

NOVEMBRE 2019

**PAULA FORTEZA**

Députée des Français d'Amérique latine  
et des Caraïbes

**JEAN-PAUL HERTEMAN**

Ex-PDG de SAFRAN

**IORDANIS KERENIDIS**

Directeur de Recherche au CNRS

**QUANTIQUE :  
LE VIRAGE  
TECHNOLOGIQUE  
QUE LA FRANCE  
NE RATERA PAS**

37 PROPOSITIONS POUR UNE  
STRATÉGIE NATIONALE AMBITIEUSE

Rapporteurs de la mission

NEIL ABOUG

THIERRY DAVID

MATTHIEU RATIÉVILLE

JEAN VANNIMENUS



**Mission confiée  
par le Premier Ministre  
Édouard Philippe**

---

Mission parlementaire  
du 15 avril 2019  
au 3 octobre 2019

Avec l'appui de :

**Marianne Billard • Marion Dos Reis Silva • Jean Éric Michallet • Sébastien Kunz Jacques**



## Avant-propos

### Paula Forteza

Lorsque l'on évolue dans l'écosystème numérique depuis plusieurs années, il est impossible de passer à côté du quantique. Un concept qui apparaît régulièrement dans les échanges entre experts, de manière quasi mystique : d'un côté les convertis, de l'autre les sceptiques. Agnostique sur la question, mais toujours prête à objectiver les débats technologiques, j'ai été honorée que le premier ministre me confie cette mission.

Le quantique n'est pas à l'aube de sa première révolution, puisque dès le début du XX<sup>e</sup> siècle, la physique quantique était déjà à l'origine de nombreux bouleversements technologiques majeurs tels que l'invention du transistor ou du laser. Aujourd'hui, grâce à de nouvelles découvertes en physique fondamentale, nous sommes à nouveau face à l'émergence imminente de nouvelles innovations de rupture, basées, cette fois-ci, sur l'informatique quantique.

À l'heure où j'écris ces quelques lignes, Google serait parvenu à atteindre la suprématie quantique, en arrivant à stabiliser 53 *qubits* suffisamment longtemps pour réaliser en quelques minutes un calcul qui aurait pris 10000 ans au plus puissant des supercalculateurs existants. Le secret et la précaution entourent ces informations émietées dans la presse, indicateur du caractère stratégique qui recouvre ces technologies.

Comprendre la nature de ces innovations, leurs catalyseurs, les obstacles auxquelles elles font face, afin d'identifier les opportunités pour la France et ainsi bâtir une stratégie nationale, a été notre travail au cours de ces derniers mois. Premier

constat : face à la rapidité et à l'incertitude de ces évolutions, seuls les pays qui auront osé prendre des risques trouveront une place dans ce nouveau tournant technologique et pourront donc garantir leur souveraineté. Il y a urgence à agir.

La France est dotée d'un écosystème d'une immense qualité, grâce, notamment, à un tissu de chercheurs académiques hors pair. Mais, si le monde de la recherche est encore principalement à la manœuvre de cette révolution, elle ne peut se passer d'industriels réalisant des investissements importants et testant ces nouvelles innovations. Nos recommandations ont pour principal objectif de tisser des ponts entre ces deux univers, évoluant trop souvent côte à côte.

Je tiens à souligner le volontarisme et l'enthousiasme de cet écosystème. Derrière un sujet complexe, d'une technicité sans égal, demandant de manier physique et ingénierie, quand ce n'est mathématiques avancées et informatique, j'ai rencontré des personnes accessibles, passionnées et tenant à cœur de sensibiliser largement. Nous saurons compter sur eux, tant la prise de conscience des enjeux liés au quantique est l'une des conditions de succès de notre stratégie nationale.

Je me réjouis particulièrement de la présence de nombreuses femmes dans ce domaine. Face à un monde de la recherche et du numérique encore très masculins, elles ont su s'imposer grâce à leur professionnalisme et à la qualité de leur travail. Je pense notamment à Maud

Vinet, à Alexia Auffèves, Pascale Senellart, Elham Kashefi, Eleni Diamanti, ou encore Hélène Perrin que je félicite et remercie de m'avoir inspirée tout au long de cette mission.

Enfin et surtout, un mot sur mes co-porteurs, auprès desquels j'ai énormément appris. Iordanis Kerenidis, expert en algorithmie quantique et digne représentant du monde de la recherche, a su être notre boussole pour ne rien omettre sur le plan technique. Jean-Paul Herteman, quant à lui, a su apporter son expertise du monde de l'entreprise et son retour d'expérience face à de précédents bouleversements technologiques comparables, notamment dans l'aéronautique.

Outre la participation des co-porteurs et l'expertise de l'écosystème français, la réussite de cette mission doit beaucoup au dévouement dont l'administration a su

faire preuve pour nous accompagner dans la construction de cette stratégie. Un remerciement particulier à Neil Abroug pour sa persévérance. Et enfin mon équipe, au sein de laquelle Marianne Billard et Marion Dos Reis Silva ont su admirablement coordonner ce travail collectif.

Entrer dans le jeu international et européen des technologies quantiques est possible à condition que nous déclenchions une mise en mouvement rapide. Aujourd'hui, les ressources humaines et intellectuelles sont prêtes ; nous pouvons nous appuyer sur elles, mais nous devons mobiliser les moyens nécessaires. Grâce à une stratégie nationale ambitieuse, les technologies quantiques sont appelées à faire de notre pays un acteur incontournable dans la scène internationale.

Notre rapport vous invite à cette réflexion.

