de stratégies sectorielles pour faire le lien entre recherche fondamentale, recherche appliquée, développement et innovation et sur la nécessité de multiplier les efforts de financements conjoints sur les infrastructures de recherche.

1.3. UNE AVANCE TECHNOLOGIQUE RÉELLE, MAIS UNE OFFRE ENCORE ÉMERGENTE

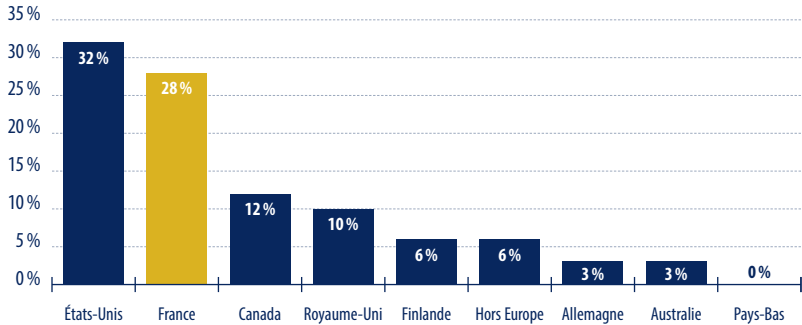
Ce volontarisme politique a permis à la France de créer des fournisseurs d'infrastructure quantique d'envergure mondiale et des acteurs de pointe pour être prêts à les commercialiser, une fois les usages démontrés. De fait, l'informatique quantique ne résout pas tous les problèmes, mais c'est un outil qui permet de passer de la découverte accidentelle dans certains domaines (de type essai / erreur⁴⁵) à de la prédictibilité sur certains problèmes qu'on ne sait pas prédire en l'état actuel des connaissances scientifiques.

Concernant les infrastructures, les acteurs français sont deuxièmes au niveau mondial avec une part de marché de 28 %, derrière les États-Unis à 32 %. La France est également en deuxième position en matière d'exportation de machines quantiques, derrière les États-Unis, avec une part de 20 % contre 29 %⁴⁶. **Malgré ces bonnes performances, la situation reste fragile, car les autres pays rattrapent le retard et sont dans une dynamique de course, ce qui fait peser un réel risque de décrochage sur l'infrastructure quantique sans enveloppe budgétaire supplémentaire pour la v2 du plan.** Les acteurs français doivent impérativement réussir sur ce point, car la France a l'opportunité unique de ne pas accumuler de retard en matière d'infrastructure quantique.

⁴⁵ Par exemple, la molécule de pénicilline a été découverte par accident, alors que sa découverte aurait théoriquement pu être modélisée par un algorithme quantique.

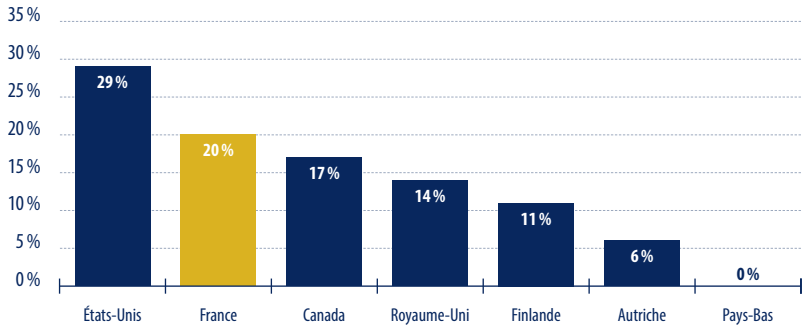
⁴⁶ France 2030 : Point d'étapes trois ans après le lancement de la stratégie nationale des technologies quantiques et lancement du programme Proqcima, mars 2024.

Graphique n° 4 • Parts de marché mondiales par pays fournisseur d'ordinateurs quantiques en août 2024



Source : Gouvernement.

Graphique n° 5 • Exportation d'ordinateurs quantiques par pays fournisseur en août 2024



Source : Gouvernement.

Concernant les offres d'usage, deux technologies permettent de faire la passerelle entre l'informatique quantique et l'informatique binaire pour tester les algorithmes quantiques sur des usages réels :

- 1. Le cloud computing, qui offre un accès à des machines quantiques à distance :** IBM, Google, Microsoft, AWS, IonQ, Xanadu, Rigetti Computing, D-Wave Systems, OVH, etc. Quatre des cinq pépites françaises⁴⁷ du quantique ont mis au point des machines quantiques commercialisées sur des interfaces cloud classiques, comme par exemple OVH. Ces machines sont essentielles pour tester les solutions quantiques sur des machines classiques. Les acteurs intégrés sont essentiellement américains et s'inscrivent naturellement dans une logique de verticalisation, dans laquelle les solutions quantiques développées par des ingénieurs spécialisés peuvent être intégrées de bout en bout, par le biais des plateformes cloud existantes et des environnements applicatifs rattachés à ces plateformes. Cette approche semble aujourd'hui être la plus répandue pour consommer de l'informatique quantique sur des besoins non souverains.
- 2. L'émulation quantique, qui permet de simuler le comportement de qubits sur des ordinateurs classiques :** Qiskit Aer de IBM, QVM de Rigetti, Cirq de Google, Quantum Simulator de Microsoft, Quantum Inspire de Qutech, D-Wave Leap de D-Wave Systems, Amazon Bracket développé par Amazon, Qaptiva de Eviden, Quantum Exact Simulation Toolkit du Quantum Theory Group de Oxford University. **Les émulateurs permettent aujourd'hui aux acteurs de s'acculturer aux logiques de programmation de l'informatique quantique.**

À terme, certaines machines quantiques et émulateurs quantiques ont vocation à être intégrés aux data centers des constructeurs de supercalculateurs, notamment dans des programmes européens de

³⁹ Pasqal, Quandela, Alice & Bob et C12 – Quobly a fait le choix de se reposer sur l'écosystème de l'industrie des semi-conducteurs, plus adapté à la technologie du silicium.

calcul intensif, à l'instar du supercalculateur Joliot-Curie de GENCI et du supercalculateur JUWELS du centre Jülich allemand avec EuroHPC⁴⁸ dans le cadre du projet hybride de calcul à haute performance et de simulateur quantique (HPCQS) de 2021. **Ils doivent permettre à leurs clients d'exécuter des calculs complexes en combinant la puissance de calcul classique et la puissance de calcul quantique. En outre, les calculateurs intensifs de type HPC sont nécessaires pour faire de la simulation quantique à l'échelle, sur des bits, puis sur des qubits.** EuroHPC est un modèle qui a bien fonctionné et qui a été utile pour développer et soutenir des infrastructures de calcul à haute performance (HPC) de classe mondiale en Europe. Doté de 8 Mds€ et financé par la Commission européenne, ce programme a fait advenir des ordinateurs avec des puissances entre 250 et 550 pétaflops ($>10^{15}$ flops), équivalentes ou supérieures aux 200 pétaflops de Summit aux États-Unis ou aux 537 pétaflops de Fugaku au Japon.

Focus sur l'émulateur Qaptiva de Eviden (Atos-Bull)

Présenté sous la forme d'une bibliothèque prête à l'emploi, Qaptiva permet aux entreprises de développer et de tester leurs algorithmes quantiques dans des environnements simulés sur des ordinateurs classiques. L'émulation quantique permet en effet de décrire les règles de comportement de NISQ et LSQ dans des environnements réels. Ces machines contrôlent les interactions entre qubits par de l'intégration de mémoire et de puissance de calcul dans des serveurs optimisés dans ce but. Concrètement, cela permet d'exécuter trois types d'actions :

⁴⁸ Commission européenne, *L'UE déploie la première technologie quantique sur six sites à travers l'Europe, 2022.*

- Simuler des circuits quantiques en utilisant des ressources de calcul classiques, pour modéliser le comportement des qubits et des portes quantiques dans un environnement contrôlé;
- Valider la performance d'algorithmes quantiques sur des machines classiques, avant de les exécuter sur des machines quantiques, en optimisant les paramètres et en vérifiant les résultats attendus;
- Gérer de la simulation à grande échelle, pour tester les algorithmes les plus complexes faisant intervenir un grand nombre de qubits.

Contrairement au super ordinateur, l'ordinateur quantique ne vise pas la puissance de calcul, mais la capacité à résoudre des problèmes de manière innovante. De la même manière que les contrats intelligents, bien que techniquement puissants, ne sont pas toujours adaptés aux problématiques simples en raison de leur complexité et de leur consommation de ressources, les ordinateurs quantiques ne seront véritablement bénéfiques que pour des tâches nécessitant une résolution de problèmes complexes et non pour des applications triviales.

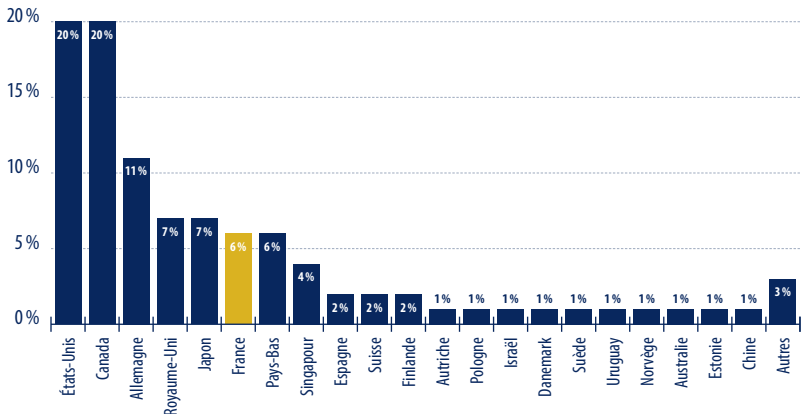
Néanmoins, la France enregistre un réel retard sur la commercialisation de logiciels quantiques, que ce soit sur les outils de développement ou sur l'applicatif⁴⁹. Aucune entreprise française n'a pour l'instant commercialisé des outils de développement quantiques, à l'exception notable de plusieurs ventes de processeurs quantiques, qui sont les composants matériels qui exécutent directement des algorithmes quantiques, à des organisations publiques et privées alors que des entreprises canadiennes, autrichiennes, israéliennes et allemandes l'ont fait. En France, seule l'entreprise Qubit Pharmaceuticals propose une offre pour

⁴⁹ Pour lesquels seuls des modèles de type HPC sont viables aujourd'hui.

accompagner les acteurs à mettre en place des algorithmes quantiques sur mesure. Leur solution, destinée aux acteurs pharmaceutiques, propose un algorithme quantique qui aide à détecter quelle molécule produire. Ce ne sont donc pas des applications packagées, mais des solutions clés en main. De façon plus générale, **la plupart des projets concrets sur le marché aujourd’hui sont des solutions « sur mesure » bâties dans le cadre de partenariat entre les constructeurs et les clients finaux** : l’écosystème d’outils qui rend la technologie accessible à tous n’existe pas encore (au contraire de ce que l’on connaît dans le monde de l’informatique traditionnelle, avec par exemple la richesse et la diversité des outils proposés à leurs clients par les *hyper-scalers* du cloud).

Sur 85 start-ups de logiciel quantique créées dans le monde, 5 sont françaises, et la France représente moins de 1 % des 1,6 Md \$ levés dans le monde sur des solutions de logiciel quantique⁵⁰.

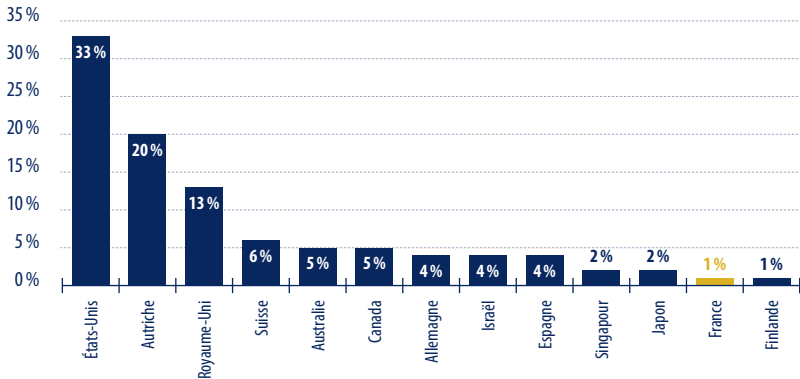
Graphique n° 6 • Part de chaque pays dans le nombre total de start-ups commercialisant du logiciel quantique en août 2024



Source : Gouvernement.

⁵⁰ Source : Coordination Nationale.

Graphique n° 7 • Part de chaque pays dans les levées de fonds totales de *start-ups* en logiciel quantique en août 2024



Source : Gouvernement.

Cette situation est d'autant plus regrettable que le logiciel quantique est *business to business* (B2B) et non *business to consumer* (B2C), soit précisément dans le domaine où l'Europe possède de nombreux atouts pour faire émerger des acteurs compétitifs au niveau mondial. Il est possible de citer, entre autres, des acteurs comme le français Dassault Systèmes pour les logiciels de conception assistée par ordinateur (CAO) et de gestion de cycle de vie des produits (PLM), ou encore l'allemand SAP pour les logiciels de gestion de type Enterprise Resource Planning (ERP), avec de nombreuses expertises sectorielles B2B de pointe.

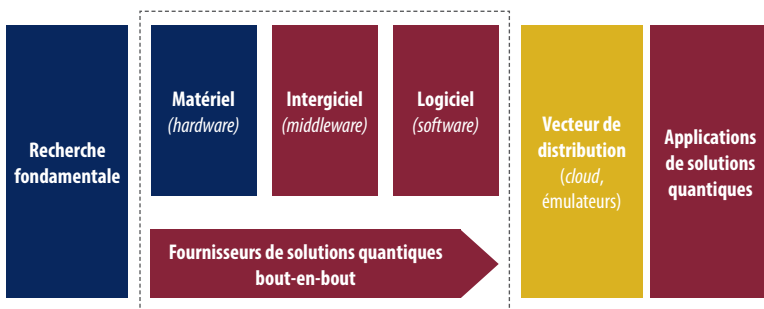
En somme, les acteurs français sont moins présents sur l'aval de la chaîne de valeur quantique et n'ont pas encore mis au point de solutions bout en bout contrairement à leurs concurrents américains.

La chaîne de valeur de l'informatique quantique ne se cantonne pas au matériel, mais englobe toutes les étapes et les acteurs impliqués dans la création d'ordinateurs quantiques, du développement de solutions à

leurs applications, en passant par la distribution de solutions quantiques. Cette chaîne de valeur est complexe et interconnectée, et fait intervenir de nombreux acteurs de manière entremêlée.

Prise dans sa globalité, cette chaîne de valeur montre les forces des acteurs français sur le matériel, indispensable à la sécurisation de nos approvisionnements, et leurs faiblesses sur l’applicatif, indispensable à la conquête de parts de marchés.

Graphique n° 8 • : Illustration simplifiée du positionnement des acteurs français sur la chaîne de valeur quantique



Acteurs français en position dominante



Acteurs français présents mais insuffisamment compétitifs



Acteurs français quasi absents du marché

Graphique n° 9 • Illustration simplifiée du positionnement des acteurs américains sur la chaîne de valeur quantique



■ Acteurs américains en position dominante

■ Acteurs américains présents mais insuffisamment compétitifs

1.4. UN CONTEXTE INTERNATIONAL INSTRUCTIF QUI MOTIVE UNE APPROCHE FRANÇAISE PLUS OFFENSIVE SUR LES PRIORITÉS ET SIMPLE SUR LES STRUCTURES DE PILOTAGE

Les approches internationales de l’informatique quantique se distinguent de l’approche française par leurs priorités et leurs structures de pilotage. Sur le plan des priorités, les pays qui ont conquis le plus de parts de marché⁵¹ (Cf *supra*) se distinguent par des approches «bout-en-bout» sur toute la chaîne de valeur et des objectifs chiffrés en matière de partenariats internationaux. Sur le plan des structures de pilotage, ces mêmes pays ont rattaché leur stratégie quantique à des organes de pilotage uniques, adaptés à l’innovation de rupture et faisant une large part aux industriels et aux personnalités qualifiées. Tous les pays mettent l’accent sur la nécessaire pluridisciplinarité de leurs stratégies quantiques.

⁴² États-Unis, Royaume-Uni, Union Européenne, Canada.

Tableau n° 2 • Perspectives comparées qualitatives

Pays	Priorité	Pilotage
France	<p>La <u>stratégie nationale quantique de 2021</u> repose sur plusieurs piliers :</p> <ul style="list-style-type: none"> • HQI pour du calcul hybride ; • des programmes de recherche (PEPR) pour nourrir les actions aval et faire émerger une offre industrielle ; • le soutien d'entreprises à différents stades de leur maturité par le biais de France 2030 ; • la réponse aux besoins en compétences dans les métiers critiques. 	<ul style="list-style-type: none"> • Ministère de l'économie et des finances et coordinateur national de la stratégie quantique. • ANR avec le CNRS, l'INRIA et le CEA pour les PEPR. • Comités de suivi France 2030 pour le soutien des entreprises. • Appel à projet « Compétences et métiers d'avenir » QUANTÉdu France pour répondre aux besoins de talents.
États-Unis	<p>La <u>National Quantum Strategy de 2018</u> repose sur trois piliers :</p> <ul style="list-style-type: none"> • avoir une approche scientifique qui tient compte des délais à l'issue desquels les applications quantiques seront diffusées ; • renforcer la compétitivité de l'écosystème quantique en accélérant les applications quantiques et les partenariats internationaux ; • créer les bonnes filières de talents quantique. 	<ul style="list-style-type: none"> • Office of Science and Technology Policy. • National Institute of Standards and Technology (NIST) pour piloter les sujets relatifs à la standardisation. • DARPA pour orchestrer les efforts du secteur privé.
Europe	<p>La vision quantique de l'Union européenne est portée par le programme FET Flagship européen doté de 1 milliard d'euros depuis 2018, et structuré autour de 5 piliers :</p> <ul style="list-style-type: none"> • soutien aux <i>startups</i> et PME ; • Investissements dans la recherche fondamentale ; • élargir le pool d'investissements quantiques ; • développer la coopération internationale ; • garantir une coordination efficace au niveau de l'UE. 	<p>Pilotée par la DG CONNECT au sein de la Commission européenne.</p> <p>Financée par le programme « Numérique, industrie et espace » d'Horizons Europe de 2023-2024, avec un financement de 112 M€ annoncé en avril 2024.</p>
Canada	<p><u>Stratégie qui se concentre sur toutes les composantes de la chaîne de valeur :</u></p> <ul style="list-style-type: none"> • recherche fondamentale et appliquée avec l'<u>écosystème de Sherbrooke</u> ; • commercialisation de technologies quantiques ; • développement de main d'œuvre ; • collaborations internationales. 	<p>Gouvernement fédéral qui pilote différents programmes sur trois piliers : recherche, commercialisation et talents.</p> <p>Des sociétés comme Nord Quantique et Xanadu qui se spécialisent dans des technologies de pointe, que ce soit les « codes bosoniques » pour corriger des erreurs sans utiliser trop de qubits, ou des <u>simulateurs</u> pour rendre plus accessible le déploiement de solutions quantiques.</p>

Pays	Priorité	Pilotage
Corée du Sud	<p>La <u>stratégie nationale quantique</u> repose sur trois piliers pour « prendre des parts de marché » :</p> <ul style="list-style-type: none"> • La création d'un écosystème quantique avec des talents, une infrastructure et des applications ; • Le « saut quantique » pour continuer sur l'avance technologique ; • La convergence entre le quantique et d'autres industries, notamment dans le secteur de la défense. 	<p>Le ministère des Sciences et des Technologies de l'information et de la communication :</p> <ul style="list-style-type: none"> • la Fondation nationale de la recherche de Corée (NRF) et l'Institut de planification et d'évaluation des technologies de l'information et de la communication (IITP) pour la planification ; • l'Institut coréen d'évaluation et de planification des sciences et technologies (KISTEP) pour l'évaluation de la stratégie.
Japon	<p>Dans la <u>Vision de la future société quantique formulée en 2022</u> par le MEXT japonais, l'accent est mis sur l'influence du quantique dans la société et sur son importance pour la sécurité économique.</p> <p>En particulier, d'ici à 2030, le Japon estime qu'il y aura 10 M d'utilisateurs de l'informatique quantique dans le pays.</p>	<p>Piloté par le MEXT et structuré en hubs d'innovations pluridisciplinaires autour de l'ordinateur quantique national (RIKEN), en particulier le National Institute of Advanced Industrial Science and Technology (AIST) qui a un rôle central pour fournir de l'accompagnement à l'industrie pour adopter la technologie.</p>
Espagne	<p><u>Vision Ikur 2030</u> : recherche, formation d'une main-d'œuvre qualifiée et développement économique via des collaborations pour explorer des problématiques complexes comme la modélisation de nouveaux matériaux et le développement durable.</p>	<p>Piloté par le Ministère de la Science et de l'Innovation avec le <u>Conseil supérieur de la recherche scientifique espagnol (CSIC)</u> qui gère l'<u>écosystème quantique QTEP</u>.</p> <p>Partenariat public-privé avec IBM avec le <u>centre de calcul quantique IBM-Euskadi</u>.</p>
Finlande	<ul style="list-style-type: none"> • Recherche fondamentale et appliquée pour développer l'infrastructure quantique en mettant deux centres de recherche nationaux en compétition : <u>le VTT et le IQM</u>. • Commercialisation et formation avec <u>Business Q</u>. 	<p>Piloté par le Gouvernement finlandais, un groupe de travail « <u>QST Community</u> » est responsable du <u>Finish Quantum Agenda</u>, essentiellement composé de personnalités académiques.</p>

2 La nécessité de consolider l'offre technologique quantique

2.1. EN LA SÉCURISANT DANS LA LIGNÉE DE PROQCIMA

Le programme Proqcima a été lancé pour déterminer quelle technologie sera en mesure de passer à l'échelle sur un marché mondial fortement concurrentiel. Piloté par la DGA, l'objectif de Proqcima est de sélectionner la technologie qui répondra à un maximum d'usages dans les années à venir en appliquant **une approche en entonnoir pour sélectionner les deux technologies les plus prometteuses⁵² à partir des 5 start-up françaises en lice.**

Le programme se déroule en deux phases :

- **Phase 1 : examen**, où pendant 4 ans, les acteurs doivent démontrer un contrôle avancé de deux qubits avec des opérations logiques précises et efficaces, tout en minimisant les erreurs et en dépassant les limitations technologiques actuelles. Trois acteurs seront sélectionnés à l'issue de cet examen.
- **Phase 2 : compétition** sous la forme d'un concours où seules les startups ayant démontré que leurs technologies pouvaient satisfaire 4 critères clés seront retenues.

Ces critères sont des jalons techniques communs à tous les acteurs du matériel quantique français. Ils doivent se lire davantage comme un processus de « fermeture de porte » partagé que comme une volonté de choisir de manière immédiate la technologie retenue. En effet, l'état d'avancement scientifique en informatique quantique et les données du marché ne permettent pas encore de faire de choix sans une part de risque très élevée.

⁵² ZDNET, *Sur le quantique, la France fait le point et lance Proqcima*, 2024.

Les critères sont les suivants :

1. atteindre un ratio de nombre de qubit physique / qualité du qubit physique dans des zones dédiées;
2. gérer efficacement deux qubits logiques avec des systèmes de correction d'erreurs;
3. démontrer un certain nombre de portes logiques pour manipuler 2 qubits logiques;
4. passer à l'échelle en atteignant un palier à 128 qubits logiques (ce qui nécessite potentiellement plusieurs centaines / milliers de qubits physiques).

Proqcima est novateur et bienvenu, car il comporte une obligation de résultat pour faire converger les enjeux de la recherche appliquée et les enjeux industriels, en lien avec les industriels français. En parallèle de Proqcima, la stratégie nationale quantique française a confié à des laboratoires nationaux, comme l'Institut d'Optique ou le CEA-LETI, la mission d'assurer la souveraineté française sur les filières d'approvisionnement permettant de construire un ordinateur quantique à 128 qubits.

Deux instruments portés par les acteurs académiques et industriels permettent aujourd'hui de transposer cette obligation de résultat au passage à l'échelle des technologies quantiques les plus prometteuses.