## Jean-Paul Herteman

J'ai accepté avec un grand intérêt de contribuer à cette mission relative à l'informatique quantique tant le sujet paraissait à la fois passionnant et stratégique à l'ingénieur et dirigeant d'entreprise que je fus. Cet intérêt ne s'est pas démenti, bien au contraire, au fil des auditions et de nos travaux. Et j'espère que vous le partagerez à la lecture de ce rapport.

Cette technologie est une véritable rupture. Ses applications peuvent révolutionner des branches industrielles comme la chimie, la pharmacologie, l'énergie, la métallurgie, l'aéronautique ou les communications. Le terme et l'ampleur de son développement ne sont pas encore cernés avec certitude, mais c'est maintenant ou jamais que les orientations déterminantes doivent être prises.

J'ai eu la chance de consacrer ma carrière à une industrie □ l'aéronautique □ dont la France peut être fière et qui doit son succès à une stratégie constante d'innovation scientifique et technologique et à l'exigence d'excellence industrielle qui prévaut chez ses ingénieurs, techniciens et compagnons.

Je me souviens, également, combien la politique industrielle « des années Pompidou » a été décisive pour redonner à notre industrie la place de premier plan mondial que la seconde guerre mondiale avait occultée.

La situation de l'informatique quantique, plus disruptive et plus complexe est aujourd'hui différente mais les enjeux sont au moins du même ordre, comme l'est la capacité de notre pays à agir et réussir.

Nos recommandations visent à nous donner les moyens de cette réussite.

Sur le plan de l'organisation et des méthodes, nous recommandons de regrouper les acteurs scientifiques et technologiques en « campus », de mettre en place un pilotage de la politique de recherche scientifique, technologique et industrielle étroitement coordonné entre les pouvoirs publics, les instituts de recherche et les entreprises.

Il faudra, également, veiller à mettre en place des formations anticipant les besoins clefs.

Sur le plan des thèmes de développement, l'ambition est de construire une industrie inclusive maîtrisant la totalité de la chaîne de valeur, allant du matériau de base jusqu'aux logiciels optimisés pour les secteurs applicatifs, en passant par la réalisation des puces quantiques, l'intégration des calculateurs et leurs algorithmes spécifiques, sans oublier les technologies habilitantes (cryogénie, lasers etc.) qui font la vraie force d'un tissu industriel.

Cela nécessite évidemment un financement public non négligeable mais incontournable car la seule logique de marché ne permet pas le démarrage de telles ruptures et tous les grands acteurs mondiaux, d'une façon ou d'une autre, y consacrent l'investissement stratégique indispensable.

Je suis personnellement convaincu que cet effort (qui pour être concret représentera de l'ordre de quelques euros par Français et Française pendant 5 à 10 ans peut-être) sera très largement payé de retour et contribuera grandement au développement de notre pays.

## Iordanis Kerenidis

Ma première rencontre avec les algorithmes quantiques remonte à plus de vingt ans, quand, jeune étudiant en Grèce, je découvris l'existence de l'algorithme de factorisation de Peter Shor. Bien que je n'eusse pas alors une idée très claire des répercussions que pourraient avoir ces travaux, il me parut évident qu'il s'agissait là d'une révolution. Cette découverte me convainquit aussi de préparer une thèse en informatique quantique à Berkeley (Université de Californie) et de briguer après mon doctorat un poste de chercheur au MIT, à une époque où cette science était encore un domaine d'étude essentiellement théorique, sans application immédiate, en raison de l'absence de matériel quantique.

En fait, même pendant la décennie suivante, alors que j'avais rejoint les rangs du CNRS, à Paris, depuis 2006, l'idée de disposer d'un ordinateur quantique opérationnel restait un lointain rêve partagé par quelques rares scientifiques. Ce n'est plus le cas aujourd'hui. Ces dernières années, nous avons vu ce rêve devenir celui d'une génération entière, une possibilité de changement total de paradigme dans le domaine des technologies de l'information et de la communication, une promesse de capacités de calcul et de communication sans précédent.

Comme pour tout rêve, le chemin à parcourir pour concrétiser la promesse des technologies quantiques est long et ardu, mais il est aussi parsemé de récompenses, à savoir l'acquisition de nouvelles connaissances scientifiques et des bénéfices technologiques inattendus. Il faut aussi souligner que nous avons déjà réalisé des avancées considérables en la matière : Google annonçait avoir atteint la « suprématie quantique » à l'heure où

nous terminions la rédaction de ce rapport, de nouvelles applications dans les domaines de la chimie, de l'optimisation et de l'apprentissage automatique (*machine learning*) ont considérablement accru les retombées potentielles de l'informatique quantique, et des satellites de communication quantique sont actuellement en orbite autour de la terre. L'heure est à l'optimisme, teinté de prudence. L'heure est aussi venue de reconnaître le potentiel que recèle ce champ d'étude et d'investir dans ce qui constitue l'une des voies les plus prometteuses de découvertes scientifiques, de progrès technologiques et de bienfaits économiques et sociétaux. Les technologies quantiques apportent des avantages remarquables dans les simulations chimiques et physiques, avec des applications potentielles dans l'agriculture, la découverte de nouveaux médicaments et la conception de batteries ; les algorithmes quantiques permettent des accélérations considérables dans les applications d'optimisation et d'apprentissage automatique, notamment dans les domaines de la finance, de l'énergie, de l'automobile et des sciences environnementales ; les réseaux de communication quantique peuvent améliorer à long terme la sécurisation des données sensibles. La révolution quantique pourrait bien voir le jour et il nous incombe de la mener à bien. C'est aussi pour cette raison que nous avons créé en 2014 le « Paris Centre for Quantum Computing » (PCQC), centre de recherche interdisciplinaire à la pointe des technologies quantiques en Europe.

Lorsque l'on m'a demandé de participer à la mission parlementaire chargée de proposer une stratégie nationale en



matière de technologies quantiques, j'ai tout naturellement ressenti une grande émotion, d'abord parce que la France avait décidé d'explorer plus activement les technologies quantiques et, ensuite, parce que j'étais conscient de la responsabilité qu'implique une telle tâche.

En tant que scientifique, mon but est d'aider à créer, grâce aux progrès de la science, un monde meilleur pour chacun, un monde plus équitable, plus éthique et plus respectueux de l'environnement. Pour atteindre ce but, il est important de rassembler nos forces et de créer des alliances avec tous les partenaires à

même de favoriser ces transformations : le secteur public, le secteur privé, la communauté scientifique, les industriels, les investisseurs, les médias, les citoyens et les décideurs politiques.

Je suis convaincu que nos recommandations sont un premier pas vers la création d'un écosystème quantique sain et dynamique associant toutes les parties prenantes, qui permettra de concrétiser le potentiel de rupture des technologies quantiques et d'asseoir le rôle de chef de file de la France et de l'Union européenne dans ce domaine.

## Glossaire

<b>QUBIT</b>	En informatique quantique, un qubit ou « <i>quantum bit</i> » est la plus petite unité de stockage d'information quantique. C'est l'analogue quantique du bit en informatique classique.
<b>SUPERPOSITION</b>	Un bit classique se trouve toujours soit dans l'état $ 0\rangle$ , soit dans l'état $ 1\rangle$ . Dans le cas général, un qubit se trouve dans une superposition de ces deux états, que l'on peut décrire par une combinaison linéaire des deux états : $\alpha \cdot  0\rangle + \beta \cdot  1\rangle$ . Les coefficients $\alpha$ et $\beta$ étant deux nombres complexes vérifiant la relation $ \alpha ^2 +  \beta ^2 = 1$
<b>INTRICATION</b>	L'intrication quantique, ou enchevêtrement quantique, est un phénomène dans lequel deux particules (ou groupes de particules) forment un système lié et présentent des états quantiques dépendant l'un de l'autre quelle que soit la distance qui les sépare. Un tel état est dit « intriqué » car il y a des corrélations entre les propriétés physiques observées de ces particules distinctes. Ainsi, deux objets intriqués $O_1$ et $O_2$ ne sont pas indépendants même séparés par une grande distance, et il faut considérer $\{O_1 + O_2\}$ comme un système unique.
<b>NON-CLONAGE</b>	Une autre particularité du qubit par rapport à un bit classique est qu'il ne peut être dupliqué. En effet, pour le dupliquer, il faudrait pouvoir mesurer les amplitudes $\alpha$ et $\beta$ du qubit unique initial, tout en préservant son état, de sorte à préparer un autre qubit dans le même état $\alpha \cdot  0\rangle + \beta \cdot  1\rangle$ . Ceci est doublement impossible en raison du théorème de « non-clonage »
<b>NISQ</b>	Des calculateurs quantiques NISQ « <i>Noisy Intermediate-Scale Quantum</i> » sont disponibles en accès Cloud depuis quelques années. Les calculateurs quantiques de 50-100 <i>qubits</i> pourront réaliser des calculs qui dépassent les capacités des supercalculateurs classiques d'aujourd'hui. Cependant, le bruit des portes quantiques limitera la taille des circuits quantiques qui peuvent être exécutés de façon fiable. Les dispositifs NISQ permettront d'explorer la physique quantique à corps multiples et pourraient avoir d'autres applications utiles, mais l'ordinateur quantique à 100 <i>qubits</i> ne changera pas le monde tout de suite.
<b>LSQ</b>	Les calculateurs quantiques LSQ « <i>Large Scale Quantum</i> », ne sont pas attendus avant 2030. Grâce à un nombre élevé de <i>qubits</i> et un niveau de bruit faible, ces machines dépasseront de plusieurs ordres de grandeurs, nos capacités de calcul actuelles représentant ainsi des enjeux de compétitivité (e.g. temps de mise sur le marché) et de souveraineté (e.g. renseignement et dissuasion) majeurs.

<b>Suprématie Quantique</b>	La suprématie quantique désigne une situation où un ordinateur quantique permet de réaliser certains calculs inaccessibles aux supercalculateurs actuels dans un temps humainement raisonnable.
<b>Supercalculateur</b>	Un supercalculateur est un ordinateur conçu pour atteindre les plus hautes performances possibles avec les technologies disponibles lors de sa conception. La science des supercalculateurs est appelée « calcul haute performance » ou « calcul intensif » (en anglais : « <i>High-Performance Computing</i> » ou HPC). En 2019, les constructeurs de supercalculateurs font la course pour atteindre « l'Exascale », puissance de calcul correspondant à un milliard de milliard d'opérations par seconde.
<b>Cryogénie et cryostats</b>	La cryogénie est l'étude et la production de très basses températures (inférieures à -150 °C) dans le but de comprendre les phénomènes physiques qui s'y manifestent. La cryogénie possède de très nombreuses applications notamment dans les secteurs alimentaire, médical, industriel, physique et de l'élevage. Les dispositifs permettant d'atteindre ces températures sont appelés Cryostats.
<b>fabless</b>	Le terme <i>fabless</i> , contraction des mots anglophones <i>fabrication</i> et <i>less</i> , désigne une société qui conçoit ses produits et sous-traite l'intégralité de sa fabrication. Ce modèle est principalement développé dans le secteur des semi-conducteurs.
<b>Cryptographie post-quantique</b>	La cryptographie post-quantique désigne des mécanismes de chiffrement classiques basés sur des problèmes mathématiques dont la difficulté reste intacte face à un ordinateur quantique.