1. D'une part, les laboratoires communs qui font intervenir chercheurs et industriels pour passer à l'échelle certaines technologies. Par exemple, des unités mixtes de recherche (UMR) comme le Kastler Brossel du Collège de France sur le refroidissement et le piégeage des atomes pourraient s'associer avec un industriel pour transformer un de leurs prototypes en un produit commercialisable dans le cadre d'un laboratoire commun. Les laboratoires communs sont des structures de recherche collaborative créées pour favoriser l'innovation et le développement de nouvelles technologies en réunissant des chercheurs d'horizons variés, du secteur public et du secteur privé. Ils se concentrent souvent sur la fabrication de prototypes et

de démonstrateurs pour tester les applications quantiques sur des cas d'usages réels. Ils fonctionnent sur la base d'un contrat cadre entre un industriel et les tutelles du laboratoire, généralement le CNRS, des universités ou des grandes écoles. **Surtout, les laboratoires communs réunissent des compétences académiques et industrielles autour de projets en recherche appliquée en faisant appel aux bons acteurs pour les bonnes compétences et avec les bons outils.** Les chercheurs font les prototypes (jusqu'à des niveaux de TRL 3-4), les industriels les transforment en produit (jusqu'à des niveaux de TRL 7-8), et dans l'intervalle, les structures de type CRT (Centres de recherche en technologie), sous l'impulsion de la Coordination Nationale quantique, fournissent des méthodes et du personnel **pour faire les bons paris technologiques, favorisant ainsi le transfert de technologie de la recherche vers l'industrie.**

- 2. D'autre part, les contrats de partenariat d'innovation entre les entreprises et les laboratoires de recherche sont spécifiquement orientés vers le développement d'une solution technologique ou d'un produit innovant, en s'appuyant sur des avancées issues de la recherche académique.** Ces contrats comprennent généralement plusieurs phases, allant du prototypage vers le produit, avec un objectif clair de mise en marché des résultats. Contrairement aux contrats de recherche classiques, qui reposent sur une obligation de moyens, c'est-à-dire une collaboration visant à atteindre un objectif commun sans garantie de résultat et souvent sur une durée indéterminée, les contrats de partenariat d'innovation se caractérisent par une obligation de résultat. Ce type de contrat engage les parties à atteindre un objectif précis et mesurable dans des délais fixés, avec des livrables concrets, souvent à court ou moyen terme. **Par exemple, dans le cadre des technologies quantiques, des entreprises comme Atos ont signé des contrats de partenariat d'innovation avec des laboratoires pour développer des simulateurs quantiques capables d'accélérer des processus de calcul complexes.** Ce type de partenariat combine recherche théorique et application pratique, avec

des phases de développement étroitement encadrées visant à rendre opérationnel un prototype utilisable dans l'industrie d'ici quelques années.

L'exemple du laboratoire commun iXAtom, partenaire clé du programme atomQtrl⁵³ de l'Institut d'Optique

Le laboratoire commun iXAtom est une structure de recherche commune regroupant l'Université de Bordeaux, le CNRS, et l'Institut d'Optique au sein du laboratoire photonique, numérique et de nanosciences (LP2N) et l'industriel EXAIL. Il s'intéresse aux systèmes quantiques pour le positionnement de la navigation inertielle et utilise les atomes froids pour développer la prochaine génération de navigateurs inertiels (deuxième révolution quantique). Une des applications importantes concerne les horloges atomiques modernes qui utilisent des atomes froids, entre autres. Ce laboratoire commun vise un marché à plus de 100 M€ à terme dans le secteur industriel, de la défense et de l'espace. Il a pour l'instant déposé 5 brevets, 2 thèses CIFRE et réalisé 5 publications.

L'objectif du programme atomQtrl est de soutenir le développement industriel des lasers et d'assurer de nouvelles bandes spectrales en adressant les risques les plus importants pour la maîtrise technologique, au premier rang desquels la chaîne d'approvisionnement des composants et sous-composants qui vont s'intégrer dans les capteurs et ordinateurs quantiques. De fait, cette chaîne d'approvisionnement repose sur des composants critiques, comme par exemple certains cristaux qui permettent de passer

⁵³ Ce programme bénéficie d'une aide de l'État gérée par l'ANR au titre de France 2030.

des lasers d'un point A à un point B et qui sont en situation de monopole hors du territoire européen.

Plus d'une vingtaine de longueurs d'onde est nécessaire pour manipuler les atomes froids, le cœur des ordinateurs quantiques et des capteurs quantiques. À ce jour, les approvisionnements sont essentiellement chinois⁵⁴. Les entreprises françaises Toptica et Exail sont l'équivalent en France et le programme atomQtrl a vocation à soutenir le développement de cette filière industrielle, incontournable pour assurer une souveraineté nationale face aux concurrents asiatiques.

Si le programme Proqcima est une première étape nécessaire pour sécuriser la technologie quantique française, il est confronté à trois défis :

- **Premièrement, ce programme doit être capable d'évoluer pour tenir compte de l'incertitude technologique et de l'accélération des roadmaps des start-up concernées.** À peine lancé, Proqcima est confronté au défi de l'accélération des *roadmaps* des acteurs dont il a la charge d'évaluer la maturité technologique. Par exemple, Alice & Bob a accéléré sa *roadmap* pour concevoir un ordinateur quantique universel (FTQC) en 2027-2028 au lieu de 2035, avec seulement 40 qubits logiques et non 128. Dans ce contexte, il n'est pas certain que les paliers choisis restent pertinents une fois que les deux acteurs auront été sélectionnés, si d'autres portes logiques sont par exemple découvertes dans l'intervalle.

⁵⁴ L'entreprise chinoise PreciLaser a notamment réussi à développer de nombreuses longueurs d'ondes en peu de temps pour faire du prototypage et des manipulations.

- **Deuxièmement, il inclut trop peu de mesures d'impact, liées notamment à la capacité des acteurs à déployer leurs solutions sur des logiciels et intergiciels français.** De fait, les 4 critères retenus doivent être d'emblée définis dans une logique de rentabilité et d'alignement avec le marché mondial du quantique. Tout comme avec le réseau Cyclades (*Cf supra*), il est important de prendre en compte le facteur coût / bénéfices dans le choix des deux technologies qui seront ensuite commercialisées mondialement. Autrement dit, la viabilité économique des deux solutions retenues à la fin doit être au cœur des mesures d'impact et d'évaluation de Proqcima, tout au long de sa durée de vie. En outre, le passage à l'échelle de la technologie quantique dépendra d'autres avancées technologiques classiques, ce qui plaide pour l'introduction d'un outil universel d'évaluation des performances des systèmes quantiques et de leur avantage comparatif par rapport à d'autres technologies.
- **Troisièmement, les trois technologies non retenues à l'issue de la phase de compétition doivent continuer à faire l'objet de recherche fondamentale pour s'assurer de la réversibilité de nos choix en cas d'évolution imprévue du marché quantique :** en effet, pour maximiser la capacité de l'informatique quantique, se limiter aux deux technologies qui fonctionnent le mieux peut limiter les perspectives d'exploration si les temporalités de la recherche fondamentale et de l'industrialisation ne sont pas distinguées. Le pendant de Proqcima en matière de recherche fondamentale QuLoop, doté de 40 M€, doit ainsi évoluer à mesure que les technologies les plus prometteuses pour passer à l'échelle sont sélectionnées.

En outre, Proqcima comporte deux effets de bord à l'échelle européenne : d'une part, il risque de limiter les exportations de machines quantiques françaises à l'échelle mondiale s'il reste cantonné à la sphère militaire, et d'autre part, il risque de verrouiller le marché européen si d'autres pays se lancent dans des programmes similaires, par un effet signal, se fermant l'accès à leurs marchés

respectifs. Sur l'infrastructure et le matériel (*hardware*), les institutions néerlandaises Tu Delft et QuTech sont mondialement reconnues pour leurs avancées dans le domaine du *wiring* des qubits⁵⁵ dans les systèmes quantiques, car ils ont accès à des installations de pointe en nanofabrication et une expertise dans la fabrication de câblages ultrafins et dans l'intégration de ces câblages avec des qubits à très basse température. La Suisse et la Norvège sont quant à elles très avancées sur les protocoles de communication quantique, l'Université de Genève⁵⁶ et l'ETH Zurich⁵⁷ ayant développé des QKD déjà commercialisées et le [Gemini Center de la Simula Research Laboratory](#)⁵⁸ norvégienne des méthodes robustes de sécurisation des infrastructures critiques. En 2023, ID Quantique, spin-off de l'Université de Genève, a développé des technologies QKD de pointe qui permettent une communication ultra-sécurisée en utilisant des clés quantiques.

Pour protéger les technologies françaises les plus en pointe, et faire de Proqima un programme pertinent pour les usages civils comme militaires, il est ainsi nécessaire de réserver les technologies quantiques les plus performantes aux usages militaires, tout en ouvrant les technologies quantiques moins pointues aux usages civils et à la concurrence internationale. Cette ouverture aux usages civils doit en retour permettre de nourrir le développement des technologies réservées aux usages militaires. En effet, ces technologies réservées pourraient se nourrir des innovations technologiques du civil pour augmenter leur performance.

⁵⁵ Ensemble des interconnexions et câblages nécessaires pour contrôler, manipuler, et lire l'état des qubits dans un ordinateur quantique. Cela inclut les connexions entre les qubits eux-mêmes, ainsi que les liaisons vers les dispositifs de contrôle externes, tels que les générateurs de signaux et les amplificateurs.

⁵⁶ IDQ, *Unprecedented detector performance opens new perspectives for quantum cryptography*, 2023.

⁵⁷ ETH Zurich, Quantum Center.

⁵⁸ Simula, *Gemini Center on Quantum Computing*.

Le modèle de la société Palantir est à cet égard instructif de la manière de valoriser une technologie émergente, telle que le quantique, à l'échelle européenne sans transiger sur les intérêts sécuritaires nationaux. Dans le cadre de l'étape 2 du plan national quantique, Proqcima pourrait être porté à l'échelle européenne sur ce modèle pour créer un marché intérieur européen en soutenant la R&D des acteurs tout en les encourageant à exporter et vendre leurs solutions à des acteurs étrangers. Cela permettrait à nos technologies de conserver une avance pour que la solution la plus performante reste dans le pays d'origine, tout en répondant à un besoin de marché. Pour rappel, Palantir Technologies est une entreprise de logiciels qui fournit des services d'analyse de données et de renseignement à travers deux plateformes : Palantir Gotham pour les opérations gouvernementales et militaires et Palantir Foundry pour les applications commerciales.

Pourquoi transposer le modèle de Palantir à la diffusion de Proqcima à l'échelle européenne ?

D'abord, parce que Palantir a été créée en faisant le pari technologique d'un logiciel qui permette de traiter de la donnée à grande échelle et de manière personnalisée pour fournir un avantage tactique essentiel dont les armées ne pourraient pas se passer, mais qui ne s'était pas encore matérialisé, comme avec le quantique. Palantir a été aidé par le gouvernement américain dans sa phase préalable de mise sur le marché, puis a bâti son développement commercial en cercles concentriques : d'abord dans ses propres agences de renseignement parmi lesquelles NSA, FBI, département d'État, département de la défense, et département de la justice pour la solution la plus avancées et les gouvernements alliés en offrant des garanties et des prix subventionnés,

puis en ciblant les grandes entreprises privées ayant des besoins complexes en matière de gestion des données. En s'appuyant sur ses succès dans le secteur public, Palantir a démontré la robustesse et l'efficacité de ses solutions, facilitant ainsi leur adoption par le secteur privé. **Cela montre qu'il est possible de réserver des capacités technologiques à un usage souverain tout en diffusant une technologie sensible à un marché le plus large possible.**

Ensuite, parce que Palantir a démontré qu'il est possible de mener en parallèle de la recherche sur un domaine technologique complexe à haut risque, comme le quantique, tout en développant une offre commerciale par étapes auprès d'acteurs choisis. Pour se donner les moyens de ses ambitions, Palantir a mis en place un système permettant d'absorber les coûts induits par la prise de risque, en verrouillant progressivement le marché associé avec une offre commerciale agile. Cette offre commerciale vient tout à la fois financer la recherche, compléter les travaux par des boucles d'expérimentation en situation réelle et fidéliser des clients pour développer leur offre à mesure que leurs besoins se matérialisent. **La condition de succès d'une telle stratégie a été la conception de leurs conditions de passage à l'échelle, ce qu'a déjà fait Proqima.** Par exemple, les solutions de Palantir ont été conçues pour être suffisamment flexibles pour intégrer différents types de données et répondre aux besoins spécifiques de divers secteurs, de la défense à la santé publique. **Ce modèle montre qu'une double approche gouvernementale et privée, pour peu qu'elle réponde à un besoin réel, peut créer un marché. En l'occurrence, Palantir a non seulement démontré la valeur de ses solutions pour des usages réels, mais aussi façonné la demande en matière de capacités d'analyse avancée de données, à mesure de son développement.**

Enfin, parce que le modèle de tarification de Palantir répond à la préoccupation principale des acteurs privés sur l'informatique quantique, qui est de démontrer et de monétiser l'avantage quantique sur des usages spécifiques. Ce modèle facture les clients en fonction des avantages tangibles et des gains d'efficacité obtenus grâce à l'utilisation des logiciels de Palantir, plutôt qu'un simple abonnement ou une licence. En plus des frais initiaux facturés pour la mise en place de la solution, des frais récurrents fonction des résultats obtenus avec la solution peuvent être calculés en fonction des économies réalisées, des gains d'efficacité permis et de la valeur inhérente à la résolution de certains types de problèmes. Avec une politique dite de « services managés », Palantir prend des engagements financiers pour faire évoluer son offre en fonction des besoins et garantir son fonctionnement optimal.

Recommandation 1

Confier à Proqcima, reconnu à l'échelle européenne comme l'acteur le plus légitime en la matière, l'identification et la sécurisation de la technologie française la mieux adaptée à une offre compétitive militaire et civile à l'échelle de l'Europe.

1/ Confronter les 2 technologies françaises retenues aux technologies européennes d'égale maturité. En effet, la « logique d'entonnoir » de Proqcima est constituée de jalons techniques communs à tous les acteurs qui construisent des ordinateurs quantiques pour choisir les technologies qui seront les plus performantes pour les

usages militaires comme civils. Il faudra ainsi prendre en compte les partenaires européens qui sont en pointe sur les technologies de qubits quantiques comme par exemple le VTT en Finlande, l'IFN en Italie, la Chalmers University of Technology de Suède, le Gemini Center norvégien, l'Université de Genève, l'ETH de Zurich, l'école de Copenhague au Danemark ou encore le TU Delft et QuTech des Pays-Bas. Le choix des technologies quantiques les plus performantes à l'échelle européenne permettra la définition d'une ambition véritablement mondiale.

2/ Rendre Proqcima plus dynamique compte tenu de l'évolution rapide du milieu industriel qu'il a vocation à adresser en :

- confiant les deux technologies retenues à des laboratoires communs (laboratoires associant recherche appliquée et entreprises) pour s'assurer de leur pertinence industrielle une fois les machines construites, tout en gardant une marge de manœuvre pour gérer l'incertitude scientifique des autres technologies non retenues tout au long du programme.
- mettant en place des mesures d'impact adaptées aux usages industriels, avec un indicateur permettant de quantifier la valeur ajoutée en milieu industriel des avantages quantiques permis par les deux technologies retenues.
- veillant à confier au programme de recherche fondamentale QuLoop le suivi des technologies non retenues par Proqcima afin de garantir une éventuelle réversibilité de la technologie si sa maturité évolue ou si le marché le décide. Le procédé de sélection doit être proche du terrain et simple dans l'exécution.

3/ Pour protéger les technologies quantiques françaises les plus en pointe, **une logique de réservation des technologies les plus performantes pour les usages militaires et régaliens pourra être appliquée** (sur un modèle de type Palantir) permettant d'ouvrir des versions technologiques moins performantes aux usages civils et à la concurrence internationale.

2.2. EN DIFFUSANT LES STANDARDS FRANÇAIS À L'ÉCHELLE EUROPÉENNE

Le passage à l'échelle de nos technologies quantiques est tant un enjeu vertical, comme vu plus haut, qu'horizontal, puisqu'il dépend aussi de notre capacité à construire des systèmes d'interconnexion entre ordinateurs quantiques pour garantir leur interopérabilité une fois que les usages seront débloqués et identifiés.

C'est dans cette optique que la France a mis en place une stratégie de normalisation incarnée par le programme MetriQs-France⁵⁹ de 2022, et coordonnée par le Laboratoire national de métrologie et d'essais (LNE). BACQ est le premier projet lancé dans le cadre du programme et fournit des benchmarks pour évaluer les performances des systèmes quantiques en définissant des problèmes de référence qui font sens pour les utilisateurs finaux de cette technologie. L'objectif est de les agréger en un indicateur opérationnel qui permette de comparer différentes machines entre elles au niveau mondial. **Sur 11 commissions IEEE (Cf encadré), 9 sont présidées par des Français, un groupe de travail a un secrétaire général français au sein de la Commission européenne et le**

⁵⁹ Agence Nationale de la Recherche, *Développement des référentiels de mesure, des standards et l'évaluation des technologies quantiques*, 2022.

secrétariat ISO est aujourd'hui français, ce qui témoigne de l'impact de MetriQs-France pour consolider l'influence européenne dans les instances de normalisation européennes.

Focus sur les Commissions IEEE

Les Commissions IEEE sont le vecteur mondial par lequel sont développés et promus les standards techniques dans le secteur des technologies de l'information et de la communication (TIC), en particulier en informatique quantique. Elle est composée de commissions (*IEEE Standards Committees*) responsables du développement, de la maintenance et de l'actualisation des standards techniques associés. Ses attributions se concentrent sur trois domaines :

1. Le développement de standards interopérables, sécurisés, et performants, en élaborant des normes techniques basées sur les meilleures pratiques de l'industrie ;
2. La mise à jour régulière de ces standards, en lien avec les industriels et les découvertes des scientifiques ;
3. La diffusion de ces standards au grand public, pour faciliter leur adoption.

En matière d'informatique quantique, c'est le *Standard for Quantum Computing Definitions (IEEE P7130)* qui fait foi, qui pour l'instant se concentre sur la définition des termes et concepts fondamentaux de l'informatique quantique pour s'assurer d'une compréhension commune à l'échelle mondiale.

En janvier dernier, l'Organisation internationale de la normalisation (ISO) et la Commission électronique internationale (IEC) ont créé **un comité technique mixte pour les technologies quantiques, l'ISO/IEC JTC 3**. Cette création a pour objectif de coordonner les approches normatives sur la technologie quantique pour assurer la plus grande cohérence possible sur le marché. Ce nouveau comité mixte, présidé par la Corée du Sud, et dont le Secrétariat général est assuré par le Royaume-Uni (British Standards Institution), aura la charge d'élaborer les normes relatives à la technologie quantique. En parallèle, l'Union internationale des télécommunications (UIT) au sein des Nations Unies a organisé en mai dernier un atelier sur le thème « Points de vue sur la certification de la distribution des clés quantiques et des réseaux de distribution de clés quantiques » au sein de l'organisme dédié à la standardisation des normes autour de la distribution de clés quantiques, le JCA-QKDN⁶⁰. L'objectif était de faire le point sur les normes en vigueur, et sur la manière avec laquelle elles sont appliquées et mises en œuvre dans les réseaux de production.

Hors instances de normalisation, c'est toutefois l'usage qui a historiquement déterminé si une norme était utilisée ou non sur le marché. En effet, toute stratégie normative doit être fondée sur le principe de la preuve technologique, soit en s'imposant comme un standard de facto, car répondant à une demande sur le marché. Il est ainsi crucial de mettre en œuvre des stratégies normatives fondées sur l'évolution du marché. De fait, des référentiels de mesure, d'évaluation et de normalisation des technologies quantiques doivent être prêts une fois que les systèmes quantiques seront interopérables entre eux. L'interopérabilité des systèmes quantiques entre eux est en effet un enjeu majeur, tant sur le plan technologique que sur le plan commercial et de l'adoption. Elle repose essentiellement sur l'intergiciel (*middleware*), qui fait le lien entre le matériel, les ordinateurs quantiques, et les logiciels sur lesquels ces ordinateurs peuvent être déployés.

⁶⁰ UIT, Joint Coordination Activity on Quantum Key Distribution Network (JCA-QKDN).

- **Sur le plan technologique**, un intergiciel quantique interopérable sera nécessaire pour utiliser plusieurs technologies de qubits sur un même ordinateur quantique, pour combiner leurs atouts et optimiser les charges de travail. C'est aussi une manière d'intégrer plus facilement les mises à jour, de manière modulaire, sans avoir à réaliser de changements majeurs sur l'architecture à chaque fois. En outre, le principal défi de l'informatique étant de maintenir l'intrication dans la durée (*Cf supra*), un intergiciel interopérable permettrait de minimiser les pertes potentielles de cohérence des états des qubits quand ils sont transférés ou manipulés. Enfin, l'interopérabilité augmente la redondance des systèmes, et de ce fait leur tolérance aux pannes.
- **Sur le plan commercial et de l'adoption**, un intergiciel quantique interopérable permet de réduire les coûts de développement, d'exploitation et de maintenance, ce qui en retour facilite la mise en œuvre d'un modèle de tarification et de licences favorables, garants d'une meilleure accessibilité. C'est une brique essentielle, à l'échelle européenne, pour faciliter l'adoption de solutions quantiques, en abaissant les barrières à l'entrée pour les nouveaux utilisateurs.

La spécificité de Nvidia, comment ont-ils réussi à s'imposer ?

Nvidia a réussi à imposer son standard d'intergiciel (*middleware*) CUDA (*Compute Unified Device Architecture*) grâce à une combinaison de stratégies technologiques, commerciales et communautaires :

- Concernant la technologie, CUDA a permis d'exploiter les performances des GPU fabriqués par Nvidia, qui offrent des performances supérieures à celles des CPU traditionnels. CUDA a aussi simplifié le langage de programmation des GPU en fournissant

une API⁶¹ et un environnement facile à utiliser pour les développeurs, réduisant ainsi les barrières à l'entrée pour le développement en parallèle.

- Sur le plan commercial, Nvidia a maintenu une politique de licences favorables pour CUDA (gratuites pour les développeurs, dans le but de faciliter l'adoption dans un premier temps, puis de verrouiller le marché dans un second temps) et a optimisé son modèle de tarification des GPU, ce qui a fait de CUDA un standard de facto par sa performance.
- Sur le plan communautaire, Nvidia a consolidé un écosystème autour de CUDA (bibliothèques optimisées, outils de développement, frameworks de *machine learning* populaires) qui s'intègre facilement avec de nombreux logiciels, favorisant ainsi son adoption. En retour, un effet de réseau s'est créé, où de plus en plus de développeurs et d'entreprises ont suivi, ce qui a créé un effet vertueux pour CUDA, devenu un standard mondial incontournable pour toute entreprise ayant besoin de puissance de calcul.

Néanmoins, les acteurs européens n'ont pas la force de frappe financière et technologique pour imposer un standard d'intergiciel quantique fermé au niveau mondial aujourd'hui. En revanche, les standards ouverts gagneraient à être davantage exploités pour favoriser l'adoption des technologies quantiques en créant un effet réseau. L'open-source quantique renvoie à la pratique de rendre les logiciels, algorithmes et protocoles quantiques accessibles à tous, permettant ainsi à la communauté mondiale de chercheurs et d'ingénieurs de collaborer, d'améliorer, et de standardiser ces outils. De nombreux

⁶¹ Interface logicielle qui permet de « connecter » un logiciel ou un service à un autre logiciel ou service afin d'échanger des données et des fonctionnalités.

programmes open-source permettent aujourd’hui à des milliers de développeurs et chercheurs de contribuer à un écosystème commun, facilitant l’innovation rapide et l’interopérabilité entre différentes plateformes quantiques. Les plus significatifs sont le programme Qiskit d’IBM, le programme Cirq de Google, le programme Q-Sharp de Microsoft, et le programme Forest de Rigetti Computing. Si ces dispositifs sont efficaces pour faciliter l’adoption de solutions quantiques à l’échelle mondiale, ils sont encore trop peu exploités par les acteurs français et européens, qui gagneraient toutefois à contribuer aux bases communes sur lesquelles les technologies quantiques sont amenées à être développées. Cette absence est d’autant plus incompréhensible que les barrières à l’entrée pour ce type de programmes sont encore faibles, et que le moment est stratégique puisque le marché est en cours de création.

Recommandation 2

Conscient de la nécessité de prioriser les solutions tout en veillant à ne pas se faire imposer *de facto* des standards structurés par d’autres, inciter les acteurs français et européens à contribuer aux programmes open-source internationaux dans lesquels il y a un intérêt commercial à être contributeur. Les programmes les plus prometteurs à ce stade sont le programme Qskit d’IBM, le programme Cirq de Google, le programme Q-Sharp de Microsoft et le programme Forest de Rigetti Computing. Le Quantum Flagship européen pourrait inclure une obligation de contribution à ce type de programme dans ses critères de financement de projets de recherche fondamentale et appliquée en technologies quantiques.

La normalisation joue pourtant un rôle clé pour ne pas se faire imposer en Europe des standards structurés par d'autres acteurs aux intérêts divergents.

De manière immédiate, cela se traduit par les efforts qui sont en cours pour anticiper un monde « post-quantique », où l'algorithme de Shor pourrait compromettre systématiquement les méthodes de chiffrement actuelles. En réponse à cela, l'ANSSI a proposé dès 2022 une approche dite « hybride ». Cette démarche consiste à combiner un algorithme de chiffrement classique offrant une protection contre les cyberattaquants traditionnels, et un algorithme post-quantique capable de résister aux futures attaques menées par des ordinateurs quantiques. Cependant, l'ANSSI ne considère pas cette technologie comme suffisamment mature pour remplacer à court terme les standards de chiffrement actuels. Plusieurs raisons expliquent cette réticence, notamment l'absence de tests à grande échelle et le manque de garanties sur la solidité des algorithmes post-quantiques face à des cyberattaques complexes. Ce sont les organisations les plus sensibles qui sont particulièrement concernées. Les instances gouvernementales, par exemple, pourraient être vulnérables à la stratégie du « *Harvest now, Decrypt later* » (capturer aujourd'hui, déchiffrer plus tard), stratégie qui consiste à capturer aujourd'hui des documents chiffrés, avec l'intention de les déchiffrer plus tard, lorsque les capacités technologiques auront progressé. Ce risque est particulièrement pertinent pour des données à longue durée de sensibilité, telles que des informations militaires ou d'État.

Pour parer à cette menace, des mesures doivent être prises à court terme dans les organisations publiques et privées. L'une des solutions envisagées est l'intégration de surcouches de chiffrement. Ces surcouches permettent de renforcer la sécurité en ajoutant un second niveau de chiffrement, par exemple en combinant un algorithme classique avec une méthode post-quantique ou encore des techniques de chiffrement de bout en bout (E2EE). Cela offrirait une protection supplémentaire pour les données sensibles, même en cas de percée technologique future dans le domaine du calcul quantique.

En août 2024, le National Institute of Standards and Technology (NIST) américain a publié trois normes pour des algorithmes cryptographiques post-quantiques ouvrant ainsi la voie à la mise en place de solutions de cybersécurité adaptées aux FTQC :

- 1. CRYSTALS-Dilithium :** Cet algorithme de signature numérique repose sur des *treillis modulaires*, une structure mathématique complexe qui résiste même aux puissants calculs des ordinateurs quantiques. CRYSTALS-Dilithium est conçu pour authentifier les données et les systèmes à distance, en remplaçant les algorithmes classiques comme RSA, qui sont vulnérables aux attaques quantiques. Il garantit que seules les entités autorisées peuvent accéder aux informations, en utilisant des signatures numériques résistantes aux capacités des futurs ordinateurs quantiques.
- 2. CRYSTALS-KYBER :** Cet algorithme d'encapsulation, également basé sur des *treillis modulaires*, protège la confidentialité des données. L'encapsulation dans ce contexte fait référence au processus par lequel des clés cryptographiques sont sécurisées et partagées entre deux parties de manière confidentielle. CRYSTALS-KYBER génère des clés symétriques partagées, utilisées pour chiffrer les communications. Cet algorithme est destiné à remplacer l'algorithme de Diffie-Hellman, une méthode traditionnelle de négociation de clés qui permet à deux parties de générer une clé secrète partagée sur un canal non sécurisé. Cependant, Diffie-Hellman devient vulnérable face aux ordinateurs quantiques, d'où la nécessité de solutions comme CRYSTALS-KYBER qui résistent à ces menaces.
- 3. SPHINCS+ :** Cet algorithme de signature numérique utilise un *code de hachage sans état*, une technique qui n'exige pas de suivre l'historique des opérations précédentes, ce qui améliore l'efficacité et réduit les temps de traitement. SPHINCS+ produit des clés publiques de petite taille tout en générant des signatures plus grandes. Cela le rend particulièrement adapté à des scénarios où la sécurité est

critique, même si les signatures sont volumineuses. Il peut être utilisé en complément d'autres algorithmes, comme ML-DSA, pour renforcer la sécurité contre les attaques futures, notamment celles menées par des ordinateurs quantiques.

Recommandation 3

À long-terme, et au sein des instances internationales de normalisation, dans le cadre du programme MetriQs France, définir une stratégie de normalisation à partir des acteurs et des technologies françaises et européennes en matière de normes de calcul, normes de sécurité et de compatibilité des technologies habilitantes et protocoles de communication entre infrastructures quantiques :

- Sensibiliser les intervenants français et européens à l'importance d'une approche plus offensive et plus structurée sur la base d'une stratégie de normalisation définie en amont par MetriQs France avec le concours des industriels amenés à les commercialiser.
- Créer des cellules de veille sectorielle dans les commissions ISO/IEC JTC 3 et JCA-QKDN avec des outils de veille informatisés pour collecter l'information en temps réel, sur le modèle du *Quantum Economic Development Consortium* (QED-C) du NIST.
- Mettre en place une collaboration entre les laboratoires communs et le LNE pour diffuser des normes permettant un passage à l'échelle plus rapide des technologies quantiques sur le modèle du Fraunhofer-Gesellschaft avec

l'Institut allemand de normalisation (DIN) pour mettre en place des spécifications quantiques dans la norme ISO/IEC 2382.

- Suivre en intelligence économique les positions américaines dominantes ainsi que les positions chinoises extrêmement actives dans les organisations internationales afin de comprendre les évolutions du marché, identifier les éventuels syndromes NVidia (développement vélocité d'une technologie moins disante mais facilement adoptable) et adapter notre technologie à la demande.

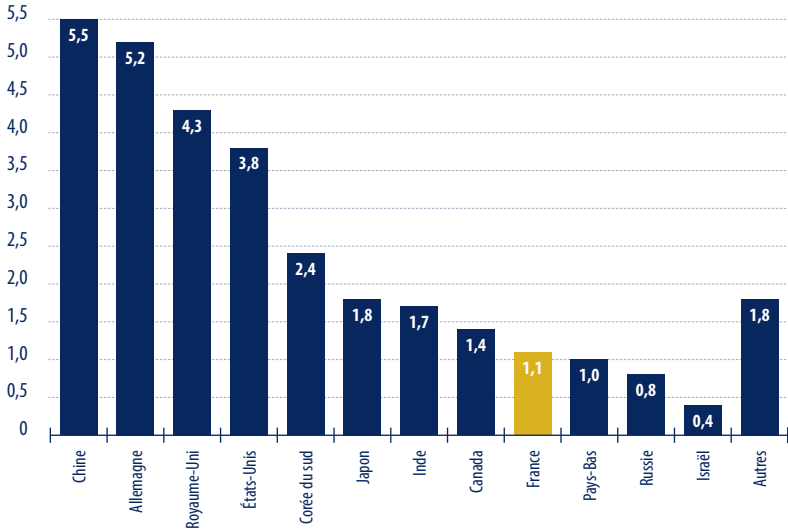
2.3. EN ALIGNANT L'INVESTISSEMENT PUBLIC AVEC L'INVESTISSEMENT PRIVÉ

Les investissements publics dans l'informatique quantique sont aujourd'hui 3 fois plus élevés au niveau mondial que les investissements privés. En juin 2024, ils atteignent près de 40 Mds \$⁶² contre près de 10 Mds \$⁶³ pour l'investissement privé.

⁶² Quobly, *Le calcul quantique, vers la grande échelle en France, 2024.*

⁶³ *The Quantum Insider.*

Graphique n° 10 • Panorama des investissements publics en quantique par pays, en Mds \$



Source : *McKinsey, avril 2024* et *Gouvernement*.

Dans le même temps, les investissements privés dans l'informatique quantique ont baissé de 7 %⁶⁴ depuis 2023. D'après un récent rapport de McKinsey⁶⁵, 62 % des investissements privés dans l'informatique quantique sont allés vers des startups ayant plus de 5 ans, ce qui témoigne d'**une appétence des investisseurs pour des technologies éprouvées et prêtes à passer à l'échelle.** À l'inverse, les investissements du secteur public ont augmenté de près de 50 % depuis 2022, pour établir un *leadership* sur les technologies quantiques, considérées comme essentielles à l'autonomie stratégique. Ces investissements s'inscrivent

⁶⁴ *The Quantum Insider, The Quantum Quarterly, 2024.*

⁶⁵ *Ibid.*

aussi dans une démarche d'impulsion pour stimuler les investissements privés. Certains pays, à l'instar du Royaume-Uni⁶⁶, ont désormais énoncé des objectifs chiffrés d'investissement privé dans leurs stratégies nationales quantiques. Ce problème est mondial, mais il est plus marqué en France qu'aux États-Unis. **L'écart entre les financements publics et les financements privés en France est de 610 M \$ (490 M \$ levés contre 1,1 Mds \$ de financements publics) alors qu'il est de 75 M \$ aux États-Unis (3 Mds \$ levés contre 3,75 Mds \$ de financements publics).**

Cependant, pour attirer les investissements privés, il est crucial que les investisseurs perçoivent un horizon clair et prometteur. Actuellement, l'informatique quantique est encore considérée comme un investissement à haut risque. Les investisseurs qui suivent les initiatives publiques ne sont pas forcément ceux qui ont les poches les plus profondes. **L'intervention de l'État est donc nécessaire pour investir là où le secteur privé ne peut pas supporter le risque associé, créer un marché si pertinent et partager le risque en tant que *limited partner*⁶⁷ minoritaire.**

En outre, l'absence de grands fonds d'investissement européens spécialisés *Deeptech* limite structurellement les possibilités pour l'écosystème de se financer à hauteur de ses besoins. La fragmentation du financement européen limite encore la croissance du secteur quantique quand les entreprises ont besoin de lever des sommes importantes, une fois leur stratégie de passage à l'échelle définie. Pour des levées supérieures à 100 M€, les entreprises n'ont d'autre choix que d'ouvrir leur capital à des investisseurs étrangers, ce qui est particulièrement préoccupant au moment du *late stage* (série B ou C). Par exemple, dans le cas de la récente levée de Pasqal en série B, il aurait fallu un fonds *deep tech* doté

⁶⁶ *National Quantum Strategy, 2023.*

⁶⁷ *Acteurs qui apportent le capital aux fonds mais qui n'interviennent pas dans les décisions quotidiennes (passifs), et dont la responsabilité est limitée à la somme investie dans le fonds. Ils reçoivent une partie des profits générés par le fonds selon les termes du partenariat, après que les General Partners aient reçu leur management package.*

de 1 Md€ pour être en mesure de ne pas ouvrir son capital à mesure des tours de financement. En effet, le montant maximum d'exposition des fonds sur les tickets est de 5 % du montant total du fonds⁶⁸, alors que nos plus grandes levées ne dépassent pas les 300 M€.

Enfin, même si les fonds européens qui investissent dans la technologie quantique sont moins spécialisés et suivent de plus en plus une logique de type push avec des consortiums dans lesquels des entreprises technologiques s'associent aux acteurs industriels, il convient de réfléchir à plus long-terme à la mise en place d'un véritable fonds de consolidation à l'échelle européenne pour tirer toute la valeur des applications commerciales quantiques une fois qu'elles se matérialiseront.

Recommandation 4

Mettre en place des incitations ciblées pour les grandes entreprises françaises afin de motiver l'acquisition des jeunes pousses quantiques et d'encourager les acteurs du capital risque et du capital croissance à investir dans le quantique.

- Mettre en place des **avantages fiscaux de type CIR** ou autres pour les grandes entreprises qui réaliseraient des acquisitions de jeunes pousses quantiques pour un montant supérieur à 300 M € (compatible avec les règles de financement des fonds Deeptech européens), en considérant ces acquisitions comme des dépenses d'investissement d'avenir, conformément à la logique initiale du CIR. Il est à noter que les grandes entreprises françaises achètent des prestations quantiques mais n'investissent

⁶⁸ Aux États-Unis, les règles d'exposition dans les fonds deeptech sont moins strictes, les taux d'exposition pouvant aller jusqu'à 10-20 % en fonction du fonds.

pas directement à leur capital, contrairement aux entreprises américaines qui y voient un moyen de créer de la valeur rapidement.

- Mettre en place des indicateurs de performance valorisant ce type d'acquisition dans les **programmes d'allocation de fonds certifiés européens**.
- Le marché européen du capital risque et du capital croissance restant très timoré vis-à-vis des startups quantiques (pour des raisons de retour sur investissement dans des temporalités inférieures à 7 ans), militer en faveur de la **création d'un fonds de capital-risque multiples entreprises** (*multi corporate ventures*) dédié à l'achat de *startups* quantiques au moment de la série B, permettant la constitution d'expertises dédiées au secteur et l'identification des brevets utiles technologiquement ou valorisables financièrement pour le secteur quantique.

2.4. EN ATTIRANT ET EN FORMANT LES BONS TALENTS

L'étape 1 du plan quantique a mis en place de nombreuses actions en faveur de la recherche fondamentale sous l'égide de l'Agence nationale de la recherche (ANR) et des organismes nationaux de recherche (ONR).

Ces actions ont donné lieu au lancement de projets prioritaires pour la recherche (PEPR) en 2020, pilotés par le CEA, le CNRS et l'INRIA⁶⁹, qui ont permis de renforcer les liens entre les différents pôles de

⁶⁹ Secrétariat général pour l'Investissement, *France 2030 : Des résultats concrets pour les 2 ans de la stratégie quantique, 2023.*

compétitivité sur le territoire français (Grenoble, Toulouse, Rennes).

Ces projets ont vocation à accélérer la recherche et l'innovation dans les domaines considérés comme étant les plus stratégiques en technologies quantiques, dans les phases les plus en amont, de la recherche fondamentale à la preuve de concept (TRL 2 à 4).

Il a été doté de 10 projets ciblés répartis dans 4 axes distincts⁷⁰ :

1. les qubits robustes à l'état solide, dits « solid state » pour faire du calcul quantique;
2. les atomes froids pour le calcul et les capteurs quantiques;
3. les algorithmes quantiques;
4. la communication quantique à la frontière entre la calculabilité et la sécurité.

Les projets retenus au sein de ces axes doivent être cohérents avec les priorités stratégiques du plan quantique et visent à explorer les technologies qui pourraient émerger dans un monde avec des avantages quantiques réels. Par exemple, sur les qubits robustes à l'état solide, le projet baptisé RobustSuperQ⁷¹, vise à préserver les qubits supraconducteurs de décohérence en construisant un processeur quantique haute fidélité et pilotable qui n'existe encore sur aucune plateforme. **En complément, des collaborations européennes ont été menées, à l'instar du Grand défi sur l'innovation de rupture à l'université de Delft aux Pays Bas.** En janvier dernier, l'entreprise Fujitsu a ainsi ouvert un laboratoire dédié aux technologies quantiques à l'Université de Delft pour accélérer la R&D quantique dans le réseau cristallin de diamants et faire progresser le développement d'applications quantiques réelles.

En outre, pour répondre à l'ambition initiale du Plan national quantique, qui était de sécuriser toutes les composantes de la chaîne de valeur des technologies quantiques, des comités d'experts ont été

⁷⁰ CNRS, *Le PEPR Quantique démarre, 2022.*

⁷¹ Agence nationale de la Recherche, *Projets ciblés du PEPR Quantique, 2023.*

instruits par maillon de cette chaîne. Ces comités se sont concentrés sur la criticité et le niveau de maîtrise, sur les instruments d'accompagnement de la puissance publique et sur la capacité de l'écosystème à être mobilisé (matériaux, composants, systèmes, déploiement, usages). Par exemple, le comité d'experts présidé par Benoît Potier a permis d'identifier les filières émergentes à fort contenu technologique.

Cependant, malgré les 150 M€ d'investissements publics consacrés à la recherche fondamentale en informatique quantique, aucun renforcement significatif de la masse salariale dédiée à cette recherche n'a été observé. Si ces fonds ont permis aux chercheurs existants de se concentrer sur des projets à long terme, ils n'ont pas suffi à attirer de nouveaux talents. Des obstacles administratifs, tels que les plafonds d'emploi dans les ministères et les restrictions sur l'embauche de post-doctorants, continuent de freiner la progression de la masse salariale de la recherche en informatique quantique. **Pour rester à la pointe de la recherche scientifique et attirer les meilleurs talents vers les métiers du quantique, il est toutefois essentiel de nous donner les moyens de recruter les meilleurs talents. Cela passe notamment par la création de chaires scientifiques dans les laboratoires de recherche français comme l'INRIA, l'Institut d'Optique, ou encore le CEA, autour de grandes figures du quantique.** De manière plus globale, la question de la rémunération des chercheurs français, qui dépasse le cadre de l'informatique quantique, doit également être adressée, avec des comparatifs par rapport aux autres pays européens.

Recommandation 5

Mettre en place des chaires quantiques dans les laboratoires de recherche fondamentale et appliquée généraux aux méthodologies éprouvées.

- Motiver les jeunes scientifiques à s'intéresser au quantique et débaucher des profils connexes susceptibles de contribuer à l'informatique quantique par des synergies scientifiques.
- Proposer des dispositifs dérogatoires par rapport aux salaires publics sur certains profils internationaux afin d'attirer les profils clés sur des projets d'étude critique, en limitant l'écart, à titre exceptionnel et sur une durée donnée, par rapport aux salaires internationaux. Le dispositif « Chaire d'excellence » lancé en mai 2023 et opéré par l'ANR pourrait être utilisé pour mettre en œuvre cette proposition.

De manière plus structurelle, pour que ces talents soient correctement formés aux futurs besoins des entreprises, il est crucial d'insérer dans les cursus pédagogiques de mathématiques des enseignements permettant de formuler correctement des problèmes quantiques. En effet, c'est parce que les problèmes quantiques ne sont pas bien formulés qu'ils sont aujourd'hui peu adoptés. Actuellement, des formations initiales en informatique quantique existent, mais elles sont embryonnaires. Le programme QuanTEdu France⁷², qui regroupe un consortium de 21 établissements d'enseignement supérieur, est une première étape déterminante pour créer des emplois dans la filière quantique à l'horizon 2030. Toutefois, ce programme reste cantonné à des aspects partiels comme la cryptographie quantique, en dépit de masters 100 % quantiques. **En effet, les formations françaises manquent de programmes spécialisés qui intègrent les concepts fondamentaux de la logique non binaire (dite « non booléenne »), propres à la mécanique**

⁷² Université Sorbonne Paris-Nord, QuanTEdu-France, se former au quantique.

quantique. La logique non booléenne désigne un ensemble de cadres logiques conceptuels qui dépassent la logique booléenne classique, selon laquelle une proposition est soit vraie, soit fausse.

Ces logiques englobent deux grands ensembles théoriques :

- 1. La logique floue, dite « fuzzy logic », a été introduite par Lotfi Zadeh en 1985⁷³ pour modéliser des situations où les frontières entre le vrai et le faux ne sont pas nettes, permettant de traiter des « vérités partielles ».** Cette approche est utilisée en informatique pour intégrer la gestion des connaissances imparfaites avec des probabilités. En milieu industriel, elle permet d'améliorer la gestion de l'incertitude à travers des algorithmes. Par exemple, dans le freinage des véhicules autonomes, alors qu'une logique booléenne appliquerait un freinage maximal en cas de route glissante, la logique floue permettrait de modéliser un freinage gradué : si la route est moyennement glissante, le freinage serait ajusté à 50 % au lieu de 80 %. **Un sous-ensemble de la logique floue est la logique multivalente qui propose plusieurs valeurs de vérité intermédiaires plutôt qu'une simple dichotomie entre le vrai et le faux.** Par exemple, la logique trivalente de Lukasiewicz⁷⁴ introduit une troisième valeur, souvent appelée « indéterminée », entre le vrai et le faux.
- 2. La logique modale introduit des concepts tels que la nécessité et la possibilité en ajoutant des modalités comme « nécessairement vrai » ou « possible » aux propositions logiques.** Fondée par Clarence Irving Lewis en 1918⁷⁵, qui établit la distinction entre vérités nécessaires et contingentes, elle a ensuite été développée par Saul Kripke en 1963. Kripke a montré que les vérités pouvaient

⁷³ Claude Rosental, *Histoire de la logique floue. Une approche sociologique des pratiques de démonstration*, 1998.

⁷⁴ Denise Becchio, *Logique trivalente de Lukasiewicz, Annales scientifiques de l'Université de Clermont-Ferrand*, 1978.

⁷⁵ Shahid Rahman, *Notions basiques de logique modale propositionnelle*, 2015.

varier d'un monde à l'autre, en fonction des croyances des agents dans un monde donné ou dans le temps. Cette logique permet de raisonner sur des événements qui doivent arriver (nécessité) ou qui peuvent arriver (possibilité). En informatique, elle est utilisée pour la vérification formelle de programmes, notamment dans le *model-checking*. Ce terme désigne une méthode qui a été développée par Clarke, Emerson et Sifakis (lauréats du prix Turing en 2007). Cette approche est largement employée dans l'industrie des circuits intégrés et des systèmes embarqués pour concevoir des systèmes complexes qui soient conformes à des exigences de sécurité dans des environnements extrêmes. En philosophie, la logique modale aide à discuter des vérités nécessaires ou contingentes, comme par exemple l'argument ontologique de l'existence de Dieu qui a été modélisé par Kripke. **La logique intuitionniste, qui approfondit la logique modale, rejette le principe du tiers exclu – selon lequel une proposition est soit vraie, soit fautive – affirmant que si P est vrai, non P n'est pas nécessairement faux.** Introduite en 1948 par Luitzen Egbertus Brouwer, cette logique utilise des systèmes de preuves dits « constructivistes », où les preuves dépendant du tiers exclu ou de la contradiction sont rejetées.

Depuis plusieurs années, la logique non booléenne a été progressivement écartée des programmes scolaires de mathématiques au profit de concepts jugés plus applicables ou fondamentaux. Étant souvent limitée à des domaines spécifiques comme l'informatique et l'intelligence artificielle, il a été considéré que la maîtrise de la logique non booléenne n'était pas essentielle pour la plupart des étudiants dans leur insertion professionnelle. Par conséquent, les formations se sont recentrées sur la logique booléenne, qui est plus directement applicable pour résoudre des problèmes pratiques. **La logique non booléenne est pourtant cruciale pour comprendre la superposition et l'intrication des états dans les environnements réels et quantiques. Son absence des programmes éducatifs peut poser un obstacle majeur à la formation de professionnels compétents dans ces domaines.** Intégrer

ces concepts dans les curriculums de mathématiques est essentiel pour préparer efficacement les futurs ingénieurs et faciliter l'adoption des technologies quantiques. **En effet, cela donnerait aux élèves des clés conceptuelles pour comprendre les impacts réels de la mécanique quantique.**

Pourtant, la logique non booléenne reste enseignée dans plusieurs pays, notamment au niveau universitaire. Aux États-Unis, des institutions comme le MIT et Stanford incluent la logique formelle dans leurs cours de mathématiques avancées et de sciences cognitives. En Inde, la logique non booléenne a une résonance culturelle profonde, liée à l'histoire des écoles de logique indiennes telles que le Nyaya⁷⁶ ou la philosophie jaïne⁷⁷. Certains Instituts Indiens de Technologie (IIT) enseignent donc des aspects de logique multivalente ou floue, notamment en ingénierie et en gestion des systèmes industriels complexes. Au Japon, la logique floue est intégrée dans les cursus technologiques en raison de la tradition en ingénierie et robotique, pour la construction de systèmes de contrôle avancés et en sciences de la décision. En Allemagne, la logique non booléenne est enseignée dans les départements de philosophie et de mathématiques, en lien avec la recherche en intelligence artificielle et la modélisation des systèmes de décision. Enfin, en Italie, la Scuola Normale Superiore di Pisa en Italie avance la recherche en logique modale et multivalente⁷⁸, contribuant ainsi à l'évolution de la représentation de la connaissance et du raisonnement informatique.