## Résumé exécutif du rapport

### Contexte technologique

Si la première révolution quantique a permis l'invention du transistor, des lasers et du GPS, la seconde révolution en cours, fruit de la maîtrise des phénomènes de superposition et d'intrication où les particules peuvent revêtir plusieurs états en même temps ou le même état en deux endroits différents, permettra de décupler exponentiellement nos puissances de calcul, de « téléporter » des informations et d'effectuer des mesures avec des précisions jamais égalées.

### Enjeux

#### CROISSANCE ÉCONOMIQUE

Plusieurs projections macroéconomiques, sur les deux prochaines décennies, attribuent aux technologies quantiques un potentiel de contribution significatif au PIB ainsi qu'à l'emploi dans les pays développés. La stratégie proposée s'inscrit donc dans les objectifs de plein emploi du « Pacte Productif » annoncé par le Président de la République le 25 avril 2019. Les retombées attendues concernent aussi bien les filières qui industrialiseront ces technologies (microélectronique, photonique, logiciels etc.) que celles susceptibles de les exploiter, à court, moyen et long terme et pour lesquelles ces technologies pourront induire un différentiel de compétitivité disruptif (pharmacologie, chimie, matériaux, pharmacologie, pétrole, aéronautique, cyber sécurité etc.).

#### SOUVERAINETÉ TECHNOLOGIQUE

L'évolution du contexte géopolitique, ainsi que la montée en puissance industrielle, particulièrement lente et difficile, incitent les industries de haute technologie mondiales à adopter des stratégies de silos fragilisant les pays ne maîtrisant pas la totalité de la chaîne de valeur technologique.

Ne pas disposer de capacités technologiques propres pourrait, ainsi, poser, à terme, des difficultés en matière d'approvisionnement pour les besoins nationaux, avec des impacts économiques et de souveraineté, ainsi que des barrières à l'export pour les produits industriels.

### Vision

La profondeur de la rupture que pourraient induire les technologies quantiques dans les prochaines décennies est au moins comparable à celle qui résulte de l'invention du transistor au milieu du XX<sup>e</sup> siècle. La France, pionnière de la recherche amont en physique quantique grâce, notamment à la présence de plusieurs prix Nobel ainsi que de chercheurs de premier plan, accuse aujourd'hui un retard réel mais non rédhibitoire en matière de développement technologique et industriel.

Les principales grandes puissances mondiales à l'instar des États-Unis, de la Chine, du Royaume-Uni ou de l'Allemagne, ont mis en place des programmes nationaux globaux ambitieux en matière de technologies quantiques.

En capitalisant sur l'excellence de son tissu de recherche et ses industriels précurseurs, la France pourra, par une politique industrielle et de recherche ambitieuse, développer une vision à long terme couplée à une stratégie de gestion des risques adaptée. Ainsi, la France confirmera sa place de puissance industrielle de premier plan et de leader européen, en développant, avant la fin de la

décennie, une offre technologique de rang mondial en matière de technologies quantiques à l'instar de ce qu'elle a réussi à développer pour le nucléaire et l'aérospatial.

## Ambitions

### DEVENIR L'UN DES LEADERS MONDIAUX EN MATIÈRE DE CALCULATEURS QUANTIQUES TOLÉRANTS AUX DÉFAUTS (LSQ)

Le développement de calculateurs quantiques tolérant aux défauts (LSQ) vise à rendre possible des calculs et modélisations de plusieurs ordres de grandeurs plus complexes que ce qui est aujourd'hui envisageable avec les supercalculateurs traditionnels. Le développement de machines LSQ nécessite de fabriquer des millions de *qubits* de bonne qualité. Le Silicium, l'un des rares matériaux pouvant permettre à terme un tel passage à l'échelle, bénéficie en France d'une recherche de pointe et d'un socle industriel solide en micro-électronique, malgré un retard de quelques années vis-à-vis d'autres pays dont les progrès semblent par ailleurs lents.

La France pourrait ainsi se doter de l'ambition de créer, avant la fin de la décennie, la première entreprise *fabless* européenne proposant des processeurs quantiques à base de Silicium en étroite association avec sa chaîne de valeur amont dont la criticité technologique, industrielle et géostratégique sera majeure.

### DEVENIR LE LEADER EUROPÉEN EN MATIÈRE DE CALCULATEURS QUANTIQUES BRUITÉS DE TAILLE INTERMÉDIAIRE (NISQ)

Sans attendre l'arrivée des calculateurs LSQ, les calculateurs NISQ pourront déboucher à plus court terme sur des usages disruptifs dans les secteurs de la chimie, la logistique et l'intelligence artificielle. En bénéficiant des compétences de ses industriels du calcul intensif et de différentes startups européennes qui développent des processeurs NISQ, la France pourrait développer et diffuser, dès 2023, la première offre européenne d'accélération quantique pour le marché du calcul intensif, en cohérence avec l'agenda européen sur l'acquisition de supercalculateurs Exascale.

### DEVENIR L'UN DES LEADERS MONDIAUX EN MATIÈRE DE LOGICIELS MÉTIERS

Sans outils de développement logiciel adaptés spécifiquement au comportement très particulier des processeurs quantiques, l'usage du calcul quantique aura du mal à s'imposer dans les secteurs aval. Traditionnellement, l'offre logicielle française se caractérise par son positionnement moins générique mais à plus forte valeur ajoutée que ce qui est développé outre-Atlantique.

Les premiers développements de machines NISQ impactant prioritairement des métiers spécifiques, la France pourrait capitaliser sur ses chercheurs en algorithmie et industriels du logiciel pour se positionner en acteur de rang mondial des logiciels métiers exploitant le calcul quantique en proposant, dès 2023, avec le concours de l'Allemagne, la première offre logicielle quantique métier « clé en main » pour les domaines de la chimie, la pharmacologie, les matériaux avancés, la logistique et l'apprentissage en IA.

## JOUIR D'UNE LARGE AUTONOMIE INDUSTRIELLE SUR LES TECHNOLOGIES HABILITANTES

Les technologies habilitantes à l'informatique quantique (cryogénie, ultravide, lasers, câblage etc.) sont un prérequis au développement des différentes technologies quantiques et font appel à des savoir-faire particulièrement rares et pointus. Elles sont ainsi très sensibles à un risque d'embarco de la part des pays qui les maîtrisent.

A l'exception de quelques cas limités, les acteurs français des technologies quantiques s'approvisionnent actuellement à l'étranger.

La France pourrait ambitionner de devenir, avant la fin de la décennie, l'un des principaux fournisseurs mondiaux en technologies habilitantes à l'informatique quantique, en particulier pour la cryogénie et les lasers.

De par leur performance et complexité, ces technologies pourront naturellement trouver des débouchés dans d'autres secteurs hautement technologiques.

## JOUIR D'UNE LARGE AUTONOMIE INDUSTRIELLE SUR LES CAPTEURS À BASE DES IMPURETÉS DANS LE DIAMANT

Les capteurs quantiques à base d'impuretés dans le diamant présentent l'avantage de pouvoir passer aisément à l'échelle industrielle.

Forte de ses acteurs industriels positionnés sur l'aval de la chaîne de valeur, la France pourrait avoir pour ambition, en profitant d'une part du retrait de certains acteurs étrangers historiques, d'autre part des compétences et savoir-faire de ses laboratoires académiques de pointe, de devenir un fournisseur mondial de premier plan de diamants pour les capteurs à base d'impuretés dans le diamant, à horizon 2026, et ainsi couvrir l'ensemble de la chaîne de valeur industrielle des capteurs quantiques.

## MAINTENIR UNE INDÉPENDANCE STRATÉGIQUE SUR LES TECHNOLOGIES DE CRYPTOGRAPHIE

L'avènement possible de calculateurs quantiques suffisamment puissants (LSQ) pour casser les schémas de chiffrement actuels (e.g. RSA), même si cela ne se réalisera qu'à relativement long terme, appelle des actions immédiates en matière de sécurisation des communications sensibles.

Forte d'une communauté de cryptographes de rang mondial et d'industriels de sécurité de premier plan, la France pourrait viser le développement, dès 2022, de la première offre de cryptographie post-quantique pour des dispositifs de sécurité de haute performance et à ressources de calcul limitées (module cryptographiques, cartes à puces, routeurs etc.).

A plus long terme, la France pourrait envisager de proposer, dans les 5 ans, la première solution de distribution quantique de clés de chiffrement, déployable à coût d'infrastructures marginal et résistant aux attaques par canaux auxiliaires et par déni de service.

# Recommandations de la mission

## UNE INFRASTRUCTURE DE POINTE POUR LA RECHERCHE ET L'INDUSTRIE

La mise en place, sur le sol français, d'une infrastructure de rang mondial, intégrant différents émulateurs et accélérateurs quantiques basés sur des principes technologiques divers, représentera un levier d'action fort permettant de développer l'écosystème logiciel et les usages et de développer la légitimité et le rayonnement de la France à l'international ;

Un rapprochement avec l'Allemagne pourrait permettre de développer une offre commune et un portail commun permettant l'accès à l'ensemble des technologies de calcul quantique européennes.

## UN PROGRAMME DE SOUTIEN AU DÉVELOPPEMENT TECHNOLOGIQUE

Avec des programmes de recherche et développement technologique associant acteurs publics et privés en combinant les approches « *top-down* » et « *bottom-up* », la France se donnera les moyens nécessaires à la levée des différents verrous scientifiques et technologiques jalonnant le développement de l'ordinateurs quantique, ainsi que des dispositifs de cryptographie nécessaires à la sécurisation des communications sensibles à l'ère du quantique.

En matière de dispositifs « *bottom-up* », la France pourrait renforcer les dispositifs existants et y inclure des priorités sur les technologies quantiques : appels à projets ANR, concours d'Innovation, PSPC (Projets Structurants pour la Compétitivité), etc.

En matière de dispositifs « *top-down* », les Grands-Défis ainsi que des actions du Plan d'Investissement d'Avenir pourront permettre d'atteindre les ambitions françaises en matière d'ordinateur quantique, en matière de logiciel, de capteurs, et de cryogénie.

## UN PROGRAMME DE SOUTIEN AU DÉVELOPPEMENT DES USAGES

Des « challenges quantiques » associant secteurs d'usages et secteurs technologiques, aussi bien dans le domaine du calcul quantique que dans le domaine des capteurs quantiques permettront de renforcer la compétitivité des secteurs aval tout en sécurisant les débouchés court-terme des secteurs technologiques.

## UN ENVIRONNEMENT D'INNOVATION EFFICACE

La création de trois instituts interdisciplinaires en information quantique (3IQ) sera un levier déterminant du brassage interdisciplinaire nécessaire à la levée des verrous jalonnant les objectifs de la stratégie nationale. Le développement des compétences et l'accès au capital risque permettront de lever les freins à l'innovation et à la création de startups, vecteur incontournable du transfert de technologies vers le tissu économique.