⁷⁶ Le Nyaya établit la vérité par des « pramanas » ou moyens de connaissance. Les pramanas incluent l'expérience sensorielle, l'inférence, la comparaison et le témoignage. Le système considère que la vérité peut être confirmée par plusieurs méthodes et non seulement par des valeurs binaires.

⁷⁷ Philosophie qui introduit la logique non booléenne à travers le concept de « Anekāntavāda » (la doctrine de la pluralité des aspects) et « Syādvāda » (la doctrine du conditionnement). La doctrine de l'Anekāntavāda affirme que la réalité est complexe et que les vérités ne peuvent être comprises que sous plusieurs perspectives, qui vont au-delà de la dichotomie vrai / faux. La doctrine du Syādvāda stipule que toutes les propositions doivent être considérées en fonction de différentes conditions et perspectives, ce qui signifie qu'une proposition peut être vraie ou fautive, selon le contexte.

⁷⁸ Mario Piazza ; Gabriele Pulcini ; Matteo Tesi, Fractional-valued modal logic, 2021.

Institué par la loi d'orientation et de programmation pour la refondation de l'École de la République du 8 juillet 2013, le Conseil supérieur des programmes émet des avis et formule des propositions sur l'élaboration des programmes d'enseignement primaire, secondaire et supérieur, et s'assure de leur cohérence. Par une lettre de saisine du 13 mars dernier de la ministre de l'Éducation nationale et de la Jeunesse, il a été chargé de refondre le socle commun de connaissances, de compétences et de culture, et en particulier de réécrire les programmes de français et de mathématiques des cycles 3 et 4. Les programmes de mathématiques du cycle se prêtent tout particulièrement à la logique non booléenne. Leur harmonisation et leur révision doivent entrer en vigueur en 2026. **Cependant, dans la lettre de saisine du 13 mars dernier qui détaille les grandes orientations de cette refonte, la logique non booléenne n'est pas mentionnée alors que la prise en compte des apports concrets de l'IA, au travers de l'utilisation raisonnée des possibilités offertes par les outils», fait l'objet d'un paragraphe entier.** Pourtant, la lettre propose de mettre en place un programme d'initiation à la pensée informatique dès le cycle 3 et de mettre à jour les programmes d'informatique au cycle 4 pour permettre le développement d'une pensée informatique en lien avec le programme de technologie. **Dans le programme de technologie du cycle 4, qui a été rendu suite à une lettre de saisine d'avril 2023, le renforcement de la pensée informatique fait l'objet d'un paragraphe détaillé autour de notions comme la « logique spiralaire de complexité croissante » mais la logique non booléenne n'y est jamais mentionnée.** Cette pensée informatique inclut uniquement l'analyse externe et interne de systèmes techniques plus ou moins complexes, et la conception de solutions concrètes dans des « mini-projets techniques ».

L'intelligence artificielle (IA) est un bon repère des possibles, où bien que les compétences statistiques ne soient pas toujours omniprésentes chez les ingénieurs, de nombreux ingénieurs d'application savent aujourd'hui déployer des algorithmes avec succès car les problèmes sont bien définis. À titre d'exemple, distinguer un chat d'un

chien est un problème clairement formulé, ce qui permet aux ingénieurs de mobiliser des compétences pertinentes, quel que soit le langage de programmation utilisé. En revanche, dans le domaine quantique, sans une sensibilisation adéquate aux méthodes non booléennes, il est beaucoup plus difficile de définir correctement les problèmes dès le départ.

Recommandation 6

Intégrer des compétences fondamentales faisant appel à la logique mathématique non binaire (dite logique non booléenne) dans les programmes mathématiques révisés du cycle 4 qui seront prochainement publiés par le Conseil Supérieur de Programmes. Ces compétences doivent inclure les deux grands ensembles théoriques de la logique non booléenne que sont les écoles de logique floue (dite *fuzzy logic*), et en particulier de la logique multivalente, et de logique modale avec une attention particulière pour les systèmes de preuve dits « constructivistes » de la logique intuitionniste. Ce sont ces ensembles théoriques qui permettent d'analyser et de construire des systèmes techniques non binaires, dans lesquels une proposition n'est pas uniquement vraie ou fausse. Surtout, **ce sont ces bases théoriques qui permettront aux élèves intéressés par la filière quantique de modéliser correctement des problèmes quantiques par nature, pour ensuite les transposer dans des environnements réels / industriels.**

3 Une méthode pour porter un marché haut de gamme avec cette offre

L'avance française en matériel quantique doit permettre de créer un marché mondial du quantique, en s'appuyant sur des partenaires européens pour conserver une spécificité propre. De la même manière qu'Apple a créé le marché de l'appareil (mobile, tablettes, montres connectées, ordinateur) ou que Chat GPT a créé le marché de l'IA conversationnelle et des modèles de langage, des entreprises françaises peuvent aujourd'hui créer un marché de la « haute couture » du calcul complexe et de la sécurité haute précision.

Le gouvernement français a considéré que le quantique était un pari d'avenir majeur, au même titre que l'IA – en investissant le même montant – le quantique représentant déjà 12 % du budget de France 2030, alors que le marché mondial du quantique n'est aujourd'hui valorisé qu'à 1,3 Md \$⁷⁹ contre près de 215 Mds \$ pour l'IA⁸⁰.

Non seulement cela témoigne d'un décalage entre la réalité du marché et les investissements consentis par le secteur public, mais en plus les résultats ne sont pas au rendez-vous des investissements réalisés. De fait, si l'Europe et les États-Unis adressent tous deux près de 30 % du marché du quantique, les États-Unis ont pourtant investi 3 Mds € dans ce marché, soit moins de la moitié des 7 Mds € investis par les Européens⁸¹. **Cela témoigne d'un marché encore essentiellement porté par le secteur public en Europe, qu'il faut donc créer de toutes pièces pour le rendre concurrentiel et dynamique.**

⁷⁹ Markets and markets, Quantum Computing Market Size, 2023.

⁸⁰ Markets and markets, Technology Roadmap of Artificial Intelligence Market, 2023.

⁸¹ BCG, L'informatique quantique : la course que l'Europe ne doit pas perdre, 2022.

3.1. DÉPLOYER UNE OFFRE QUANTIQUE FRANÇAISE À VOCATION INTERNATIONALE

Malgré notre avance technologique, la plupart des projets quantiques sont aujourd’hui au stade de preuve de concept (POC). Certains usages concrets commencent toutefois à se matérialiser, en ce qui concerne l’amélioration des prévisions de calcul, l’optimisation et la simulation avancée. D’autres usages sont toutefois encore tributaires de verrous technologiques importants, et mettront plusieurs décennies à se matérialiser.

Pour se projeter dans le moment où les avantages quantiques commenceront à se matérialiser, et orienter les choix stratégiques des décideurs publics et privés, l’Institut Montaigne a identifié les usages les plus prometteurs pour les principales technologies quantiques existantes que sont l’informatique quantique, les capteurs et la communication quantique. Ces technologies quantiques ont un impact plus ou moins fort en fonction des secteurs d’activité et des impacts métiers directs. Le risque cyber est lui aussi à prendre en compte, en fonction de la criticité de chaque acteur.

Pour tester les avantages quantiques sur des usages réels, il faut les simuler à l’aide de machines faisant intervenir de l’informatique classique, soit les machines dites « analogiques ». À partir de la robustesse et de la fiabilité du matériel quantique européen, deux priorités doivent guider l’action des décideurs publics et privés pour sécuriser une offre quantique compétitive sur le plan mondial :

- i) **Sécuriser l’accès aux interfaces standardisées**, soit les couches permettant à différents systèmes informatiques de communiquer entre eux et ainsi faire le lien entre l’environnement quantique et l’environnement binaire (émulateurs et cloud).
- ii) **Développer des applications et algorithmes quantiques sur des usages démontrés** pour capitaliser sur les avancées majeures réalisées par les acteurs français spécialisés dans la conception des ordinateurs et autres technologies quantiques (matériel).

Malgré les nombreuses incertitudes scientifiques et technologiques qui demeurent, il y a toutefois un consensus au sein de l'écosystème quantique et économique au sens large, sur le fait que les technologies quantiques ont une probabilité élevée de fonctionner dans un avenir proche. L'incertitude porte essentiellement sur le niveau de performance des futurs calculateurs quantiques (taux d'erreurs, nombre de qubits logiques, etc.) et de la montée à l'échelle des technologies habilitantes associées⁸². Néanmoins, tous les scénarios prospectifs montrent qu'il y aura *a minima* une coexistence entre des machines de type NISQ et des machines analogiques dans les centres HPC. Dans les scénarios les plus optimistes, les processus industriels sont toutefois durablement impactés, que ce soit dans le cadre d'une arrivée de processeurs de type FTQC ou d'un « saut quantique » avec des architectures modulaires permettant d'interconnecter des FTQC entre eux. **En tout état de cause, les ordinateurs quantiques ne pourront vraisemblablement pas se développer de manière indépendante du HPC.**

Quel que soit le scénario retenu, les technologies quantiques auront un impact économique majeur pour les entreprises qui peuvent capitaliser sur des gains significatifs dès que la correction d'erreur sera améliorée (palier à 128 qubits logiques de Proqima), ou sur un *first mover advantage*, car elles se seront préparées à l'avènement du FTQC.

- a. Adresser prioritairement les applications de calcul intensif pour la simulation de systèmes complexes et pour optimiser des grands systèmes

Comme beaucoup de technologies de rupture, c'est aujourd'hui sur le plan militaire que l'informatique quantique est considérée comme une « révolution technologique » et une « priorité stratégique ».

⁸² CEA ; Futurable, *Quantum 2042 : étude prospective sur les impacts du calcul quantique en 2042*, Avril 2024.

Dans le Document de référence de l'Orientation de l'Innovation de Défense (DrOID) de 2023⁸³, c'est parce que le calcul quantique permet de traiter de nombreuses opérations en même temps qu'il est considéré comme une rupture stratégique. Une fois les verrous de la variabilité et du nombre de qubits levés (*Cf supra*), le calcul quantique sera un catalyseur pour de nombreuses actions : optimiser les systèmes d'information, planifier les missions militaires, exploiter le renseignement, résoudre des problèmes liés aux champs électriques et magnétiques ou encore modéliser des systèmes physiques.

Plusieurs secteurs et industries seront en mesure de bénéficier tout particulièrement de l'informatique quantique à correction d'erreurs avec des avantages partagés et spécifiques à chaque secteur.

*Le secteur de la chimie, de la santé
pharmaceutique et de la biotechnologie*

Pour les entreprises pharmaceutiques, l'informatique quantique est un outil puissant pour améliorer les capacités de modélisation et de simulation des molécules. En effet, il permet de modéliser les interactions de ces molécules entre elles, ainsi que leurs propriétés physiques en fonction de leur environnement.

À court-terme, des POCs ont démontré que le calcul quantique permet d'améliorer les prédictions de propriétés de composés chimiques avant leur synthèse, ce qui accélère la mise au point de nouveaux traitements. Par exemple, le laboratoire Roche s'est associé en 2021 avec Cambridge Quantum Computing⁸⁴ pour tester l'efficacité des

⁸³ Les priorités du Document de Référence de l'Orientation de l'Innovation de Défense (DrOID) de 2023 sont cohérentes avec les avancées technologiques des acteurs de l'informatique quantique et la réalité des menaces militaires actuelles. Elles nous donnent une indication précieuse du type d'applications civiles quantiques qui pourraient se matérialiser dans un futur proche.

⁸⁴ *The Quantum Insider, CQC, Roche Partner to Use Quantum Algorithms to Tackle Drug Discovery for Alzheimer's Disease, 2021.*

algorithmes quantiques pour améliorer la découverte de médicaments en phase précoce, pour des maladies comme Alzheimer. Il est apparu que ce type d'algorithme permet de simuler de manière plus précise les interactions entre des candidats-médicaments et des cibles biologiques complexes, réduisant ainsi des besoins de tests coûteux et chronophages. En effet, ils améliorent le criblage virtuel qui permet de sélectionner les molécules les plus prometteuses pour ensuite faire des essais cliniques. Contrairement aux méthodes classiques qui nécessitent des simulations approximatives ou des tests *in vitro* onéreux, les algorithmes quantiques sont capables d'explorer simultanément plusieurs configurations moléculaires possibles grâce à la superposition et à l'intrication. Cela permet de simuler des interactions complexes à l'échelle subatomique, comme celles entre un médicament potentiel et des milliers de cibles biologiques différentes, éliminant ainsi de nombreuses hypothèses erronées avant même que des expériences en laboratoire ne soient lancées. Roche exploite ainsi la plateforme EUMEN de Cambridge Quantum Computing⁸⁵, qui est une suite d'algorithmes et d'outils de calcul quantiques conçue spécifiquement pour simuler des processus chimiques dont la complexité augmente avec le nombre d'atomes qu'il faut simuler.

L'informatique quantique ouvre de nouvelles perspectives pour la conception de processus de synthèse plus efficaces, comme l'a démontré l'expérience menée en janvier dernier par Dow Chemical en partenariat avec IonQ et 1QBit⁸⁶. Ce projet visait à optimiser les chemins de réaction chimique en réduisant les coûts et en améliorant l'efficacité des procédés. En juin dernier, Unilever a également exploré ces potentialités en s'associant avec Microsoft⁸⁷ pour tester des algorithmes quantiques capables d'optimiser la formulation chimique de leurs produits de consommation (savons, shampoings). **C'est ainsi que l'industrie chimique dans son ensemble pourrait bénéficier d'avantages**

⁸⁵ DCD, Roche strikes quantum computing deal to develop early-stage Alzheimer's drugs with CQC, 2021.

⁸⁶ IONQ, A New Approach for Accurately Simulating Larger Molecules on IonQ Computers, Janvier 2024.

⁸⁷ Unilever, La recherche et développement dans le futur : Comment Unilever transforme l'innovation avec Microsoft, Juin 2024.

quantiques sur de nombreux usages, qui sont encore à tester et à démontrer. En simulant avec précision la structure électronique et les interactions atomiques, il devient possible de concevoir des matériaux innovants adaptés à des applications spécifiques. Par exemple, les batteries de nouvelle génération pourraient être rendues plus performantes par des algorithmes quantiques, et les catalyseurs utilisés pour la production d'hydrogène ou la conversion de CO₂ pourraient être améliorés en simulant la structure électronique et les interactions atomiques de manière plus fine. Un catalyseur, dans ce contexte, est une substance qui accélère une réaction chimique sans être consommée par celle-ci, augmentant ainsi l'efficacité des processus industriels. L'un des défis historiques de l'industrie chimique concerne l'optimisation des réactions elles-mêmes. Les paramètres comme la température, la pression ou le choix des catalyseurs nécessitent souvent un *fine-tuning* laborieux. L'informatique quantique pourrait révolutionner cet aspect en permettant une modélisation précise et rapide de ces variables, maximisant ainsi les rendements et réduisant les sous-produits indésirables. Par exemple, l'entreprise BASF, qui utilise des catalyseurs dans près de 80% de ses processus de production, s'est associée en février 2023 avec le consortium QuPharma mené par l'entreprise américaine SEEQC⁸⁸ pour explorer l'utilisation des simulateurs quantiques pour concevoir de nouveaux matériaux polymères et des solutions énergétiques durables. En exploitant les algorithmes quantiques, BASF peut réduire les essais et les erreurs liés à la création de catalyseurs plus efficaces, ce qui pourrait réduire la consommation d'énergie dans des processus tels que la méthode Haber-Bosch, qui est très énergivore et permet de synthétiser l'ammoniac. Cette méthode consomme à elle seule 1 à 2% de la production mondiale d'énergie chaque année.

À plus long terme, le calcul quantique pourrait être utilisé pour modéliser toutes sortes de molécules plus ou moins complexes⁸⁹, pour faire de l'analyse génomique avancée et éventuellement

⁸⁸ *The QUantum Insider, SEEQC Partners With BASF To Explore Applications of Quantum Computing in Chemical Reactions for Industrial Use, 2023.*

⁸⁹ *Pennylane, Top 20 molecules for quantum computing, Janvier 2024.*

modéliser la structure de certaines protéines. Sur l'hydrogène, IBM et Google ont démontré la capacité des ordinateurs quantiques à calculer l'état fondamental de la molécule plus précisément⁹⁰. Sur le benzène, une molécule plus complexe utilisée pour comprendre des structures électroniques, Google a réussi à modéliser des orbitales moléculaires, pour décrire le comportement des électrons dans la molécule. Enfin, l'informatique quantique ouvre des perspectives de modélisation de repliement protéique, qui consiste à prédire la structure complète d'une protéine à partir de sa séquence⁹¹, ce qui permettrait de progresser dans le traitement de nombreuses maladies neurodégénératives. De fait, de nombreuses protéines, comme l'insuline, ne sont pas encore modélisables rapidement dans les environnements binaires de l'informatique classique.

Le calcul quantique gagne aussi à s'enrichir d'autres technologies de rupture, au premier rang desquelles l'intelligence artificielle, pour améliorer la détection précoce de certaines pathologies. Récemment, Pasqal a démontré que pour des cas de dépistage de toxicité à partir d'une structure moléculaire, l'informatique quantique combinée à du *machine learning* est jusqu'à 20 000 fois plus efficace que si ces deux procédures étaient conduites séparément. Le nouveau simulateur de Qubit Pharmaceuticals Hyperion-1 a réussi à simuler des molécules avec environ 20 qubits au lieu de 250 en couplant du calcul haute performance avec du calcul quantique.

Enfin, des disciplines de recherche comme la génétique quantique⁹², au croisement de la mécanique quantique et de la génétique, font aujourd'hui leur apparition pour optimiser les traitements existants contre des pathologies graves. De fait, les fluctuations quantiques semblent jouer un rôle encore à définir dans la structure et le

⁹⁰ *Communication Physics, Simulating molecules on a cloud-based 5-qubit IBM-Q universal quantum computer, 2021.*

⁹¹ *Jacques M. Bahi ; Wojciech Bienia ; Nathalie Côté ; Christophe Guyeux, Is protein folding problem really a NP-complete one?, 2013.*

⁹² *Medium, J. Lamri, (Prospective) Les promesses de la génétique quantique, Décembre 2022.*

fonctionnement des protéines, et dans le transfert de l'information génétique. Si des molécules biologiques, ou même l'ADN, s'avèrent être perméables aux influences quantiques, les perspectives d'innovation pouvant se matérialiser dans les années à venir sont infinies, des vaccins quantiques utilisant des algorithmes de calcul quantique pour cibler plusieurs gènes à la fois en contrant une maladie infectieuse, à des implants médicaux quantiques pour des patients atteints de maladies chroniques qui pourraient mesurer en temps réel les signes vitaux d'un patient tels que le rythme cardiaque ou la pression artérielle.

Zoom sur les problèmes à N corps en chimie, que le calcul quantique pourrait permettre de mieux simuler et, à terme, de résoudre

Les problèmes à N corps sont au cœur de nombreux défis en recherche fondamentale, notamment dans les domaines de la physique nucléaire, de la physique du solide et de la chimie. Ces problèmes impliquent l'étude des interactions entre un grand nombre de particules, telles que les électrons, les noyaux atomiques ou les atomes dans un matériau. La complexité de ces systèmes réside dans le fait que chaque particule interagit avec toutes les autres, rendant les simulations et les calculs extrêmement compliqués. Le calcul quantique émerge aujourd'hui comme une solution prometteuse pour aborder ces défis. En utilisant des algorithmes quantiques et des ordinateurs quantiques, il devient possible de modéliser de manière plus fine les interactions complexes entre les particules à l'échelle atomique.

Un exemple concret est la recherche sur les matériaux supraconducteurs à température ambiante. Actuellement, la supraconductivité n'est observée qu'à des températures très basses, ce qui

limite les applications pratiques de cette propriété. Les simulations quantiques permettent d'étudier des systèmes moléculaires et des structures cristallines avec une précision telle que l'on peut prédire et concevoir de nouveaux matériaux susceptibles de devenir supraconducteurs à température ambiante. Des progrès dans ce domaine pourraient induire des innovations de rupture dans le stockage et la transmission d'énergie.

*Le secteur de l'industrie manufacturière
et du transport (routier / ferroviaire)*

Avec des chaînes de production de plus en plus complexes à mesure de l'intensification des échanges, le secteur de l'industrie manufacturière et du transport est confronté à de forts enjeux logistiques en matière d'optimisation de processus et d'approvisionnement. Le calcul quantique pourrait avoir de nombreux impacts sur l'ensemble de la chaîne d'approvisionnement et des méthodes de production et de distribution en traitant plus efficacement – car en parallèle – des milliers de variables interconnectées.

À court terme, l'optimisation des routes de transport, prenant en compte les itinéraires en fonction de la circulation, des conditions météorologiques et des restrictions de livraison, est l'un des rares domaines où les projets de calcul quantique franchissent le stade de POC. L'entreprise canadienne D-Wave a développé des applications quantiques opérationnelles et efficaces dans divers secteurs⁹³. Leur technologie est intégrée dans la solution HyperOptimized Nodal Efficiency Engine (HONE), développée par SavantX, une entreprise spécialisée dans les solutions d'optimisation et de gestion des ressources basées sur

⁹³ D-Wave, *Unlocking the Power of Quantum: Applications in Production with D-Wave*, 2024.

l'intelligence artificielle et les technologies avancées. Cette solution est utilisée pour améliorer les opérations au Port de Los Angeles. HONE utilise l'*annealing* quantique, une technique de calcul quantique développée par D-Wave. L'*annealing* quantique est un processus qui utilise les principes de la mécanique quantique pour résoudre des problèmes d'optimisation complexes en recherchant des configurations optimales parmi de nombreuses possibilités (Cf. encadré *infra*). Grâce à cette approche, HONE a considérablement amélioré l'efficacité des opérations portuaires, réduisant les besoins en ressources pour les grues RTG (Rubber-Tired Gantry) utilisées au déchargement de 40% et diminuant le temps de rotation des camions de 30%. Ce cas illustre comment les applications quantiques de D-Wave peuvent offrir une valeur commerciale tangible. **De plus, ExxonMobil en partenariat avec IBM cherche à optimiser les itinéraires de flottes de navires marchands à l'échelle mondiale**⁹⁴. Leur objectif est d'améliorer la prise de décision en temps réel en analysant de vastes ensembles de données pour identifier les risques, tels que les retards dus aux conditions météorologiques ou aux pannes de matériel, et en proposant des stratégies pour les atténuer. **Cette approche montre le potentiel du calcul quantique pour développer une logistique urbaine intelligente, prédictive et réactive, capable de prendre en compte une multitude de facteurs.**

Comprendre la parallélisation et l'*annealing* quantique

- La parallélisation se réfère à l'exécution simultanée de plusieurs tâches ou opérations. Dans le contexte de l'informatique quantique, elle implique souvent l'utilisation de plusieurs qubits ou processeurs quantiques pour effectuer des calculs en parallèle.

⁹⁴ IBM, ExxonMobil s'efforce de résoudre des défis énergétiques complexes, 2020.

Cette approche permet d'accélérer le traitement de problèmes complexes en répartissant la charge de travail sur plusieurs unités de traitement. Par exemple, dans les systèmes quantiques utilisant des qubits en réseau, la parallélisation peut permettre à différents qubits d'exécuter des parties d'un algorithme simultanément, augmentant ainsi l'efficacité et la vitesse du calcul.

- L'*annealing* quantique est un type d'ordinateur quantique spécifiquement conçu pour résoudre des problèmes d'optimisation. Il utilise les principes de la mécanique quantique pour trouver des solutions optimales à des problèmes complexes, où l'objectif est de trouver la meilleure solution parmi un grand nombre de possibilités. Ils initialisent un système quantique dans un état simple et facile à atteindre et le font évoluer vers un état de moindre énergie qui correspond à la solution optimale du problème. Dans le cadre du chauffage de matériaux, par exemple, cela permet d'utiliser une montée graduelle en température. Les *annealers* ne sont pas considérés comme des ordinateurs quantiques universels, car ils sont optimisés pour une classe spécifique de problèmes et ne peuvent pas exécuter l'ensemble des algorithmes quantiques.