## UNE STRATÉGIE DE SÉCURITÉ ÉCONOMIQUE ADAPTÉE

La position de la France en matière de technologies quantiques encourage certains organismes ou États à s'intéresser à l'écosystème français et à cibler les acteurs les plus vulnérables, en pointe au niveau mondial. La protection du patrimoine scientifique et technologique et la diplomatie économique seront les piliers d'une stratégie d'intelligence économique efficace.

## UNE GOUVERNANCE EFFICACE

Compte tenu du niveau élevé d'incertitudes relatif à certaines voies de développement des technologies quantiques, les horizons de temps longs des actions à mener et l'intensité capitalistique nécessaire, l'État aura besoin d'une gouvernance agile et dotée d'un pouvoir décisionnel.

# Liste des 37 propositions

## Propositions transverses

<b>Proposition 5</b>	<i>Reconduire, à partir de 2021, les appels à projets (AAPR) de l'axe « Technologies Quantiques » de l'Agence Nationale de la Recherche (ANR) visant à financer annuellement vingt projets exploratoires pour une enveloppe annuelle globale de 10 M€.</i>
<b>Proposition 6</b>	<i>Renforcer l'axe « Technologies Quantiques » de l'ANR par une enveloppe annuelle spécifique visant à financer trois projets exploratoires ciblant les voies technologiques prioritaires identifiées.</i>
<b>Proposition 7</b>	<i>Inciter les laboratoires et entreprises français à répondre aux appels à projets européens Flagship « Quantum Technologies ».</i>
<b>Proposition 8</b>	<i>Inclure une priorité sur les technologies quantiques dans les futurs appels PSPC et Concours d'innovation.</i>
<b>Proposition 26</b>	<i>Créer, à Paris, à Saclay ainsi qu'à Grenoble, trois « Instituts Interdisciplinaires en Information Quantique » (3IQ) rassemblant chercheurs en physique quantique, chercheurs en informatique théorique et appliquée, ingénieurs, industriels des filières technologiques, et utilisateurs finaux.</i>
<b>Proposition 27</b>	<i>Intégrer un critère d'évaluation relatif à l'interdisciplinarité dans les appels à projets collaboratifs de l'ANR et de la BPI.</i>
<b>Proposition 28</b>	<i>Inclure 6 ECTS d'algorithmie quantique dans les vingt principaux cycles d'ingénieurs en informatique et 6 ECTS de cryptographie post-quantique et quantique dans les masters de cryptographie.</i>
<b>Proposition 29</b>	<i>Concevoir des parcours de formation avec une spécialisation en ingénierie et en informatique quantique et anticiper la croissance du besoin en ingénieurs et techniciens des filières industrielles.</i>
<b>Proposition 30</b>	<i>Sensibiliser les acteurs de l'écosystème aux nouvelles dispositions de la loi PACTE relatives à la mobilité des chercheurs et l'accès aux moyens des laboratoires par les startups.</i>
<b>Proposition 31</b>	<i>Accompagner la création d'une cinquantaine de startups du quantique jusqu'en 2024.</i>
<b>Proposition 32</b>	<i>Faire émerger un fond d'investissement « late-stage » de confiance de 300-500 M€ dédié aux startups du quantique.</i>
<b>Proposition 33</b>	<i>Sensibiliser les différents acteurs les plus stratégiques aux risques de pillage technologique et aux outils disponibles permettant d'y faire face.</i>



<b>Proposition 34</b>	<i>Repérer et surveiller les actifs et activités stratégiques et déployer, au besoin, le dispositif de Protection du Potentiel Scientifique et Technologique (PPST).</i>
<b>Proposition 35</b>	<i>Identifier les espaces de coopérations et les synergies possibles avec les partenaires internationaux de la France en matière de technologies quantiques.</i>
<b>Proposition 36</b>	<i>Constituer un Comité Stratégique chargé de prendre les décisions d'orientation des actions de recherche.</i>
<b>Proposition 37</b>	<i>Nommer un coordinateur interministériel du plan national, chargé de veiller à la cohérence globale des actions des différents acteurs publics et privés au niveau national.</i>

## Propositions relatives au calcul quantique

<b>Proposition 1</b>	<i>Héberger, au « Très Grand Centre de Calcul » (TGCC), une plateforme de Calcul Quantique diversifiée, évolutive et accessible aux communautés de chercheurs et développeurs académiques et industriels.</i>
<b>Proposition 2</b>	<i>Ouvrir un appel à contributions permanent à destination des startups et laboratoires français et européens développant des processeurs d'accélération quantique en vue d'une intégration à l'infrastructure de calcul.</i>
<b>Proposition 3</b>	<i>Développer une offre public-privé de QCaaS ou « Quantum Computing as a Service » compétitive.</i>
<b>Proposition 9</b>	<i>Renforcer les équipes microélectroniques grenobloises par des compétences en logiciels et architectures de calcul.</i>
<b>Proposition 10</b>	<i>Déployer une gestion de projet agile afin de réduire progressivement les incertitudes et les coûts tout au long du projet.</i>
<b>Proposition 11</b>	<i>Déployer, au moyen d'une action du PIA et du PPR, un programme de R&amp;D-Capitalisation visant à développer des accélérateurs quantiques scalables.</i>
<b>Proposition 12</b>	<i>Soutenir, à travers les AAPR de l'axe « Technologies Quantiques » de l'ANR, un programme de recherche visant à explorer des voies Silicon audacieuses</i>
<b>Proposition 13</b>	<i>Mettre en place, en 2019, un Grand Défi de l'Innovation « NISQ » visant à développer, avant 2023, une pile logicielle métier interopérable pour les secteurs de la chimie, de la logistique et de l'IA.</i>
<b>Proposition 14</b>	<i>Inscrire le Grand Défi dans un cadre de collaborations bilatérales avec d'autres pays européens.</i>