À long-terme, le calcul quantique revêt un potentiel important sur toutes les étapes de la chaîne de production de l'industrie manufacturière. En amont, des entreprises comme BMW Group et Honeywell Quantum Solution ont par exemple développé des optimisations pour la planification de la production⁹⁵ en tenant compte des contraintes de ressources, des délais et des coûts pour créer des plannings de production plus efficaces. En aval, l'entreprise BASF s'appuie par exemple sur Pasqal

⁹⁴ Honeywell, *How BMW Can Maximize Its Supply Chain Efficiency with Quantum*, 2024.

pour modéliser des schémas climatiques extrêmes liés au changement climatique et ainsi affiner ses prévisions sur les rendements et croissances de cultures⁹⁶. Les équipes de Pasqal ont aussi démontré que le QPU pouvait traiter ces calculs de manière plus efficace, réduisant ainsi le temps nécessaire pour planifier et gérer les satellites⁹⁷. De manière générale, l'optimisation de la gestion des stocks et des entrepôts permet d'ajuster les niveaux de stock en fonction de la demande prévue et des coûts de stockage, réduisant ainsi les coûts de surstockage et de rupture de stock. Le calcul quantique pourrait améliorer le placement des hubs logistiques à l'échelle d'un pays ou d'un continent en calculant des itinéraires optimisés pour optimiser les flux des camions et maximiser la couverture d'un marché en proposant de meilleurs délais de livraison à plus de clients. La même logique pourrait être appliquée à l'organisation des entrepôts, par exemple en optimisant le placement des produits pour minimiser le temps et le coût de préparation des commandes. Ainsi, CMA CGM s'est associé à Pasqal début juillet 2024 pour créer un centre d'excellence quantique dédié à la gestion des flux de conteneurs dans les ports et l'optimisation du placement sur les navires marchands⁹⁸.

Le secteur de l'énergie et le développement durable (dans tous les secteurs)

Le calcul quantique est aujourd'hui utilisé à titre essentiellement prospectif pour développer des énergies renouvelables, en investissant les domaines de la production et du pilotage de l'efficacité énergétique.

⁹⁶ *Les Numériques, Le quantique au défi des prédictions météorologiques, 2022.*

⁹⁷ *panel pendant l'événement Pasqal Thoughts d'avril 2024.*

⁹⁸ *CMA CGM, CMA CGM Group and Pasqal join forces to leverage quantum technologies for maritime transport and logistics, juillet 2024.*

En ce qui concerne la production d'énergies renouvelables, les POCs utilisent le calcul quantique pour optimiser le placement des centrales électriques, en intégrant les nombreuses variables associées à l'éolien et au solaire, pour *in fine* optimiser les rendements de la production d'énergie renouvelable. Par exemple, le calcul quantique se prête bien aux méthodes existantes pour identifier les emplacements optimaux pour les éoliennes ou les panneaux solaires en tenant compte de facteurs tels que les modèles de vent, l'exposition à la lumière du soleil et les contraintes d'utilisation des terres. Améliorer ces méthodes avec des algorithmes plus puissants permettrait de maximiser la quantité d'énergie produite tout en réduisant l'impact environnemental de ces installations. Pour atteindre ces objectifs, EDF s'est associée avec Quandela dès novembre 2022 pour étudier les apports du calcul quantique sur la déformation des barrages hydroélectriques pour mieux prédire le vieillissement des matériaux et améliorer la sécurité⁹⁹.

En ce qui concerne le pilotage de l'efficacité énergétique, les POCs utilisent le calcul quantique pour rendre les réseaux de transport et de distribution d'énergie plus intelligents, et ainsi réduire les coûts associés au stockage de l'énergie dans des systèmes décentralisés.

- **Sur la planification de réseaux électriques intelligents**, le calcul quantique pourrait être utilisé pour améliorer les prédictions de la demande énergétique à différents niveaux du réseau de transport, même s'il est décentralisé. En analysant de grandes quantités de données en temps réel, les algorithmes quantiques peuvent aider à anticiper les fluctuations de la demande et à ajuster la distribution d'énergie en conséquence, ce qui peut contribuer à éviter les pannes et à optimiser l'utilisation des ressources. Les réseaux de transport d'énergie, tels que les lignes électriques et les pipelines, sont complexes et nécessitent une planification précise pour maximiser l'efficacité et minimiser les pertes d'énergie.

⁹⁹ *L'Usine Digitale, EDF fait appel à Quandela... L'actu du quantique en France cette semaine, 2022.*

- **Sur l'optimisation des systèmes de stockage**, ce sont les systèmes de recharge de parcs de véhicules électriques – *vehicule-to-grid* – qui font l'objet de POCs, en utilisant le calcul quantique pour prendre en compte, en temps réel, tous les véhicules branchés sur un réseau décentralisé et redistribuer l'énergie en fonction des besoins de manière plus dynamique. EDF s'est par exemple associé avec Pasqal dès 2020 pour éclairer la recharge intelligente dite « *vehicule-to-grid* » avec le calcul quantique¹⁰⁰. L'objectif est d'utiliser l'énergie des batteries des voitures électriques pour les besoins du réseau lorsqu'elles ne roulent pas, problème aujourd'hui hors de portée des supercalculateurs classiques en raison de l'explosion combinatoire induite par l'augmentation constante du nombre de véhicules. À plus long terme, si des algorithmes quantiques parviennent à mieux prédire les bandes de valence¹⁰¹, cela permettrait de construire des systèmes de captage, stockage et utilisation du CO₂ (CCUS) avec des matériaux dits « absorbants » pour mieux piéger puis stocker définitivement le CO₂, sur lesquels Total Energies a entamé des travaux de recherche appliquée dès 2020¹⁰², en partenariat avec Cambridge Quantum Computing. Depuis 2022, IBM et Mercedes sont allés encore plus loin en explorant la « super absorption » à l'aide du calcul quantique¹⁰³, soit un procédé qui tirerait parti de la concentration de molécules pour inverser le déroulement de la charge d'une batterie et le rendre très rapide. Si cette expérimentation s'avère concluante, elle pourrait donner lieu à des batteries quantiques avec une autonomie de plus d'un million de kilomètres, qui se chargeront plus rapidement que des smartphones.

¹⁰⁰ EDF, *Quantique et mobilité électrique ? Un partenariat prometteur !*, 2020.

¹⁰¹ *La zone d'énergie occupée par les électrons d'un matériau à l'état solide qui sont liés aux atomes et participent aux liaisons chimiques. Dans un semi-conducteur ou un isolant, c'est la dernière bande d'énergie complètement remplie à température ambiante. Les électrons de cette bande ne sont pas libres de se déplacer, sauf s'ils reçoivent suffisamment d'énergie pour passer dans la bande de conduction, où ils peuvent contribuer à la conduction électrique.*

¹⁰² Total Energy, *Total explore les algorithmes quantiques pour améliorer le captage de CO₂*, 2020.

¹⁰³ NeoZone, *IBM et Mercedes travaillent sur une batterie quantique avec une autonomie d'1 million de kilomètre (sans recharge)*, 2022.

Une convergence possible entre le calcul quantique et l'intelligence artificielle sur l'efficacité énergétique

Le calcul quantique est utile pour résoudre des problèmes complexes liés au changement climatique¹⁰⁴, en étant au service de la sobriété (*quantum for green*), mais aussi pour repenser nos modèles existants en optimisant la quantité de calcul nécessaire pour produire un résultat, soit vecteur de sobriété (*green quantum*).

- Le quantique au service de la sobriété concerne par exemple la simulation de phénomènes physiques pour trouver de nouveaux matériaux renouvelables comme les cellules photovoltaïques ou les batteries. Néanmoins, de nombreuses solutions d'IA sont aussi utilisées pour atteindre les mêmes résultats, avec des bits et non des qubits. Par exemple, la [plateforme Materials Project](#) utilise de l'IA pour analyser les données générées à partir de la structure électronique de ce type de matériaux et découvrir des propriétés. Les deux approches sont toutefois différentes, en ce que l'IA se réfère à des données réelles passées, avec un mode de fonctionnement probabiliste, tandis que le quantique se réfère à des états futurs potentiels, avec un mode de fonctionnement algébrique. **Loin de s'opposer, ces deux approches se complètent pour obtenir des résultats plus précis et plus représentatifs de l'évolutivité de notre environnement.**

¹⁰⁴ Casey Berger ; Agustin Di Paolo ; Tracey Forrest ; Stuart Hadfield ; Nicolas Sawaya ; Michal Stechly ; Karl Thibault, *Quantum technologies for climate change: Preliminary assessment*, 2021.

- Le quantique sobre se réfère à l'optimisation de la quantité de ressources physiques nécessaires, comme l'énergie totale requise pour effectuer un calcul donné. Dans un contexte où l'IA pourrait nous mettre face à un « mur énergétique »¹⁰⁵, compte tenu de la demande en électricité et en eau que nécessite l'entraînement des modèles, la mécanique quantique ouvre des pistes intéressantes. En effet, **les portes quantiques sont réversibles**¹⁰⁶, ce qui signifie que chaque opération quantique a une opération inverse qui peut restaurer l'état des qubits. Théoriquement, cela pourrait permettre de dissiper une quantité minimale de chaleur dans un système en annulant l'entropie¹⁰⁷ inhérente à tout système faisant intervenir de nombreuses variables, conformément au principe développé par Landauer en 1961. Concrètement, les scientifiques explorent ce champ pour réduire les coûts d'exploitation des infrastructures énergétiques existantes et la quantité d'énergie nécessaire à leur fabrication et à leur entretien¹⁰⁸.

¹⁰⁵ Google a annoncé une augmentation de 48 % de ses émissions de GES de 2019 à 2023 en raison de la propagation de l'IA dans ses data centers, et Microsoft une hausse de sa consommation d'énergie de 30 % par rapport à 2022 pour la même raison.

¹⁰⁶ Elles sont représentées par des matrices unitaires qui ont des inverses, donc la valeur d'entrée peut être déterminée par la valeur de sortie, alors que les portes logiques classiques qui manipulent des bits (AND, OR et XOR) ne sont pas réversibles, car il est impossible de déterminer avec certitude la valeur d'entrée des sorties (sauf pour la porte NOT qui est composée de 0 et de 1, donc si la sortie est 1, l'entrée est forcément 0, mais par déduction).

¹⁰⁷ Mesure systémique qui s'applique au champ de la thermodynamique (mesure de l'irréversibilité), de la physique statistique (mesure de l'incertitude) et de la théorie de l'information (mesure de la complexité).

¹⁰⁸ Möller, M., Vuik, C, *On the impact of quantum computing technology on future developments in high-performance scientific computing*. *Ethics Inf Technol* 19, 253–269 (2017).

*Le secteur de la finance
(banque / assurance)*

Le calcul quantique est exploré dans le secteur de la finance pour traiter de grandes quantités de données simultanément afin d'améliorer les stratégies d'optimisation de portefeuilles, en résolvant des problèmes de modélisation impliquant de nombreuses combinaisons possibles. Résoudre ce type de problème permet de sélectionner les meilleurs actifs et de maximiser les rendements tout en minimisant les risques. En raison de leur capacité à traiter un nombre bien plus élevé de variables et de contraintes simultanément, ces algorithmes sont adaptés à la gestion de portefeuille d'actifs sophistiqués. JPMorgan a par exemple collaboré avec le programme Q Network d'IBM dès 2017 pour mettre au point des algorithmes quantiques d'optimisation de portefeuilles financiers, d'évaluation de certaines classes d'actifs et d'analyse des risques¹⁰⁹. Ces algorithmes quantiques reposent sur une analyse prédictive des marchés financiers pour permettre aux gestionnaires de portefeuilles d'équilibrer leurs placements en temps réel.

À plus long-terme, le calcul quantique pourrait améliorer l'évaluation des risques et les stratégies d'optimisation de portefeuilles, en rendant les calculs plus précis grâce à une prise en compte plus fine des corrélations complexes entre différents facteurs de risque. Par exemple, les modèles quantiques peuvent intégrer des interrelations non linéaires entre les actifs, ce qui permet une meilleure gestion de la diversification et de l'allocation des ressources dans des portefeuilles complexes. De plus, des fonctionnalités avancées de *stress testing* permettent de simuler un large éventail de scénarios économiques, géopolitiques ou financiers, afin de mieux évaluer la résilience des portefeuilles face à des chocs potentiels. Ces tests peuvent également aider à identifier des vulnérabilités systémiques qui échappent aux modèles classiques. Dans cette optique, **le calcul quantique est actuellement testé pour l'analyse de vastes ensembles de**

¹⁰⁹ *Le Monde Informatique, Q Network : IBM concrétise l'informatique quantique avec ses clients, 2018.*

données dans le but de détecter des schémas inhabituels ou frauduleux en temps réel. Grâce à sa capacité à traiter et à analyser des données massives bien plus rapidement que les systèmes traditionnels, l'informatique quantique permettrait d'améliorer la détection de la fraude financière. Les institutions financières pourraient ainsi réagir plus rapidement aux menaces et réduire les pertes associées à des activités frauduleuses.

Les POCs actuels se concentrent sur les modèles d'évaluation des risques de crédit, en modélisant des comportements complexes et des corrélations subtiles dans les données de crédit à l'aide d'algorithmes quantiques pour affiner les analyses en matière de solvabilité des emprunteurs. La branche d'investissement et de financement du Groupe Crédit Agricole (CACIB) a par exemple lancé deux PoC pour optimiser la valorisation de produits financiers ainsi que la mesure des risques de crédit¹¹⁰. Le premier concerne l'optimisation de la valorisation de produits financiers complexes, tels que les dérivés, où le calcul quantique peut fournir des modèles plus précis en prenant en compte les corrélations de marché et les comportements stochastiques. Le second porte sur la mesure des risques de crédit, où les capacités de simulation et de modélisation avancées de l'informatique quantique permettent de mieux anticiper les scénarios de défaut et d'ajuster les stratégies de couverture en conséquence.

b. Investir dans les capteurs quantiques et la métrologie pour améliorer les outils de mesure classiques

Les capteurs quantiques figurent parmi les priorités identifiées dans le Document de Référence de l'Orientation de l'Innovation de Défense (DrOID) de 2023, en raison de leur capacité à surpasser les outils de mesure classiques par un facteur de 10 à 100¹¹¹, tant en précision qu'en stabilité. Par exemple, certains capteurs inertiels

¹¹⁰ Évènement Pasqal Thoughts, avril 2024.

¹¹¹ DRN, *Les enjeux de la physique quantique et les ruptures à anticiper*, 2020.

offrent une stabilité supérieure au système de navigation par satellite GNSS, permettant une navigation et une géolocalisation indépendantes des signaux GPS. Dans le domaine du renseignement électromagnétique (ROEM), les capteurs quantiques sont explorés pour leur capacité à affiner l'observation dans des environnements tels que l'espace, les fonds marins ou le cyberspace, avec une sensibilité accrue par rapport aux technologies actuelles. Ces avancées sont particulièrement prometteuses pour les sous-marins, drones et autres véhicules militaires opérant dans des zones où les signaux GPS sont indisponibles ou perturbés. En outre, les capteurs quantiques permettent de détecter des variations minimales du champ magnétique terrestre, telles que celles causées par des sous-marins, offrant une précision de détection accrue et à longue distance. Le groupe Thales s'investit activement dans ce domaine, notamment à travers le projet pilote ASTERIQs, qui vise à développer des centrales inertielles quantiques basées sur des atomes froids¹¹². Ces nouveaux capteurs, libérés de la dépendance au GPS¹¹³, pourraient permettre une précision de navigation au mètre près pour des vols tels qu'un Paris–New York, contre plusieurs kilomètres avec les gyroscopes optiques actuellement utilisés. Cette précision est déterminante en contexte opérationnel militaire, notamment en cas de brouillage des signaux GPS.

Dans le civil, des entreprises comme Mag4Health, une *spin-off* du CEA-LETI, développent des solutions de magnétoencéphalographie (MEG) basées sur les capteurs quantiques hélium 4¹¹⁴, qui fonctionnent à température ambiante, pour mieux comprendre les maladies neuronales comme Alzheimer et mieux préparer certaines chirurgies liées à l'épilepsie ou aux tumeurs cérébrales. Cela permet de placer des capteurs quantiques sur le crâne d'un patient et ainsi de recevoir ses signaux cérébraux de manière plus fine et précise. Mag4Health est ainsi parvenu à diviser par trois le coût total d'achat et

¹¹² Thalès, *Sortir les capteurs quantiques des laboratoires pour en faire des objets industriels, voilà le vrai défi*, 2023.

¹¹³ *Le Figaro*, Avec Thales, les technologies quantiques montent à bord des avions, 2023.

¹¹⁴ *Le Dauphiné*, Isère : Mag4Health, le quantique au service de la santé, 2023.

de maintenance de ces machines¹¹⁵. Les capteurs quantiques ont de fait le potentiel d'améliorer certaines techniques d'imagerie médicale comme l'imagerie par résonance magnétique (IRM), qui permet d'obtenir des vues en 2D ou 3D dans un corps, ou la tomographie, qui consiste à reconstruire le volume d'un objet à partir d'une série de mesures. Leur généralisation conduirait à une détection plus précoce des maladies, comme les cancers, et à un diagnostic plus précis, en détectant des biomolécules à forte sensibilité.

À plus long terme, les capteurs quantiques, grâce à leur résolution supérieure aux capteurs conventionnels, pourraient améliorer la détection et la modélisation de phénomènes complexes. Par exemple, les systèmes LIDAR, utilisant des photons intriqués pour mesurer avec plus de précision les distances entre objets, présentent des perspectives pour la navigation autonome dans des environnements faiblement éclairés ou soumis à des conditions météorologiques difficiles¹¹⁶. Ces technologies pourraient renforcer la fiabilité des systèmes autonomes dans des conditions où les capteurs classiques sont limités. Par ailleurs, les capteurs quantiques offrent des opportunités pour les missions d'exploration spatiale, où les systèmes GPS traditionnels ne fonctionnent pas. Dans cette logique, le projet CARIOQA (Cold Atom Rubidium Interferometer in Orbit for Quantum Accelerometry), financé par la Commission européenne, a pour objectif de placer, d'ici 2032, un accéléromètre quantique à bord d'un satellite d'observation de la Terre. Ce projet vise à démontrer l'application de l'interférométrie à atomes froids, soit une technique de mesure qui utilise des atomes froids pour détecter des variations infimes dans des champs physiques. Une des applications envisagées concerne la surveillance des effets du changement climatique, comme la mesure des concentrations de gaz à effet de serre. CARIOQA pourrait ainsi contribuer à l'amélioration des outils d'observation spatiale, avec des impacts dans la gestion des ressources environnementales et la prévision des changements climatiques.

¹¹⁵ CEA, *Mag4Health, la magnétoencéphalographie enfin accessible*, 2023.

¹¹⁶ *Trust My Science, LIDAR quantique : la nouvelle tech de détection qui ferait passer les véhicules autonomes au niveau supérieur ?*, 2023.

c. Anticiper les mutations qui seront générées par les communications quantiques pour la cybersécurité

Les communications quantiques pourraient transformer la manière dont les informations sont transmises et sécurisées, notamment dans le secteur militaire, et à plus long terme pour les fournisseurs de solutions de chiffrement. En particulier, la Chine investit massivement dans ce domaine et dépose de nombreux brevets relatifs à la distribution quantique de clés (QKD)¹¹⁷. Ce mécanisme de chiffrement est également identifié comme la troisième priorité dans le Document de Référence de l'Orientation de l'Innovation de Défense (DrOID) de 2023, en raison de sa capacité à détecter en temps réel toute tentative de piratage. La QKD permettrait ainsi de renforcer la sécurité des protocoles de communication, en s'appuyant sur les infrastructures optiques de télécommunication existantes. Cette technologie présente l'avantage de protéger les clés cryptographiques contre toute forme d'interception, car le principe de superposition en mécanique quantique garantit que toute tentative d'espionnage modifie l'état quantique du système, permettant une détection immédiate.

Cependant, le développement des ordinateurs quantiques pose également des risques pour les systèmes de cryptographie actuels. Par exemple, l'algorithme de Shor, qui peut factoriser efficacement de grands nombres, rend obsolètes les systèmes de cryptographie à clés asymétriques, tels que Rivest-Shamir-Adleman (RSA) et ECC (Elliptic Curve Cryptography), qui reposent sur la difficulté de factorisation. Ces clés utilisent un couple de clés – l'une publique pour le chiffrement, l'autre privée pour le déchiffrement –, dont la sécurité serait compromise par un ordinateur quantique capable de factoriser rapidement de grands nombres. Par ailleurs, l'algorithme de Grover, qui optimise la recherche dans des bases de données non structurées, pourrait également réduire la sécurité des

¹¹⁷ GQ, *How China became a subatomic superpower with quantum technology*, 2019 ITIF, *How Innovative Is China in Quantum?*, 2024.

systèmes de cryptage symétrique en diminuant le temps nécessaire pour deviner une clé de chiffrement.

Aujourd'hui, deux risques principaux sont identifiés dans ce contexte :

- 1. la compromission des algorithmes de chiffrement largement utilisés**, comme RSA et ECC, qui reposent sur la complexité de la factorisation ;
- 2. la collecte de données cryptées actuellement**, avec la possibilité qu'elles soient déchiffrées ultérieurement grâce aux ordinateurs quantiques.

L'enjeu à long-terme est donc de trouver le bon équilibre entre la sécurisation de nos réseaux de communication et leur potentielle reconfiguration structurelle qui nécessiterait d'inventer des méthodes encore plus robustes.

Les opérateurs télécoms pourraient à terme intégrer des technologies de communication quantique pour offrir des services de communication ultra-sécurisés aux gouvernements. À long terme, le développement d'un « Internet quantique » pourrait permettre des communications instantanées et sécurisées à travers le monde, bouleversant les fondations des réseaux actuels. **Par exemple, le projet européen EuroQCI cherche à rendre possible l'échange de clés quantiques sur de grandes distances par voie terrestre, mais également par satellite.** Au-delà de la sécurisation de données ultra-sensibles, ces nouveaux réseaux permettent de connecter des ordinateurs quantiques, augmentant leur puissance collective pour résoudre des problèmes complexes comme la modélisation moléculaire ou le climat. **Si l'essentiel de l'effort doit aujourd'hui reposer sur les fournisseurs de solutions de sécurité qui vont implémenter progressivement les algorithmes « post-quantiques », les entreprises doivent s'assurer que le niveau de sécurité fourni par les nouveaux moyens de chiffrement soit au moins équivalent au niveau pré-quantique.**

Recommandation 7

Confier à la Direction Générale des Entreprises (DGE), qui se situe au cœur de l'écosystème quantique, le soin de diffuser aux entreprises et aux investisseurs une feuille de route recensant les usages quantiques dans lesquels investir de manière à en retirer des avantages concurrentiels.

Ces usages concernent prioritairement :

1/ Le calcul intensif avec les applications qui font appel à de l'explosion combinatoire et du calcul en parallèle :

- Dans le secteur de la chimie / pharmaceutique, les usages prioritaires concernent la conception automatisée de processus de synthèse et la modélisation de molécules pour détecter des pathologies de manière plus précoce. Pour cela, il faut utiliser le calcul quantique pour concevoir des algorithmes qui permettent de modéliser des problèmes à N-corps, soient des problèmes qui étudient les interactions combinées d'un grand nombre de particules entre elles.
- Dans le secteur de l'industrie manufacturière / transport, les usages prioritaires concernent l'optimisation des routes de transport ou de la logistique avec des processus intelligents. Pour cela, il faut utiliser un certain type de calcul quantique – l'*annealing* ou recuit quantique – qui permet de trouver de manière itérative la solution optimale à un problème complexe parmi un nombre exponentiel de combinaisons possibles.
- Dans le secteur de l'énergie / développement durable, les usages prioritaires concernent le pilotage des infrastructures d'énergies renouvelables, des réseaux électriques

et des systèmes de stockage sensibles aux aléas climatiques. Pour cela, il faut utiliser un mode de calcul quantique plus complet que l'*annealing* – les portes quantiques – pour construire des algorithmes plus puissants qui intègrent d'emblée la complexité de l'environnement qu'ils cherchent à simuler.

- Dans le secteur de la finance (banque / assurance), les usages prioritaires concernent l'optimisation de la gestion de portefeuille et l'analyse de corrélations de plus en plus complexes entre les différents facteurs de risque du marché. Pour cela, il faut appliquer la logique prédictive permise par le calcul quantique aux algorithmes existants de gestion de portefeuilles et d'analyse de risque de fraude, de crédit, etc.

2/ Les capteurs avec les applications pour lesquels des progrès de mesure restent à faire ou pour lesquels il n'existe pas d'outils de mesure :

- Dans le secteur militaire, il s'agit de s'affranchir de la dépendance au GPS dans les lieux connus et explorer des lieux encore inconnus. Pour cela, il faut investir les capteurs quantiques dans des environnements tels que l'espace, le cyberspace ou les fonds marins et dans des environnements dans lesquels les signaux GPS sont perturbés ou indisponibles.
- Dans le civil, il s'agit d'améliorer, avec des capteurs quantiques, les techniques d'imagerie médicale telles que les IRM et la tomographie, les techniques de détection et de modélisation de phénomènes complexes (systèmes autonomes, systèmes environnementaux, outils d'observation spatiale).

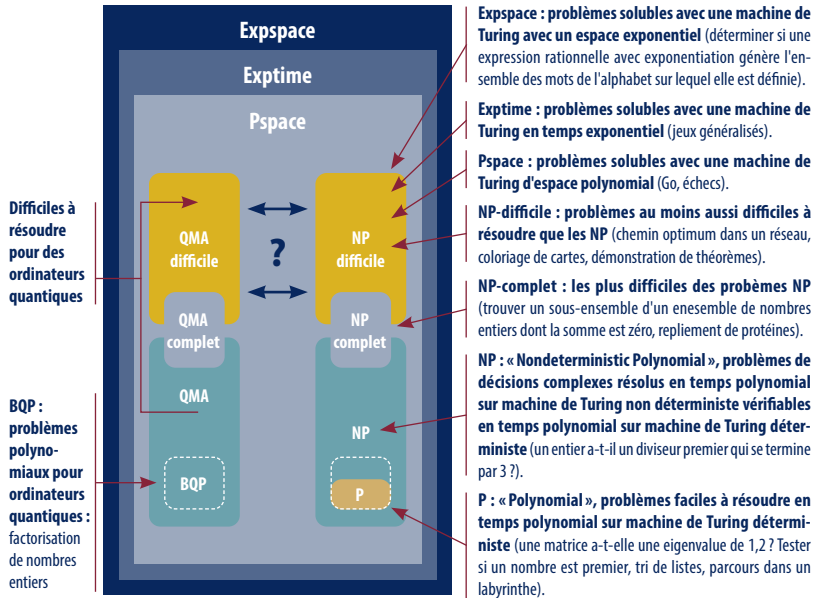
3/ Les communications quantiques, avec la sécurisation de nos réseaux existants et l'anticipation des réseaux d'un « monde post quantique » :

- Dans le secteur militaire, remplacer urgemment les algorithmes de chiffrement existants basés sur la factorisation de nombres premiers ou sur les courbes elliptiques par des algorithmes résistants aux algorithmes de Shor et veiller à empêcher la collecte de données cryptées.
- Dans le civil, favoriser le dépôt de brevets français et européens sur les distributions de clés quantiques (QKD) afin de mieux anticiper les mutations des réseaux de connectivité et résister au monopole des réseaux dits « post-quantiques » que confèrent actuellement les brevets chinois et américains.
- Favoriser l'interopérabilité des clés de distribution quantique au service d'un futur réseau quantique européen terrestre et satellitaire via le projet européen EuroQCI et l'expertise des opérateurs télécom et des fournisseurs de solutions de sécurité.

d. Veiller à la matérialisation effective des avantages quantiques sur ces usages

S'il n'est pas aisé de dire sur quels types de problèmes l'avantage quantique pourrait se matérialiser, il est toutefois évident que la mécanique quantique va induire des ruptures sur des problèmes qui sont déjà quantiques par nature.

Graphique n° 11 • Représentation visuelle de la complexité à résoudre un problème quantique



Source : Olivier Ezratty, *Comprendre l'informatique quantique*, 2018.

Cette représentation schématique permet de comprendre sur quels types de problèmes les technologies quantiques pourraient induire des ruptures. Si les machines futures s'approchent plutôt de la coexistence NIST / analogique, c'est plutôt sur des problèmes faisant intervenir des problèmes d'optimisation et sur de l'apprentissage automatique (*machine learning*) que les algorithmes quantiques apporteront de la valeur ajoutée, avec des disciplines émergentes comme le *machine learning* quantique. L'avantage de vitesse par rapport aux solutions classiques reposerait essentiellement sur de l'algèbre linéaire. Si les machines

futures s'approchent plutôt du FTQC, ce sont les problèmes polynomiaux (dits NP ou NP complets) qui seraient alors résolus en plus des problèmes précédemment cités, ce qui signifie que les technologies quantiques enrichiraient nos méthodes existantes de simulation et ouvrirait la voie à de nouvelles méthodes pour résoudre des problèmes complexes.

Cependant, au-delà de tous ces champs d'application évidents, il apparaît que ni l'avantage quantique, ni la suprématie quantique, ne se sont matérialisés. En effet, nous ne savons pas encore démontrer dans la durée que les performances d'un ordinateur quantique pourraient dépasser intrinsèquement celles d'un ordinateur classique (suprématie quantique) ou surpasser celles d'un ordinateur classique sur des tâches spécifiques (avantage quantique).

Atteindre l'avantage quantique sur des usages donnés est aujourd'hui très incertain pour plusieurs raisons :

- **Le type de problème que l'informatique quantique pourrait résoudre plus efficacement que l'informatique classique reste un objet de recherche en tant que tel, bien qu'il soit avéré que les technologies quantiques permettent de traiter plus efficacement des cas d'usages faisant appel à de l'explosion combinatoire :** les chercheurs ne disposent toutefois pas encore d'une compréhension claire du type de problème que l'informatique pourrait résoudre à terme, en raison du manque de cas concrets sur lesquels s'appuyer. La mécanique quantique, intrinsèquement, se projette dans l'avenir, ce qui implique de changer nos méthodes pour appréhender cette nature de problèmes plus finement.
- **Si la perspective de pouvoir construire un ordinateur quantique tolérant aux erreurs (FTQC) est réelle, les applications commerciales à grande échelle le sont moins :** la difficulté à atteindre une échelle pratique et à développer des systèmes quantiques durables

et résilients augmente l'incertitude sur la manière dont l'avantage quantique sera effectivement réalisé. Cheminera-t-on de manière itérative vers un nombre toujours plus important de qubits logiques, ou trouvera-t-on une manière optimisée de créer un grand nombre de qubits logiques en peu de temps?

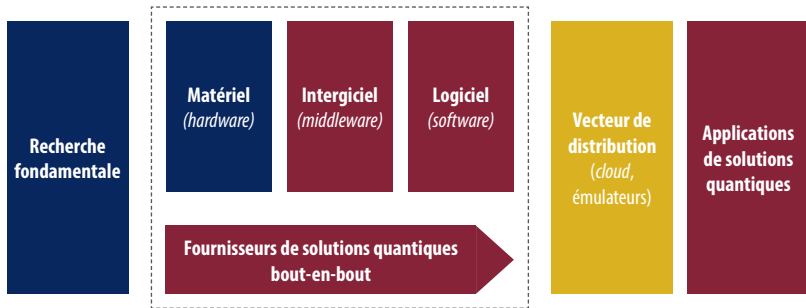
- **Les modalités d'évaluation de l'avantage quantique, même s'il est atteint, sont encore ouvertes :** la manière de qualifier et de quantifier les gains par rapport à des systèmes classiques, et notamment de prendre en compte les effets de bord, devra être mise en place et partagée pour apprécier l'impact réel de l'avantage quantique sur l'économie et la société.

Ces illustrations très pratiques montrent l'étendue des possibilités et des impacts, mais restent encore trop limitées car cantonnées au stade de POC. Désormais, l'enjeu est de diffuser la technologie quantique française de manière plus globale dans l'économie mondiale, en créant un marché à part entière.

3.2. RENTABILISER L'OFFRE QUANTIQUE

Pour créer un marché mondial du quantique, il faut surtout consolider et capter une base de clientèle diversifiée et stable. Si la France ne s'est historiquement pas distinguée dans cette étape de conquête de marché, c'est aussi généralement là qu'elle achoppe. En effet, l'étape 1 de la stratégie quantique française a permis de faire émerger des champions potentiels du matériel quantique, mais pas de créer un marché intérieur porteur. Ainsi, les acteurs français et européens du quantique sont aujourd'hui tributaires de la commande publique et de l'export, ce qui inverse le rapport de force entre les pouvoirs publics et les acteurs économiques.

Créer un marché intérieur porteur nécessite de faire advenir des acteurs français et européens compétitifs sur l'ensemble des composantes de la chaîne de valeur quantique, en se concentrant prioritairement sur les éléments en rouge et en orange de ce schéma simplifié :



- Acteurs français en position dominante
- Acteurs français présents mais insuffisamment compétitifs
- Acteurs français quasi absents du marché

Source: Institut Montaigne, Cf infra.

- a. Mettre des intergiciels quantiques performants à la disposition des entreprises, condition de recours aux technologies quantiques, à l'aide de partenariats choisis

La conclusion de partenariats internationaux stratégiques est clé pour permettre l'essor d'un marché émergent, dispersé et parfois mal appréhendé. C'est pourquoi, à l'occasion du Sommet Choose France du 13 mai dernier, des partenariats internationaux ont aussi été signés par des acteurs privés. IBM s'est associé avec le plateau de Saclay dans le cadre d'un investissement pluriannuel de 45 millions d'euros pour mener des projets de recherche avec l'écosystème quantique français¹¹⁸.

L'entreprise finlandaise IQM a également annoncé l'installation d'une ligne pilote au CEA-LETI de Grenoble pour la production de puces quantiques (QPU) et d'ordinateurs quantiques dernière génération¹¹⁹. Pendant la même période, Pasqal a aussi conclu un partenariat avec Saudi Aramco pour déployer le premier ordinateur quantique à 200 qubits en Arabie Saoudite fin 2025¹²⁰ et Alice & Bob avec Google pour mettre à disposition ses puces « Bosen » à qubit chat sur la place de marché (*marketplace*) de Google¹²¹.

Toutefois, ces partenariats n'ont pas été conclus dans le cadre d'une stratégie de partenariats dédiée à la création d'un marché mondial du quantique, mais plutôt pour attirer des investissements étrangers en matière de nouvelles technologies en France. De fait, aucun des programmes publics pour diffuser les technologies quantiques existantes au grand public ne sont centrés sur la nécessité de s'associer avec des partenaires internationaux pour tester les avantages quantiques sur des usages réels.

HQI et AQUILA ont en effet été lancés au niveau national afin de diffuser les offres quantiques existantes auprès du plan grand nombre, en industrialisant les technologies associées sur toute la pile logicielle :

- Conçue dans une perspective intégrée entre le matériel quantique et le logiciel pour le déployer, la *France Hybrid HPC Quantum Initiative* (HQI) a été lancée en 2022 pour permettre à des acteurs d'évaluer gratuitement, sur une infrastructure publique, le potentiel du calcul quantique pour leurs besoins. Pour cela, le programme doté

¹¹⁸ IBM, *l'IBM France Lab ajoute l'informatique quantique à ses missions, Mai 2024.*

¹¹⁹ IQM, *Choose France Summit with President Macron: IQM Quantum Computers announces plans to build a fabrication facility in France, Mai 2024.*

¹²⁰ Pasqal, *Aramco Signs Agreement With Pasqal To Deploy First Quantum Computer In The Kingdom Of Saudi Arabia, Mai 2024.*

¹²¹ Alice & Bob, *First cat qubit quantum chip by Alice & Bob now available on Google Cloud Marketplace, Mai 2024.*

de 72,3 M€ du plan d'investissements d'avenir (PIA) sur 5 ans permet de tester le branchement de certaines technologies quantiques sur le supercalculateur Joliot-Curie.

- L'appel à manifestation d'intérêt « *Advanced Quantum Understanding : Implementing Large-Scale Applications* » (AQUILA) a été lancé le 1^{er} juillet dernier pour structurer un marché intérieur en stimulant les usages des technologies quantiques et réduire les barrières à l'entrée pour les utilisateurs de technologies quantiques. Il s'appuie sur les entreprises qui peuvent donner accès à des moyens de calcul quantique à distance pour intensifier la distribution de technologies quantiques en Europe et dans le monde.

Néanmoins, ces programmes ne comportent pas de « doctrine de partenariats » pour construire des intergiciels (émulateurs et plateformes cloud) qui permettent de faire le lien entre nos technologies quantiques, et les usages sur lesquels elles pourraient donner lieu à des avantages quantiques réels.

Pourtant, de nombreux pays alignés avec les ambitions d'une offre quantique française sur le marché mondial ont développé des solutions performantes sur l'ensemble de la chaîne de valeur des technologies quantiques :

- Sur l'intergiciel (*middleware*) et le logiciel (*software*), les acteurs les plus avancés sont les américains (IBM, Google, Microsoft, Rigetti Computing, Honeywell, Zapata), les français (Atos, Pasqal, Quandela), et les canadiens avec Xanadu.
- Sur les vecteurs de distribution de solutions quantiques, les acteurs les plus avancés sont les américains (IBM, Google, Microsoft, Rigetti Computing, Honeywell), les canadiens (D-Wave Systems, Xanadu), les japonais (NTT, Toshiba), les coréens (SK Telecom), les singapouriens (Horizon Quantum Computing) et les indiens (QNu Labs).

Recommandation 8

Accélérer la production d'intergiciels (sur la base d'émulateurs ou de plateformes cloud existantes) pour tester des avantages quantiques en situation réelle.

Pour cela, lancer un programme de partenariats public-privé, s'appuyant sur le centre HPC de France Hybrid HPC Quantum Initiative (HQI) financé par le PIA 4 afin de tester les usages bénéficiaires du quantique et sur l'appel à projet de Bpifrance « Advanced Quantum Understanding: Implementing Large-Scale Applications » (AQUILA) voué à diffuser les technologies quantiques dans les environnements industriels.

Ce nouveau programme en lien avec HQI et AQUILA devra intégrer des partenaires de recherche et des partenaires industriels. S'appuyant prioritairement sur les technologies françaises, il s'appliquerait à développer des intergiciels quantiques opérationnels pour tester les usages identifiés :

- Identifier en première instance les partenaires industriels et académiques alignés avec l'ambition d'une offre quantique française pour le marché mondial issue de coopérations internationales ciblées par type d'enjeux, réservées sur les aspects régaliens, plus ouvertes sur les aspects civils.
- Co-construire avec les partenaires européens ayant les ressources complémentaires nécessaires une offre quantique de bout en bout (infrastructure & matériel, intergiciel, logiciel) et la commercialiser sur les usages ci-dessus. L'initiative de ce partenariat devra être portée par le coordinateur national de la stratégie quantique.

- Afin que cette offre européenne puisse s'imposer sur le marché mondial et créer une véritable demande par rapport à un besoin identifié mais encore mal appréhendé, s'associer à des partenariats de distribution de solution quantique dominant le marché : les américains (IBM, Google, Microsoft, Rigetti Computing, Honeywell), les canadiens (D-Wave Systems, Xanadu), les japonais (NTT, Toshiba), les coréens (SK Telecom), les singapouriens (Horizon Quantum Computing ou encore les indiens (QNu Labs). Une étude poussée des avantages et des risques de tels partenariats devra être conduite par le coordinateur national.

b. Inciter à la création et au développement d'un écosystème applicatif dédié au quantique en Europe

Pour garantir une adoption équilibrée des solutions quantiques, sa massification est importante, ce qui implique de démontrer leur efficacité à travers des projets concrets, mais aussi de faire advenir des acteurs du logiciel européens. En effet, les barrières à l'entrée sont moins fortes sur le segment du logiciel quantique que sur le segment du matériel quantique. Une fois les intergiciels déployés, il est crucial que des entreprises européennes de logiciel s'en saisissent, pour en tirer toute la valeur ajoutée et les bénéfices commerciaux associés. C'est dans cet objectif que le Pack Quantique de la région Île-de-France¹²² a été lancé en 2020 avec un financement de 2 M€ sur trois ans pour démontrer des avantages quantiques sur des cas d'usages concrets rencontrés au quotidien par les entreprises. Par exemple, La Matmut et

¹²² GENCI, Communiqué – Pack Quantique Île-de-France : la région Île-de-France et ses partenaires s'engagent pour renforcer le secteur de l'assurance et de la banque grâce au calcul quantique, 2024.

la startup QbitSoft ont présenté le projet AQADEF qui postule un avantage quantique sur la réduction des fraudes à l'assurance pour trouver le meilleur graphe et optimiser le modèle. Un autre exemple instructif est celui de Natixis CIB et de Multiverse Computing qui exploitent le potentiel de l'informatique pour optimiser l'évaluation de produits financiers et de leurs indicateurs de risque, dans des configurations où les modèles à noyaux¹²³ traditionnellement utilisés perdent en capacité prédictive en raison d'un nombre important de risques. Le groupe EDF a également mis au point AQADOC¹²⁴ pour explorer la parallélisation de calcul quantique avec des *pure players* (Pasqal, Quandela) et des utilisateurs finaux. De fait, la parallélisation est une piste privilégiée pour construire des systèmes quantiques avec une taille atteignable à court-terme sans sacrifier le passage à l'échelle, ce qui pourrait permettre une adoption plus large.

Le Pack Quantique est ainsi une première étape utile pour démontrer un avantage quantique clair sur des usages précis et optimiser le fonctionnement du marché intérieur quantique français.

Une fois l'efficacité démontrée, l'acculturation au quantique doit s'étendre à l'ensemble de la chaîne de valeur, intégrant non seulement les grandes entreprises mais aussi les sous-traitants et partenaires.

Les solutions quantiques doivent être intégrées de manière holistique à tous les niveaux, depuis les grandes structures jusqu'aux petites entreprises et leurs partenaires. Cette adoption globale est essentielle pour maximiser l'impact des technologies quantiques et pour démontrer leur valeur dans des contextes variés. C'est en engageant toute la chaîne de valeur que la technologie quantique pourra se diffuser le plus efficacement possible dans l'économie, et que les avantages quantiques se matérialiseront aux bons endroits sur le marché.

¹²³ *Outils statistiques utilisés pour faire des modèles de régression linéaire en mesurant la similarité entre deux points dans un espace de données, généralement en les transformant dans un espace de caractéristiques de dimension plus élevée.*

¹²⁴ *EDF, AQADOC, la parallélisation des algorithmes quantiques pour le secteur de l'énergie, 2024.*

En effet, l'essentiel de la croissance permise par les avantages quantiques sera captée par les entreprises qui se seront préparées à prendre le « virage quantique ». Si tous les secteurs d'activité ne sont pas concernés (*Cf supra*), la plupart des organisations doivent néanmoins se préparer dès à présent à exploiter les solutions quantiques, et ce dans un avenir relativement proche : les feuilles de route des constructeurs quantiques sont globalement respectées jusqu'ici, et l'arrivée à maturité de solutions « industrielles » est anticipée à partir de 2030, permettant de réellement déployer « à l'échelle » les premiers cas d'usage.

Les avantages des technologies quantiques et de l'IA sont particulièrement puissants lorsqu'ils sont combinés. En réalité, loin de s'opposer, ces deux domaines sont complémentaires, chacun exploitant des méthodes distinctes pour atteindre des objectifs similaires. L'IA utilise des approches probabilistes pour effectuer des prédictions à partir de données existantes, tandis que les technologies quantiques s'appuient sur des méthodes algébriques complexes, permettant de manipuler des états de superposition pour traiter non seulement des données présentes, mais aussi des possibilités futures.

- L'IA tire profit de la puissance de calcul parallèle et massive offerte par le calcul quantique, ce qui lui permet de résoudre des problèmes avec moins de ressources informatiques.
- De son côté, le calcul quantique bénéficie des capacités d'optimisation et de gestion des données développées par l'IA, facilitant ainsi la résolution de problèmes complexes plus rapidement.

Dans le cas de calculs intensifs, l'IA accélère les processus grâce à des techniques d'apprentissage supervisé ou non supervisé, tandis que le calcul quantique permet une optimisation accrue en réduisant la puissance de calcul nécessaire. C'est dans ce contexte qu'émerge le *Quantum Machine Learning* (QML), discipline à la croisée de l'IA et du calcul quantique, qui utilise des algorithmes quantiques pour améliorer

les performances des modèles d'apprentissage automatique traditionnels. Par exemple, la réduction dimensionnelle quantique permet d'analyser plus rapidement de grandes quantités de données, en isolant les informations les plus pertinentes pour un problème donné. Un autre exemple est l'algorithme de Grover, qui accélère la recherche dans des bases de données non structurées, offrant ainsi des gains significatifs en apprentissage non supervisé. Ce dernier, en IA, désigne une méthode où les modèles apprennent à partir de données non étiquetées, en détectant des structures cachées ou des patterns naturels sans supervision explicite, contrairement à l'apprentissage supervisé qui utilise des paires entrée-sortie définies à l'avance.

Recommandation 9

Acculturer les acteurs financiers aux avantages de l'offre quantique à venir afin d'inciter à la création et au développement d'un écosystème applicatif dédié au quantique en Europe.

- Pour cela, éduquer les acteurs économiques à la révolution quantique qui s'annonce. Le programme France 2040 pourrait produire des indicateurs de performance et de plus-value des offres quantiques appliquées aux **cas d'usage de référence identifiés** dans la recommandation 7. Ces indicateurs pourraient aussi s'enrichir d'outils de mesure des avantages quantiques par rapport aux avantages offerts par l'IA, et de plus-value du *Quantum Machine Learning* par rapport au *Machine Learning*.
- Un projet pilote européen financé par la Commission européenne et démontrant le bien fondé d'un usage quantique, dans le domaine de la santé ou de la transition

énergétique, par exemple, pourrait servir à quantifier **la valeur ajoutée des solutions quantiques dans les modèles d'affaires** et encourager la communauté financière à investir durablement dans les applications logicielles quantiques.

- Parallèlement, des opérations de sensibilisation et de partage d'expérience autour des enjeux d'adoption de technologies de rupture (en premier lieu les usages quantiques et l'IA) avec des acteurs publics tels que la DGE pourraient inciter les entreprises à considérer les solutions quantiques comme des leviers de productivité et de haute valeur ajoutée. Preuve de ce potentiel, des cabinets de conseils se spécialisent d'ores et déjà dans la sensibilisation des dirigeants d'entreprise à l'adoption du quantique dans leurs métiers et leurs méthodes de travail.

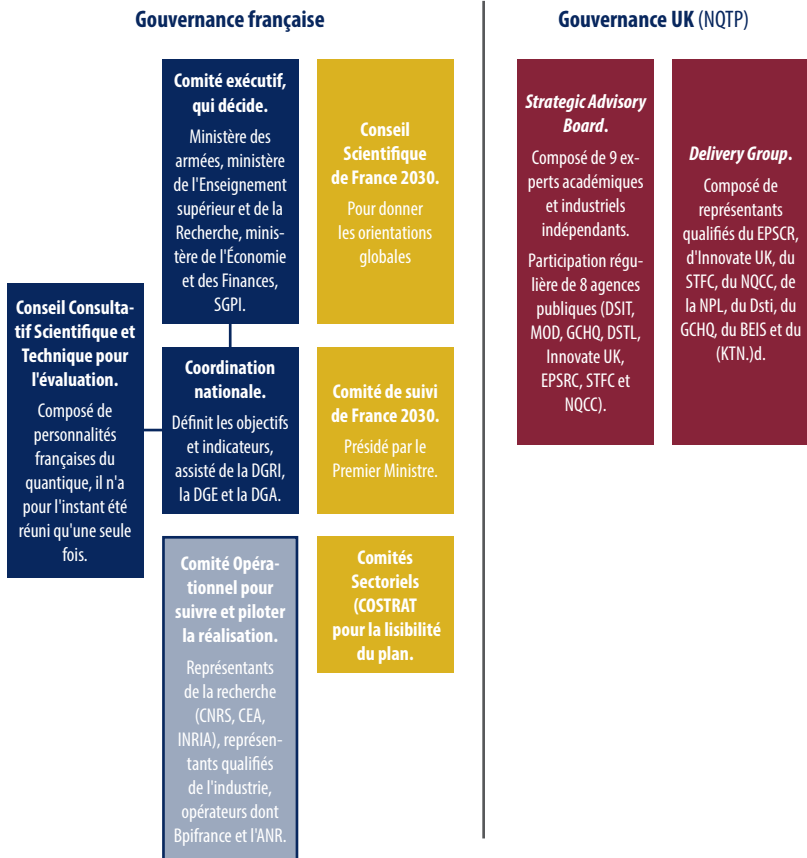
4 L'importance d'une gouvernance qui accompagne sans freiner

Le degré de maturité de l'informatique quantique, et la constitution encore balbutiante d'un écosystème et d'une filière professionnelle militent en faveur de la gouvernance la plus flexible possible. En effet, la plupart des acteurs enregistrent des niveaux de *Technology Readiness Level* (TRL) entre 1 et 6, dépendant de l'usage considéré, ce qui montre l'ampleur des incertitudes scientifiques et technologiques restant à lever pour faire advenir des usages. **Cette gouvernance doit s'exprimer à deux niveaux.**

4.1. AU NIVEAU POLITIQUE, DES RESPONSABILITÉS TROP DILUÉES

En effet, malgré de louables intentions, force est de constater la complexité de la gouvernance française, sa politisation injustifiée et les freins bureaucratiques qu'elle induit. Rappelons que des programmes essentiels à la mise en œuvre des ambitions formulées en 2021, comme Proqcima pour le choix d'une technologie ou Aquila et HQI pour la diffusion des technologies quantiques sur le marché mondial, ont mis 3 ans à se matérialiser après l'annonce de la stratégie nationale quantique en 2021, qui avait pourtant comme ambition de sécuriser « toutes les composantes de la chaîne de valeur » de l'informatique quantique. **Ces exemples illustrent le nécessaire pragmatisme des approches quantiques, au fur et à mesure que se révèlent les possibilités d'usage.** Pourtant, la gouvernance mise en place complexifie à loisir le traitement de cet impératif, contrairement aux approches plus pragmatiques mises en place dans les pays anglo-saxons, comme notamment le Royaume-Uni qui a enregistré d'excellents résultats en matière de prise de parts de marché, à 16% (*Cf supra*). Dans des pays comme les Pays-Bas, les appels à projet quantiques sont délégués à une fondation, ce qui permet de lancer des projets en un temps très réduit, et confère une flexibilité accrue aux gestionnaires de la stratégie quantique.