<b>Proposition 15</b>	<i>Renforcer les moyens de recherche en algorithmes et logiciels dans le domaine du calcul quantique.</i>
<b>Proposition 16</b>	<i>Mettre en place, en 2022, un Grand Défi de l'Innovation visant à développer une solution de calcul quantique complète, sous réserve de résultats intermédiaires probants pour le Grand Défi « NISQ » et pour l'action PIA « accélérateurs quantiques ».</i>
<b>Proposition 17</b>	<i>Inclure des spécifications pour l'acquisition d'accélérateurs quantiques expérimentaux dans certains appels d'offres de GENCI relatifs à l'acquisition, au renouvellement et à l'extension du parc de supercalculateurs français.</i>
<b>Proposition 24</b>	<i>Diffuser l'usage du calcul quantique, à travers des « Challenges » et « Hackathons » proposés par les industriels des secteurs applicatifs les plus avancés. Le « Airbus Quantum Computing Challenge » pourra être pris comme modèle.</i>

## Propositions relatives aux capteurs quantiques

<b>Proposition 18</b>	<i>Structurer au moyen d'une succession de projets i-Lab, i-Nov et PSPC-Région une chaîne de valeur industrielle de production de capteurs à base d'impuretés dans le diamant.</i>
<b>Proposition 25</b>	<i>Accompagner, à travers des « Challenges » proposés par les secteurs applicatifs, les fabricants de capteurs quantiques dans la recherche de débouchés auprès des secteurs applicatifs.</i>

## Propositions relatives à la cryptographie post-quantique et quantique

<b>Proposition 4</b>	<i>Déployer une plateforme de test pour différents dispositifs de communications quantiques.</i>
<b>Proposition 19</b>	<i>Soutenir, à travers les concours i-Nov et les dispositifs de soutien et d'accélération de l'innovation des ministères concernés, le développement, avant 2022, d'une offre compétitive de cryptographie post-quantique pour systèmes à ressources de calcul limitées.</i>
<b>Proposition 20</b>	<i>Elaborer une stratégie d'évaluation des systèmes QKD s'appuyant sur le schéma de certification français et européen.</i>
<b>Proposition 21</b>	<i>Soutenir, à travers les AAPR de l'axe « Technologies Quantiques » de l'ANR, une action de recherche relative à la maturation de la technologie QKD (systèmes à variables continues et à variables discrètes, relais quantiques, liens satellite, etc.) impliquant les experts des communications quantiques, les experts de la cybersécurité et les équipementiers télécom.</i>

## Propositions relatives aux technologies habilitantes

<b>Proposition 22</b>	<i>Soutenir, à travers les concours i-Lab, les concours i-Nov et projets PSPC, le développement d'une offre française compétitive en matière d'ultravide et de cryogénie compacts pour les températures de 1 à 40 K.</i>
<b>Proposition 23</b>	<i>Soutenir, à travers les concours i-Lab, les concours i-Nov, les projets PSPC et les dispositifs de soutien et d'accélération de l'innovation des ministères concernés, ou d'une action du PIA, le développement d'une offre française compétitive en matière de cryogénie extrême pour les températures sub-K.</i>



# Table des matières

Avant-propos.....	3
Glossaire.....	8
Résumé exécutif du rapport .....	10
Liste des 37 propositions .....	14
<b>I. Introduction aux technologies quantiques.....</b>	<b>21</b>
I.1 Calcul Quantique.....	21
I.2 Capteurs Quantiques.....	24
I.3 Cryptographie Quantique et Post-Quantique.....	24
I.4 Ecosystèmes mondiaux.....	25
<b>II. Enjeux des technologies quantiques.....</b>	<b>26</b>
II.1 Calcul Quantique .....	26
II.2 Capteurs Quantiques.....	29
II.3 Cryptographie Quantique et Post-Quantique.....	30
<b>III. Verrous du développement des technologies quantiques .....</b>	<b>32</b>
III.1 Verrous technologiques .....	32
III.1.1 Calcul quantique .....	32
III.1.2 Capteurs quantiques.....	34
III.1.3 Cryptographie Quantique et Post-Quantique.....	34
III.1.4 Technologies habilitantes .....	36
III.2 Verrous non technologiques.....	38
III.2.1 Coordination et efficacité de l'écosystème .....	38
III.2.2 Développement des compétences .....	39
III.2.3 Taille de marché et cycles de Hype.....	39
<b>IV. Ambitions de la France en matière de technologies quantiques .....</b>	<b>41</b>
IV.1 Calcul Quantique .....	41
IV.1.1 Devenir l'un des leaders mondiaux en matière de calculateurs « LSQ » .....	41
IV.1.2 Devenir le leader européen en matière de calculateurs « NISQ ».....	41
IV.1.3 Devenir l'un des leaders mondiaux en matière de logiciels métiers .....	42
IV.2 Capteurs Quantiques et Technologies Habilitantes.....	44
IV.2.1 Jouir d'une large autonomie industrielle sur les technologies habilitantes .....	44
IV.2.2 Jouir d'une large autonomie industrielle dans les capteurs à base d'impuretés dans le diamant.....	44
IV.3 Cryptographie Quantique et Post-Quantique.....	45
IV.3.1 Maintenir une indépendance stratégique sur les technologies de cryptographie post-quantique .....	45