Graphique n° 13 • Focus sur la complexification à outrance de la gouvernance française par rapport à la gouvernance britannique



Source : auditions et *UK National Quantum Technologies Programme*, Cf annexe pour les acronymes.

Par conséquent, les responsabilités sont trop diluées, et l'exécution repose trop souvent sur la Coordination Nationale paradoxalement seule responsable légale des décisions budgétaires prises. Si la décision, l'exécution et l'évaluation sont des piliers importants de toute stratégie, ils ont été noyés en étant confiés à une multiplicité d'acteurs, de telle sorte que plus personne n'est responsable. Par-dessus, est venu se greffer l'échelon de France 2030, qui ajoute trois comités (orienter, suivre et assurer la lisibilité) supplémentaires. **Par conséquent, l'informatique quantique se retrouve noyée dans les 30 priorités stratégiques de France 2030, alors que des pays comme le Royaume-Uni ou les États-Unis se sont toujours limités à 5 priorités maximum pour ne pas se disperser.** L'éclatement des responsabilités qui en résulte entraîne une double peine : d'une part, les technologies peinent à démontrer leur valeur ajoutée dans ce contexte désordonné, et d'autre part, elles se retrouvent noyées parmi d'autres priorités sectorielles, sans véritable cohérence de fond à l'œuvre, ou manière d'assurer sa convergence fructueuse avec d'autres technologies comme l'IA.

Recommandation 10

Passer de 6 à 2 instances de gouvernance de la stratégie quantique, l'une dédiée à la réflexion stratégique et l'autre à l'exécution opérationnelle :

- Confier au Comité exécutif actuel (émanant des ministères concernés) la responsabilité totale de la stratégie quantique nationale et des financements à y allouer.
- Fusionner le Conseil Consultatif Scientifique et Technique avec le Comité Opérationnel de la stratégie nationale quantique, et l'utiliser pour renforcer la Coordination Nationale en la dotant d'un Comité d'exécution sur le modèle britannique. La Coordination Nationale devra renforcer ses effectifs afin de gérer opérationnellement

les crédits budgétaires et les relations avec l'écosystème français et mondial.

- S'assurer de l'adhésion des différents comités de France 2030 en amont de la prise de décision, à des fins consultatives et d'alignement opérationnel, pour éviter désalignements et doublons.

Une action immédiate du comité d'exécution de la Coordination Nationale pourrait être de clarifier les rôles et responsabilités de chaque acteur de l'écosystème en **établissant ensuite un RACI¹²⁵, sous la responsabilité du coordinateur national, pour éviter les doublons ou des compétitions internes contraires à l'objectif global**. En outre, ce RACI devrait s'inscrire en cohérence avec les nouvelles priorités / orientations stratégiques de France 2040, qui devraient être considérablement réduites en nombre, dans une logique de choix.

4.2. AU NIVEAU SCIENTIFIQUE, DES PARTAGES DE ROADMAP ENCORE TROP PONCTUELS

Des dispositifs de partage de maturité technologique, par le biais de feuilles de route techniques (*roadmap*) existent dans d'autres domaines et peuvent servir d'inspiration pour accélérer le développement d'une filière quantique. Par exemple, dans le secteur des semi-conducteurs, la *International Technology Roadmap for Semiconductors* (ITRS) permet de mettre en commun des spécifications fonctionnelles

¹²⁵ *Domaine de management ou matrice de responsabilités, emprunté à la méthode anglo-saxonne, dans laquelle apparaissent clairement les acteurs réalisateurs (responsible), approbateurs (accountable), consultés (consulted) et informés (informed), soit les 4 rôles qu'un membre d'une équipe projet peut exercer sur une tâche spécifique.*

(specs). Elle a été remplacée par la *International Roadmap for Devices and Systems* (IRDS) en 2017 pour prendre en compte la fin de la loi de Moore à 15 ans, et l'intégration de systèmes dits *More Than Moore*, soit l'ajout de fonctionnalités supplémentaires aux puces électroniques, en lieu et place de la miniaturisation. L'objectif est de créer des systèmes plus fonctionnels et polyvalents sur une seule puce ou un seul module. **De fait, pour atteindre des TRL supérieurs à 6, et pouvoir ainsi passer en production, il faut maîtriser les bonnes technologies de base et habilitantes, qui ont déjà été cartographiées par la Coordination Nationale de la Stratégie Quantique.**

Exemple de la *roadmap* IRTS/IRDS dans l'industrie des semi-conducteurs

IRTS/IRDS ont été mises en place pour donner une feuille de route globale de l'industrie des semi-conducteurs aux acteurs, afin de leur donner toutes les informations pour identifier les défis et opportunités technologiques futures. Concrètement, IRTS a pris la forme d'un ensemble de documents produits de manière coordonnée par les experts du secteur sous la supervision de la SC Research Corporation (Taiwan, Corée du Sud, US, Europe, Japon, Chine) avec 936 entreprises affiliées avec 17 groupes de travail techniques. Elle était guidée par une feuille de route axée sur les tendances, les besoins, et les activités connexes. Avec IRDS, elle se décline désormais en un ensemble de prévisions sur les évolutions probables des appareils microélectroniques pour faciliter la coordination entre universités, fabricants, fournisseurs et laboratoires. Elle intègre des critères de références (benchmarks) d'applications, des systèmes et architectures adaptées à l'amélioration Moore dans les circuits intégrés, des technologies au-delà des CMO¹²⁶, la connectivité des systèmes externes, les

usines intégrées, la lithographie, la métrologie, les matériaux de recherche émergents, un environnement sain et durable, l'amélioration du rendement, de l'électronique de cryogénie et un traitement quantique de l'information.

Ces deux types de *roadmap* ont pour objectif de fournir aux acteurs de l'industrie des indications claires sur la date à laquelle telle ou telle technologie, dont ils pourraient avoir besoin, sera disponible. C'est très utile pour mutualiser certains coûts et construire un écosystème de fournisseurs cohérent. Dans le cas de l'IRDS, cela s'est traduit par une cartographie des composants des 17 groupes de travail techniques.

Une fois que les technologies quantiques auront été intégralement cartographiées (de base et habilitantes), les acteurs auront besoin de s'appuyer sur d'autres technologies existantes ou en cours de développement pour économiser certains coûts, tant pour les passer à l'échelle que pour les commercialiser. C'est ce qui a justifié le **lancement en 2023 par le SGPI d'un travail d'ampleur avec l'Académie des Technologies** pour construire une *roadmap* technologique quantique partagée à l'échelle nationale. L'objectif est de l'utiliser comme cadre pour **partager les risques dans les phases amont de développement d'une technologie**. Les réaliser en silo pourrait avoir pour conséquence de freiner la progression de l'industrie, dans la mesure où un produit seul est inopérant s'il ne peut pas être intégré derrière dans une chaîne de valeur et sur un marché.

¹²⁶ *Métal oxyde semi-conducteur complémentaire, soit une sorte de transistor utilisé pour construire des circuits intégrés et logiques.*

Recommandation 11

Actualiser tous les deux ans la *roadmap* technologique pilotée par l'Académie des Technologies afin de permettre un ajustement des politiques technologiques dans le temps industriel.

5 Plan d'action stratégique et opérationnel

Comme exposé précédemment, la dimension financière et la capacité de l'écosystème à se saisir correctement des solutions quantiques sont les deux axes prioritaires du plan d'action stratégique et opérationnel proposé.

En termes de financement de nos recommandations, nous avons souhaité calibrer les besoins au strict minimum au vu de la situation de nos finances publiques, de manière à maintenir l'avance des acteurs français sur l'offre technologique et à se donner les clés indispensables à la transformation de cette avance en avantage économique au niveau mondial.

Nous avons souhaité également tirer les leçons de l'étape 1 du plan quantique gouvernemental dont l'élaboration, pour autant louable qu'elle a été, a manqué partiellement sa cible.

Pour rappel, dans le cadre de l'étape 1 de la stratégie quantique, il avait été prévu :

- 1,03 Md€ d'argent public dont 350 M€ d'anciens crédits réalloués pour l'occasion, ce qui ramenait à 650 M€ les crédits réellement disponibles ;

- 545 M€ d'argent privé via des co-financements industriels ;
- 225 M€ d'argent européen qui ont été collectés et engagés.

La multiplication des sources de financement privées, publiques et européennes ont eu le mérite de mobiliser l'écosystème et de financer effectivement un certain nombre de projets mais ont également introduit une confusion dans les attentes des acteurs industriels et les marges de manœuvre réelles du gouvernement. Elle a également dilué les responsabilités et donné des engagements de moyens et non de résultats.

Forts de ces enseignements, nous voulons insister sur une méthodologie de financement responsable et efficace. Elle tient en deux points : un budget public sanctuarisé et un engagement d'au moins 3 ans.

- En effet, étant donné les incertitudes qui demeurent sur les progrès technologiques de l'informatique quantique et les disponibilités budgétaires, il est important de sanctuariser les financements sur une durée d'au moins 3 ans, correspondant aux engagements présidentiels, même si le plan quantique doit rester cohérent sur le temps long et qu'un horizon à 2032 aurait plus de sens.
- **Pour maintenir l'avance technologique française et rester cohérent avec l'ambition initiale du plan quantique, l'Institut Montaigne recommande un budget public minimum de 500 M€ sur 2025-2027 financé par France 2030 et le PIA 4 uniquement. Il sera important de le compléter par des financements privés et européens sans confusion des enveloppes allouées.**

C'est dans ce cadre que s'inscrivent nos recommandations de fond selon des étapes majeures accessibles en l'état.

Objectif 1

Affiner notre stratégie de sécurisation de la technologie quantique française pour mieux articuler la recherche fondamentale et le passage à l'échelle.

RECOMMANDATION 1

Confier à Proqcima, reconnu à l'échelle européenne comme l'acteur le plus légitime en la matière, l'identification et la sécurisation de la technologie française la mieux adaptée à une offre compétitive militaire et civile à l'échelle de l'Europe.

Proqcima, programme de l'État piloté par la direction générale de l'armement (DGA), est mandaté pour sélectionner les 2 technologies françaises de qubits les plus performantes capables de passer à l'échelle en milieu industriel.

Cette première étape clé de sélection doit s'enrichir des actions suivantes pour être véritablement efficace :

- 1. Confronter les 2 technologies françaises retenues aux technologies européennes d'égal maturité.** En effet, la « logique d'entonnoir » de Proqcima est constituée de jalons techniques communs à tous les acteurs qui construisent des ordinateurs quantiques pour choisir les technologies qui seront les plus performantes pour les usages militaires comme civils. Il faudra ainsi prendre en compte les partenaires européens qui sont en pointe sur les technologies de qubits quantiques comme par exemple le VTT en Finlande, l'IFN en Italie, la Chalmers University of Technology de Suède, le Gemini Center norvégien, l'Université de Genève, l'ETH de Zurich, l'école de Copenhague au Danemark ou encore le TU Delft et QuTech des Pays-Bas. Le choix des technologies quantiques les plus performantes à

l'échelle européenne permettra la définition d'une ambition véritablement mondiale.

2. Rendre Proqcima plus dynamique compte tenu de l'évolution rapide du milieu industriel qu'il a vocation à adresser en :

- confiant les deux technologies retenues à des laboratoires communs (laboratoires associant recherche appliquée et entreprises) pour s'assurer de leur pertinence industrielle une fois les machines construites, tout en gardant une marge de manœuvre pour gérer l'incertitude scientifique des autres technologies non retenues tout au long du programme ;
- mettant en place des mesures d'impact adaptées aux usages industriels, avec un indicateur permettant de quantifier la valeur ajoutée en milieu industriel des avantages quantiques permis par les deux technologies retenues ;
- veillant à confier au programme de recherche fondamentale QuLoop le suivi des technologies non retenues par Proqcima afin de garantir une éventuelle réversibilité de la technologie si sa maturité évolue ou si le marché le décide. Le procédé de sélection doit être proche du terrain et simple dans l'exécution.

3. Pour protéger les technologies quantiques françaises les plus en pointe, une logique de réservation des technologies les plus performantes pour les usages militaires et régaliens pourra être appliquée (sur un modèle de type Palantir) permettant d'ouvrir des versions technologiques moins performantes aux usages civils et à la concurrence internationale.

Objectif 2

Mettre en œuvre à l'échelle européenne une stratégie de normalisation intégrant des standards techniques français.

RECOMMANDATION 2

Conscient de la nécessité de prioriser les solutions tout en veillant à ne pas se faire imposer de facto des standards structurés par d'autres, inciter les acteurs français et européens à contribuer aux programmes open-source internationaux dans lesquels il y a un intérêt commercial à être contributeur. Les programmes les plus prometteurs à ce stade sont le programme Qskit d'IBM, le programme Cirq de Google, le programme Q-Sharp de Microsoft et le programme Forest de Rigetti Computing. Le Quantum Flagship européen pourrait inclure une obligation de contribution à ce type de programme dans ses critères de financement de projets de recherche fondamentale et appliquée en technologies quantiques.

RECOMMANDATION 3

À long-terme, et au sein des instances internationales de normalisation, dans le cadre du programme MetriQs France, définir une stratégie de normalisation à partir des acteurs et des technologies françaises et européennes en matière de normes de calcul, normes de sécurité et de compatibilité des technologies habilitantes et protocoles de communication entre infrastructures quantiques :

1. sensibiliser les intervenants français et européens à l'importance d'une approche plus offensive et plus structurée sur la base d'une stratégie de normalisation définie en amont par MetriQs France avec le concours des industriels amenés à les commercialiser ;
2. créer des cellules de veille sectorielle dans les commissions ISO/IEC JTC 3 et JCA-QKDN avec des outils de veille informatisés pour collecter l'information en temps réel, sur le modèle du *Quantum Economic Development Consortium* (QED-C) du NIST ;
3. mettre en place une collaboration entre les laboratoires communs et le LNE pour diffuser des normes permettant un passage à l'échelle plus rapide des technologies quantiques sur le modèle du Fraunhofer-Gesellschaft avec l'Institut allemand de normalisation (DIN) pour mettre en place des spécifications quantiques dans la norme ISO/IEC 2382 ;

4. suivre en intelligence économique les positions américaines dominantes ainsi que les positions chinoises extrêmement actives dans les organisations internationales afin de comprendre les évolutions du marché, identifier les éventuels syndromes NVidia (développement vélocité d'une technologie moins disante mais facilement adoptable), et adapter notre technologie à la demande.

Objectif 3

Embarquer les investisseurs privés à hauteur des financements publics.

RECOMMANDATION 4

Mettre en place des incitations ciblées pour les grandes entreprises françaises afin de motiver l'acquisition des jeunes pousses quantiques et d'encourager les acteurs du capital risque et du capital croissance à investir dans le quantique.

1. Mettre en place des **avantages fiscaux de type CIR** ou autres pour les grandes entreprises qui réaliseraient des acquisitions de jeunes pousses quantiques pour un montant supérieur à 300 M€ (compatible avec les règles de financement des fonds Deeptech européens), en considérant ces acquisitions comme des dépenses d'investissement d'avenir, conformément à la logique initiale du CIR. Il est à noter que les grandes entreprises françaises achètent des prestations quantiques mais n'investissent pas directement à leur capital, contrairement aux entreprises américaines qui y voient un moyen de créer de la valeur rapidement.
2. Mettre en place des indicateurs de performance valorisant ce type d'acquisition dans les **programmes d'allocation de fonds certifiés européens**.
3. Le marché européen du capital risque et du capital croissance restant

très timoré vis-à-vis des starts up quantiques (pour des raisons de retour sur investissement dans des temporalités inférieures à 7 ans), militer en faveur de **la création d'un fonds de capital-risque multiples entreprises** (*multi corporate ventures*) dédié à l'achat de *start-ups* quantiques au moment de la série B, permettant la constitution d'expertises dédiées au secteur et l'identification des brevets utiles technologiquement ou valorisables financièrement pour le secteur quantique.

Objectif 4

Faire du secteur quantique un domaine d'attrait pour les jeunes talents français et internationaux.

RECOMMANDATION 5

Mettre en place des chaires quantiques dans les laboratoires de recherche fondamentale et appliquée généraux aux méthodologies éprouvées.

1. Motiver les jeunes scientifiques à s'intéresser au quantique et débaucher des profils connexes susceptibles de contribuer à l'informatique quantique par des synergies scientifiques.
2. Proposer des dispositifs dérogatoires par rapport aux salaires publics sur certains profils internationaux afin d'attirer les profils clés sur des projets d'étude critique, en limitant l'écart, à titre exceptionnel et sur une durée donnée, par rapport aux salaires internationaux. Le dispositif «Chaire d'excellence»¹²⁷ lancé en mai 2023 et opéré par l'ANR pourrait être utilisé pour mettre en œuvre cette proposition.

¹²⁷ Dossier de presse France 2030, AQADOC, la parallélisation des algorithmes quantiques pour le secteur de l'énergie, 2024.

RECOMMANDATION 6

Intégrer des compétences fondamentales faisant appel à la logique mathématique non binaire (dite logique non booléenne) dans les programmes mathématiques révisés du cycle 4 qui seront prochainement publiés par le Conseil Supérieur de Programmes.

Ces compétences doivent inclure les deux grands ensembles théoriques de la logique non booléenne, qui sont les suivants :

1. la logique floue qui permet de traiter des « vérités partielles » ;
2. la logique modale qui introduit des concepts tels que la nécessité et la possibilité, utilisée en informatique pour la vérification formelle de programmes, dont s'inspire la méthode du *model-checking* développée par Clarke, Emerson et Sifakis, lauréats du prix Turing en 2007. Au sein de cette logique, la logique intuitionniste devra être incluse pour apprendre aux élèves à construire des systèmes de preuves propres à la mécanique quantique.

Ce sont ces ensembles théoriques qui permettent d'analyser et de construire des systèmes techniques non binaires, dans lesquels une proposition n'est pas uniquement vraie ou fausse. Surtout, ce sont ces bases théoriques qui permettront aux élèves intéressés par la filière quantique de modéliser correctement des problèmes quantiques par nature, pour ensuite les transposer dans des environnements réels / industriels.

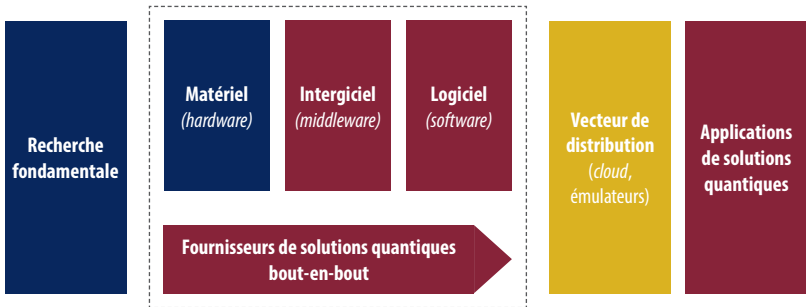
Objectif 5

Construire une offre quantique qui réponde à un besoin pour créer un marché rentable.

Une offre quantique de marché ne pourra advenir que si les avantages de l'informatique quantique sont démontrés au quotidien sur

des cas d’usage à haute valeur ajoutée. Trois conditions concomitantes doivent être remplies : i) la mise à disposition des entreprises d’intergiciels (*middleware*) performants - condition de recours à la technologie quantique, ii) des applications quantiques (*software*) développées en Europe qui permettent de tester les bénéfices quantiques sur des cas d’usage en situation réelle, iii) des méthodes d’interface entre applications classiques et applications quantiques pour permettre le basculement des unes aux autres pour des cas d’usage précis (modélisation, optimisation, sécurisation...).

Cette offre quantique a vocation à faire advenir également des acteurs européens compétitifs sur l’aval de la chaîne (sur les éléments en rouge et en orange ci-dessous) en s’appuyant sur le marché mondial :



- Acteurs français en position dominante
- Acteurs français présents mais insuffisamment compétitifs
- Acteurs français quasi absents du marché

Pour construire un *leadership* marché à partir de notre *leadership* technologique, il est nécessaire de cibler les usages sur lesquels il y a la plus forte valeur ajoutée à adopter des solutions quantiques. Ces usages sont ceux pour lesquels l’avantage quantique est le plus marqué par rapport à d’autres technologies de rupture.

RECOMMANDATION 7

Confier à la Direction Générale des Entreprises (DGE), qui se situe au cœur de l'écosystème quantique, le soin de diffuser aux entreprises et aux investisseurs une feuille de route recensant les usages quantiques dans lesquels investir de manière à en retirer des avantages concurrentiels.

Ces usages concernent prioritairement :

1. Le calcul intensif avec les applications qui font appel à de l'explosion combinatoire et du *calcul en parallèle* :

- a.** Dans le secteur de la chimie / pharmaceutique, les usages prioritaires concernent la conception automatisée de processus de synthèse et la modélisation de molécules pour détecter des pathologies de manière plus précoce. Pour cela, il faut utiliser le calcul quantique pour concevoir des algorithmes qui permettent de modéliser des problèmes à N-corps, soient des problèmes qui étudient les interactions combinées d'un grand nombre de particules entre elles.
- b.** Dans le secteur de l'industrie manufacturière / transport, les usages prioritaires concernent l'optimisation des routes de transport ou de la logistique avec des processus intelligents. Pour cela, il faut utiliser un certain type de calcul quantique - *l'annealing* ou recuit quantique - qui permet de trouver de manière itérative la solution optimale à un problème complexe parmi un nombre exponentiel de combinaisons possibles.
- c.** Dans le secteur de l'énergie / développement durable, les usages prioritaires concernent le pilotage des infrastructures d'énergies renouvelables, des réseaux électriques et des systèmes de stockage sensibles aux aléas climatiques. Pour cela, il faut utiliser un mode de calcul quantique plus complet que *l'annealing* – les portes quantiques – pour construire des algorithmes plus puissants qui intègrent d'emblée la complexité de l'environnement qu'ils cherchent à simuler.

d. Dans le secteur de la finance (banque / assurance), les usages prioritaires concernent l'optimisation de la gestion de portefeuille et l'analyse de corrélations de plus en plus complexes entre les différents facteurs de risque du marché. Pour cela, il faut appliquer la logique prédictive permise par le calcul quantique aux algorithmes existants de gestion de portefeuilles et d'analyse de risque de fraude, de crédit, etc.

2. Les capteurs avec les applications pour lesquels des progrès de mesure restent à faire ou pour lesquels il n'existe pas d'outils de mesure :

a. Dans le secteur militaire, il s'agit de s'affranchir de la dépendance au GPS dans les lieux connus et explorer des lieux encore inconnus. Pour cela, il faut investir les capteurs quantiques dans des environnements tels que l'espace, le cyberspace ou les fonds marins et dans des environnements dans lesquels les signaux GPS sont perturbés ou indisponibles.

b. Dans le civil, il s'agit d'améliorer, avec des capteurs quantiques, les techniques d'imagerie médicale telles que les IRM et la tomographie, les techniques de détection et de modélisation de phénomènes complexes (systèmes autonomes, systèmes environnementaux, outils d'observation spatiale).

3. Les communications quantiques, avec la sécurisation de nos réseaux existants et l'anticipation des réseaux d'un « monde post quantique » :

a. Dans le secteur militaire, remplacer urgemment les algorithmes de chiffrement existants basés sur la factorisation de nombres premiers ou sur les courbes elliptiques par des algorithmes résistants aux algorithmes de Shor et veiller à empêcher la collecte de données cryptées.

b. Dans le civil, favoriser le dépôt de brevets français et européens sur les distributions de clés quantiques (QKD) afin de mieux anticiper les mutations des réseaux de connectivité et résister au monopole

des réseaux dits « post-quantiques » que confèrent actuellement les brevets chinois et américains.

- c. Favoriser l'interopérabilité des clés de distribution quantique au service d'un futur réseau quantique européen terrestre et satellitaire via le projet européen EuroQCI et l'expertise des opérateurs télécom et des fournisseurs de solutions de sécurité.

RECOMMANDATION 8

Accélérer la production d'intergiciels (sur la base d'émulateurs ou de plateformes cloud existantes) pour tester des avantages quantiques en situation réelle. Pour cela, lancer un programme de partenariats public-privé, s'appuyant sur le centre HPC de *France Hybrid HPC Quantum Initiative* (HQI) financé par le PIA 4 afin de tester les usages bénéficiaires du quantique et sur l'appel à projet de Bpifrance « *Advanced Quantum Understanding: Implementing Large-Scale Applications* » (AQUILA) voué à diffuser les technologies quantiques dans les environnements industriels.

Ce nouveau programme en lien avec HQI et AQUILA devra intégrer des partenaires de recherche et des partenaires industriels. S'appuyant prioritairement sur les technologies françaises, il s'appliquera à développer des intergiciels quantiques opérationnels pour tester les usages identifiés :

- Identifier en première instance les partenaires industriels et académiques alignés avec l'ambition d'une offre quantique française pour le marché mondial issue de coopérations internationales ciblées par type d'enjeux, réservées sur les aspects régaliens, plus ouvertes sur les aspects civils.
- Co-construire avec les partenaires européens ayant les ressources complémentaires nécessaires une offre quantique de bout en bout (infrastructure & matériel, intergiciel, logiciel) et la commercialiser sur les usages ci-dessus. L'initiative de ce partenariat devra être portée par le coordinateur national de la stratégie quantique.

- Afin que cette offre européenne puisse s'imposer sur le marché mondial et créer une véritable demande par rapport à un besoin identifié mais encore mal appréhendé, s'associer à des partenariats de distribution de solution quantique dominant le marché : les américains (IBM, Google, Microsoft, Rigetti Computing, Honeywell), les canadiens (D-Wave Systems, Xanadu), les japonais (NTT, Toshiba), les coréens (SK Telecom), les singapouriens (Horizon Quantum Computing ou encore les indiens (QNu Labs). Une étude poussée des avantages et des risques de tels partenariats devra être conduite par le coordinateur national.

RECOMMANDATION 9

Acculturer les acteurs financiers aux avantages de l'offre quantique à venir afin d'inciter à la création et au développement d'un écosystème applicatif dédié au quantique en Europe.

- Pour cela, éduquer les acteurs économiques à la révolution quantique qui s'annonce. Le programme France 2040 pourrait produire des indicateurs de performance et de plus-value des offres quantiques appliquées aux **cas d'usage de référence identifiés** dans la recommandation 7. Ces indicateurs pourraient aussi s'enrichir d'outils de mesure des avantages quantiques par rapport aux avantages offerts par l'IA, et de plus-value du *Quantum Machine Learning* par rapport au *Machine Learning*.
- Un projet pilote européen financé par la Commission européenne et démontrant le bien fondé d'un usage quantique, dans le domaine de la santé ou de la transition énergétique, par exemple, pourrait servir à quantifier **la valeur ajoutée des solutions quantiques dans les modèles d'affaires** et encourager la communauté financière à investir durablement dans les applications logicielles quantiques.
- Parallèlement, des opérations de sensibilisation et de partage d'expérience autour des enjeux d'adoption de technologies de rupture (en premier lieu les usages quantiques et l'IA) avec des acteurs publics tels que la DGE pourraient inciter les entreprises à considérer les

solutions quantiques comme des leviers de productivité et de haute valeur ajoutée. Preuve de ce potentiel, des cabinets de conseils se spécialisent d'ores et déjà dans la sensibilisation des dirigeants d'entreprise à l'adoption du quantique dans leurs métiers et leurs méthodes de travail.

Objectif 6

Militer pour une gouvernance simple et agile adaptée à la maturité du secteur.

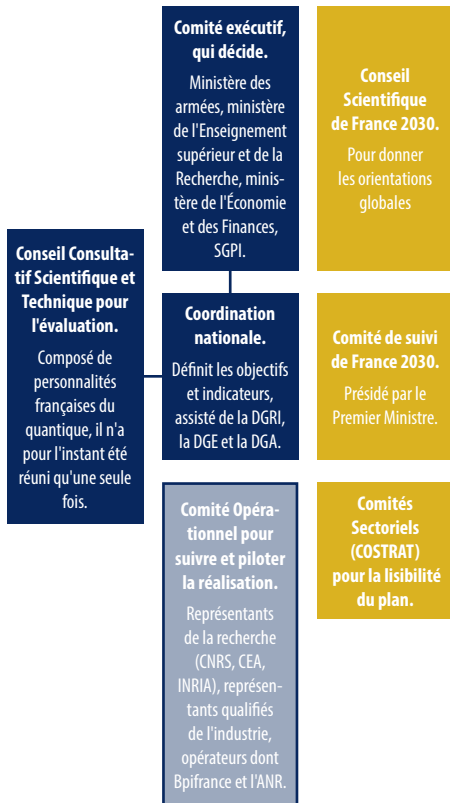
RECOMMANDATION 10

Passer de 6 à 2 instances de gouvernance de la stratégie quantique, l'une dédiée à la réflexion stratégique et l'autre à l'exécution opérationnelle :

1. Confier au Comité exécutif actuel (émanant des ministères concernés) la responsabilité totale de la stratégie quantique nationale et des financements à y allouer.
2. Fusionner le Conseil Consultatif Scientifique et Technique avec le Comité Opérationnel de la stratégie nationale quantique, et l'utiliser pour renforcer la Coordination Nationale en la dotant d'un Comité d'exécution sur le modèle britannique. La Coordination Nationale devra renforcer ses effectifs afin de gérer opérationnellement les crédits budgétaires et les relations avec l'écosystème français et mondial.
3. S'assurer de l'adhésion des différents comités de France 2030 en amont de la prise de décision, à des fins consultatives et d'alignement opérationnel, pour éviter désalignements et doublons.

Gouvernance actuelle :

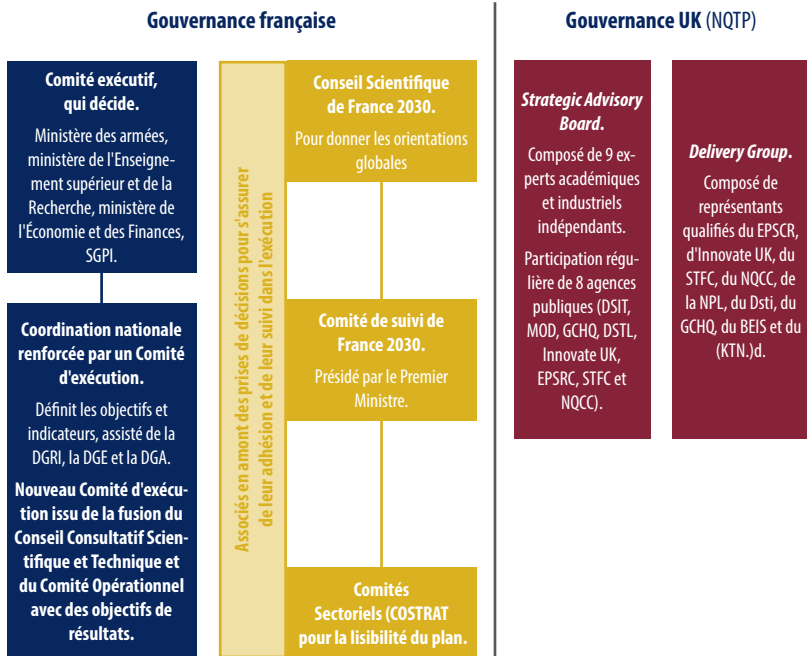
Gouvernance française



Gouvernance UK (NQTP)



Gouvernance recommandée :



Une action immédiate du comité d'exécution de la Coordination Nationale serait d'établir un RACI¹²⁸ pour éviter les doublons ou des compétitions internes contraires à l'objectif global, en cohérence avec les nouvelles priorités de France 2040.

¹²⁸ *Domaine de management ou matrice de responsabilités, emprunté à la méthode anglo-saxonne, dans laquelle apparaissent clairement les acteurs réalisateurs (responsible), approuvateurs (accountable), consultés (consulted) et informés (informed), soit les 4 rôles qu'un membre d'une équipe projet peut exercer sur une tâche spécifique.*

	Responsable	Approbateur	Consulté	Informé
Administrations centrales		✓	✓	✓
Coordinateur national	✓	✓	✓	✓
Startups	✓		✓	✓
Recherche fondamentale	✓		✓	✓
Recherche appliquée	✓		✓	✓
Industries « habilitante »	✓		✓	✓
Partenaires commerciaux			✓	✓

RECOMMANDATION 11

Actualiser tous les deux ans la *roadmap* technologique pilotée par l'Académie des Technologies afin de permettre un ajustement des politiques technologiques dans le temps industriel.

Liste des acronymes utilisés dans la partie Gouvernance

Pour la gouvernance française :

DGRI : direction générale des relations internationales

DGE : direction générale des entreprises

DGA : direction générale de l'armement

CNRS : centre national de la recherche scientifique

CEA : commissariat à l'énergie atomique

INRIA : institut national de recherche en sciences et en technologies du numérique

ANR : agence nationale pour la recherche

Pour la gouvernance britannique :

DSIT : Department for Science, Innovation and Technology

MOD : Ministry of Defence

GCHQ : Government Communications Headquarters

DSTL : Defence Science and Technology Laboratory

EPSRC : Engineering and Physical Sciences Research Council

STFC : Sciences and Technology Facilities Council

NQCC : National Quantum Computing Center

BEIS : Department for Business, Energy and International Strategy

(KTN) : Knowledge Transfer Network

Positionnement des acteurs quantique français sur le hardware

Type	Technologie	Entreprises/Vendeurs	Laboratoires/Universités
Atomes	Ions piégés	Cristal Quantum Computing, IonQ, AQT, Quantinuum, Oxford Ionics, eleQtron, Foxconn	University of Maryland, MIT, Karlsruher Institut für Technology, IQI, Universität Innsbruck, Sandia National Laboratories, NIST, Johannes Gutenberg Universität, Harvard University, University of Sussex
	Atomes froids	Pasqal, ColdQuanta, Atom Computing, QuEra Computing Inc	CNRS, Institut d'Optique , Harvard University, Caltech, Julich, PennState, EPFL, Ohio State University
Électrons, boucles supra-conductrices et spins contrôlés	Annealing	D-Wave, NEC, Qilimanjaro	Nedo, Stanford University, MIT, Karlsruher Institut für Technology, MCQST, ETH Zurich
	Supraconducteurs	Alice & Bob , IBM, Rigetti, Amazon, Google, OQC, QCI, Nord Quantique, Oxford Quantum, QW, IQM, Anyon, Alibaba, Alibaba, EeroQ, Baidu, Bleximo, Fujitsu	CEA, CNRS, Inria , MIT, QUTech, UCSB, UMass Amherst, MCQST, ETH Zurich, Universität des Saarlandes, Berkeley, Yale, Caltech, The University of Tokyo
	Silicium	Qobly, C12 , Intel, Silicon Quantum Computing, diraq, equal1. labs, Archer, QpiAI,	CEA, CNRS , University of Bristol, University of Oxford, UNSW, Yale, HRL, ETH Zurich, University of Wisconsin, EPFL, PRIKEN, Princeton, NTT, QUTech
	Spin	C12, Turing, Quantum Brilliance, Photonic, XEEQ	CEA, CNRS , MIT, University of Maryland, TU Delft, Harvard University, Universität Stuttgart, The University of Chicago
	<u>Ordinateur topologique</u> ¹²⁹	Microsoft, Nokia, Amazon avec les anyons	CEA, CNRS , University of Maryland, UCSB, TU Delft, QuTech, Niels Bohr Institutet, The University of Sydney
Photonique	Photons intriqués	Quandela , PsiQuantum, Xanadu, Orca Computing, QBoson, Duality, Quix, BardeeQ, QCI, Tundra Systems Global	CNRS , University of Bristol, University of Oxford, Sapienza, Universität Wien, The University of Tokyo

Guide de lecture : les acteurs français sont représentés en **gras**.

¹²⁹ Une méthode pour que la mémoire et les mécanismes internes des ordinateurs quantiques reste insensible au bruit: permettrait de créer des qubits simples qui s'auto-protègeraient des influences extérieures, pour diminuer le nombre de qubits simples nécessaires à la construction d'un qubit logique. Par exemple, les anyons gardent en mémoire tout échange de position au cours du temps.

Poids du quantique dans le budget de l'État et les dépenses du PIA

Technologie d'avenir	Montants investis par la France	% du budget pilotable de l'État ¹³⁰	% des dépenses du PIA (54 Mds dans LPFP 2023)
IA	2,22 Mds €	<1 %	4 %
HPC	40 M€ ¹³¹	<1 %	<1 %
Biotech	800 M€ ¹³²	<1 %	<1 %
Spatial	9 Mds € ¹³³	1,8 %	17 %
Cyber	700 M€ ¹³⁴	<1 %	1,2 %
Edge	n/a	0 %	0 %
Cloud	1,8 Mds €	<1 %	3 %
Quantique	1,8 Mds €	<1 %	3 %
Formation	250 M€ ¹³⁵	<1 %	<1 %
Total	18,8 Mds €	9 %	30,2 %

¹³⁰ Pour la clarté de l'exercice, un ordre de grandeur qui s'approche de l'ancienne norme de dépense pilotable de l'État définie dans la LFI pour 2022 (environ 300 Mds euros) a été retenu car cette norme représente les dépenses sur lesquelles l'État dispose d'une marge de manœuvre. En raison de son caractère conjoncturel, elle a toutefois été remplacée par l'agrégat de « périmètre des dépenses de l'État » dans la LFI pour 2023 en intégrant l'ODETE, et s'élève pour 2024 à 496 Mds euros.

¹³¹ Pour le programme de recherche NumPex.

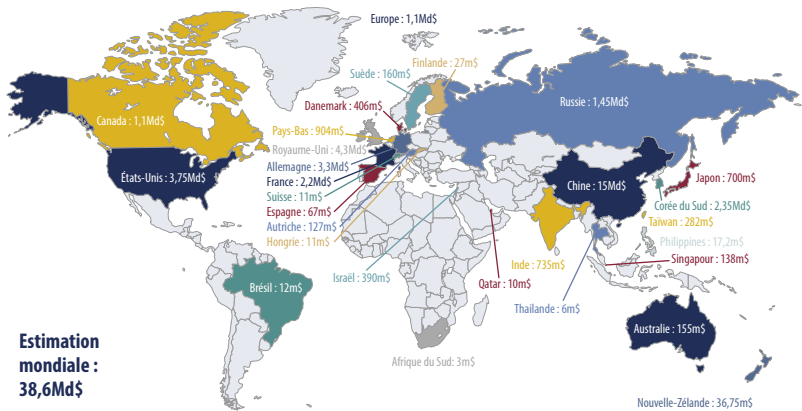
¹³² Pour faire de la France un leader dans les thérapies innovantes (Investir dans la France 2030).

¹³³ France 2030.

¹³⁴ Stratégie nationale cybersécurité – à nuancer par les levées de fonds importantes récentes de nos startups cyber.

¹³⁵ Formation des français aux compétences numériques (Un investissement inédit pour former les Français au numérique).

Efforts d'investissement mondiaux dans la technologie quantique



Source : @QURECA Ltd. 2023.

L'auteur de cette note tient à remercier les membres des ateliers de travail, les relectrices ainsi que toutes les personnes auditionnées ou consultées durant l'élaboration de cette note pour leur aide précieuse, notamment **Neil Abroug, Audrey Durand, Florian Carrière** et les équipes de Waves-tone, **Ali Saib** et **Philippe Englebert**. Une pensée particulière est portée à l'ensemble de l'équipe de l'Institut Montaigne ayant permis sa réalisation, notamment **Marie-Pierre de Bailliencourt, Nicolas Laine, Catherine Merle-Du-Bourg, Erwan Le Brasidéc, Thomas Luquiau, Gaspard Chaney**.

MEMBRES DE LA TASK-FORCE

Startups quantique :

- **Pierre Desjardin**, *CEO* de C12
- **Théau Peronnin**, *CEO* de Alice & Bob
- **Nicolas Proust**, directeur de la stratégie chez Pasqal
- **Niccolo Somaschi**, *CEO* de Quandela
- **Maud Vinet**, *CEO* chez Quobly

Industriels et entreprises :

- **Philippe Englebert**, directeur chez Lazard
- **Luc Gaffet**, *Big Science and Quantum Computing Market Director* chez Air Liquide
- **Frédérique le Grèves**, présidente et *CEO* France et *VP* Europe et France Affaires Publiques chez STMicroelectronics
- **Pierre Jaeger**, *Quantum Strategic Partnerships Executive* chez IBM
- **Béatrice Kosowski**, *CEO* France chez IBM

- **Philippe Magarshack**, *Microcontrollers & Digital ICs Group VP Strategy Technology & System Architecture* chez STMicroelectronics
- **Benoit Renon**, *Partner* chez Moelis & Company
- **Delphine Roma**, *VP Deep Tech Marketing & Strategy* chez Air Liquide
- **Stéphane Tanguy**, *CIO & CTO EDF Labs* chez EDF
- **Philippe Vannier**, *CEO* chez Crescendo Industries

PERSONNES AUDITIONNÉES

- **Neil Abroug**, coordinateur national de la stratégie quantique
- **Florian Carrière**, gérant chez Wavestone
- **Audrey Durand**, responsable de la stratégie de la direction de l'innovation de l'Institut d'Optique
- **Jean Christophe Goujeon**, responsable quantique chez Bpifrance
- **Christophe Jurczak** et **Olivier Tonneau**, gérant chez Quantonation
- **Alfred Kirsch**, doctorant CERMICS-École des Ponts
- **Raphaël-David Lasserri**, co-fondateur de Magic LEMP et docteur en physique théorique et mathématique
- **Victor Martin**, responsable du Hub R&D digital Paris-Saclay de Total Energies
- **Satu Salminem**, responsable quantique de SITRA



Institut Montaigne
59 rue La Boétie, 75008 Paris
Tél. +33 (0)1 53 89 05 60
[*institutmontaigne.org*](http://institutmontaigne.org)

Imprimé en France
Dépôt légal : octobre 2024
ISSN : 1771-6756

ABB France	D'Angelin & Co.Ltd	Katalyse	Renault
AbbVie	Dassault Systèmes	Kea	Ricol Lasteyrie
Accenture	Delair	Kearney	Rivolier
Accor	Deloitte	KPMG S.A.	Roche
Accuracy	De Pardieu Brocas	Kyndryl	Roche Diagnostics
Actual Group	Maffei	La Banque Postale	Rokos Capital
Adeo	Domia Group	La Compagnie	Management
ADIT	Edenred	Fruitière	Rothschild & Co
Air Liquide	EDF	Lenovo ISG	RTE
Airbus	EDHEC Business	Linedata Services	Safran
Allianz	School	Lloyds Europe	Sanofi
Amazon	Ekimetrics France	L'Oréal	SAP France
Amber Capital	Engie	LVMH - Moët-	Schneider Electric
Amundi	EQT	Hennessy - Louis	ServiceNow
Antidox	ESL & Network	Vuitton	Servier
Antin Infrastructure	Eurogroup	M.Charraire	SGS
Partners	Consulting	MACSF	SIER Constructeur
ArchiMed	FGS Global	Média-Participations	SNCF
Ardian	Forvis Mazars	Mediobanca	SNCF Réseau
Arqus	Getlink	Mercer	Sodexo
Arthur D. Little	Gide Loyrette Nouel	Meridiam	SPVIE
AstraZeneca	Google	Microsoft France	SUEZ
August Debouzy	Groupama	Mitsubishi France	Teneo
AXA	Groupe Bel	S.A.S	The Boston
A&O Shearman	Groupe M6	Moelis & Company	Consulting Group
Bain & Company	Groupe Orange	Moody's France	Tilder
France	Hameur et Cie	Morgan Stanley	Tofane
Baker & McKenzie	Henner	Natixis	TotalEnergies
BearingPoint	Hitachi Energy	Natural Grass	TP ICAP
Bessé	France	Naval Group	Transformation
BNP Paribas	Howden	Nestlé	Factory
Bolloré	HSBC Continental	OCIRP	Unicancer
Bouygues	Europe	ODDO BHF	Veolia
Bristol Myers Squibb	IBM France	Oliver Wyman	Verian
Brousse Vergez	IFPASS	Ondra Partners	Verlingue
Brunswick	Incyte Biosciences	OPmobility	VINCI
Capgemini	France	Optigestion	Vivendi
Capital Group	Inkarn	Orano	Wakam
CAREIT	Institut Mérieux	PAI Partners	Wavestone
Carrefour	International SOS	Pelham Media	Wendel
Chubb	Interparfums	Pergamon	White & Case
CIS	Intuitive Surgical	Polytane	Willis Towers Watson
Clariane	Ionis Education	Publicis	France
Clifford Chance	Group	PwC France &	Zurich
CNP Assurances	iQo	Maghreb	
Cohen Amir-Aslani	ISRP	Qualisocial	
Conseil supérieur du notariat	Jeantet Associés	Raise	
	Jolt Capital	RATP	

Les technologies quantiques sont un des arbitrages technologiques cruciaux que la France se doit de faire maintenant si elle entend ne pas répéter les erreurs du passé en matière de nouvelles technologies. Aujourd'hui, la France a une longueur d'avance dans le domaine quantique, ayant fait émerger 4 des 6 technologies quantiques les plus prometteuses. Ces technologies sont essentielles à la mise au point d'algorithmes de calcul plus performants, de systèmes de capteurs plus précis et de méthodes de chiffrement nouvelles.

Cependant, malgré ces atouts, la France et l'Europe accusent un retard notable sur l'adoption et les usages. La France ne capte que 3 % des parts de marché et 1 % des levées de fonds dans le logiciel quantique en 2024. Pourtant, sur les infrastructures quantiques, elle occupe la deuxième place mondiale avec 28 % du marché, juste derrière les États-Unis à 32 %. Pour maintenir cette avance, il est temps d'agir. **Dans la perspective du lancement de l'étape 2 du plan national quantique, le défi est clair : il faut transformer ces innovations en réussites commerciales, sans faire à nouveau l'erreur de rechercher la technologie la plus performante, mais qui ne s'adresse spécifiquement à aucun marché.**

C'est d'autant plus nécessaire que l'incertitude demeure importante concernant les performances futures des technologies quantiques (NISQ ou FTQC) et la montée à l'échelle des technologies habilitantes associées. **Une chose est cependant certaine : des avantages quantiques émergeront ; ils devraient transformer durablement le marché des supercalculateurs** (High Performance Computing) et impacter *a minima* les secteurs de la défense et de la sécurité. Dans quatre secteurs additionnels, la France a su démontrer la valeur des algorithmes quantiques : chimie & pharmaceutique, industrie manufacturière & transport, énergie & développement durable, et finance (banque / assurance).

Le quantique est donc une technologie clé où la France détient un avantage compétitif stratégique et un intérêt sécuritaire majeur. L'enjeu consiste désormais à créer un marché porteur et à savoir valoriser nos innovations. L'Institut Montaigne propose une réponse opérationnelle en cartographiant les usages à fort potentiel et en identifiant les secteurs prioritaires auxquels appliquer des technologies quantiques.

10 €

ISSN : 1771-6756

NAC2410-01