<b>V.</b>	<b>Recommandations de la mission pour une stratégie nationale.....</b>	<b>46</b>
V.1	<i>Une infrastructure de pointe pour la recherche et l'industrie.....</i>	46
V.1.1	Calcul Quantique.....	46
V.1.2	Communications quantiques.....	47
V.2	<i>Un programme de soutien au développement technologique.....</i>	49
V.2.1	Soutien transversal à l'ensemble des technologies quantiques.....	49
V.2.2	Soutien aux ambitions françaises en matière de Calcul Quantique.....	50
V.2.3	Soutien aux ambitions françaises en matière de Capteurs Quantiques.....	54
V.2.4	Soutien aux ambitions françaises en matière de Cryptographie.....	54
V.2.5	Soutien aux ambitions françaises en matière de Technologies habilitantes.....	55
V.3	<i>Un programme de soutien au développement des usages.....</i>	56
V.3.1	Calcul Quantique.....	56
V.3.2	Capteurs Quantiques.....	56
V.4	<i>Un environnement d'innovation efficace.....</i>	57
V.4.1	Instituts Interdisciplinaires.....	57
V.4.2	Développement des compétences.....	58
V.4.3	Mobilité des chercheurs.....	59
V.4.4	Capital Risque.....	59
V.5	<i>Une stratégie de sécurité et d'intelligence économique adaptée.....</i>	61
V.5.1	Protection du patrimoine scientifique et technologique.....	61
V.5.2	Diplomatie Economique.....	61
V.6	<i>Une gouvernance efficace.....</i>	62
	<b>La mission.....</b>	<b>63</b>
	<b>Personnes auditionnées.....</b>	<b>64</b>

# I. Introduction aux technologies quantiques

## I.1 Calcul Quantique

Dans les années 1980, Richard Feynman, l'un des physiciens les plus influents de la seconde moitié du XX<sup>e</sup> siècle et prix Nobel de physique, pose les bases d'un nouveau paradigme de calcul basé sur les étonnantes propriétés de la physique quantique que sont l'intrication et la superposition. Il propose alors le calcul quantique comme un moyen de simplifier les calculs de modélisation chimique à l'échelle atomique et moléculaire.

L'intérêt pour ce domaine s'est accru, dans les années 1990, avec l'introduction de l'algorithme de *Shor*, qui montre qu'un calculateur quantique accélérerait de façon exponentielle la résolution d'une classe de problèmes de cryptanalyse importante, menaçant potentiellement les principales méthodes de chiffrement asymétrique utilisées pour protéger les communications. Cette période se caractérise également par la découverte de l'algorithme de *Grover* qui, implémenté, pourrait accélérer quadratiquement la recherche, dans une liste non classée, d'un élément spécifique.

Ces accélérations résultent de la capacité des calculateurs quantiques à effectuer plusieurs calculs simultanément. L'unité de base des ordinateurs classiques est le *bit*, qui ne peut prendre qu'un seul état à la fois, 0 ou 1, alors que les *bits* quantiques, ou *qubits*, unités de base des ordinateurs quantiques peuvent se trouver à la fois à l'état 0 et 1. Le concept selon lequel les *qubits* peuvent exister dans plusieurs états en même temps est appelé superposition, ce qui signifie que quelque chose peut être « ici » et « là » ou « en haut » et « en bas » simultanément. Le concept selon lequel deux *qubits* peuvent avoir des états corrélés est appelé intrication : la connaissance de l'état de l'un permet de connaître l'état de l'autre même s'il en est géographiquement loin. La superposition permet à un *qubit* d'encoder plusieurs informations en parallèle, tandis que l'intrication permet, grâce à des portes logiques, de faire interagir les *qubits* entre eux et de traiter les informations simultanément. Bien que déroutants, ces principes permettent à 2 *qubits* de représenter l'équivalent de 4 *bits*, 3 *qubits*, l'équivalent de 8 *bits*, et  $n$  *qubits*, l'équivalent de  $2^n$  *bits* en même temps. Les capacités de parallélisation de calcul d'un calculateur quantique augmentent donc exponentiellement avec le nombre de *qubits*,

Cofondateur d'Intel, Gordon Moore affirmait dès 1965 que le nombre de transistors par circuit de même taille allait doubler, à prix constant, tous les dix-huit mois. Il en déduisit que la puissance des ordinateurs allait croître de manière exponentielle, et ce pour des années. Sa loi, fondée sur un constat empirique, a été vérifiée jusqu'à aujourd'hui. En 1997, il avait prédit que cette croissance se heurterait aux environs de 2020 à la limite de la taille des atomes.

permettant aux calculateurs quantiques d'effectuer des opérations de calcul physiquement inaccessibles au plus puissant des supercalculateurs.

Néanmoins, l'exploitation efficace de cette puissance n'est pas triviale et nécessite le développement de nouvelles méthodes algorithmiques et outils de développement.

À ce jour, le calcul quantique représente le seul modèle de calcul connu susceptible de nous affranchir du ralentissement de la loi de Moore et d'offrir une accélération exponentielle, économiquement tenable, par rapport aux ordinateurs et supercalculateurs classiques.

La cryptanalyse est l'étude de textes chiffrés et de systèmes de chiffrement dans le but de comprendre leur fonctionnement et d'identifier et d'améliorer les techniques permettant de les déchiffrer.

Longtemps cantonnés à la sphère de l'informatique théorique, les premiers calculateurs quantiques fonctionnels n'ont pu être développés et construits que 30 ans après la proposition de Feynman. Aujourd'hui, le nombre d'entreprises construisant des calculateurs quantiques basés sur des technologies et matériaux différents est en perpétuelle croissance. Il convient de citer : D-WAVE, IBM, RIGETTI, Google, IonQ, PASQAL (France), PsiQuantum, Honeywell, etc.

La réalisation de *qubits* repose soit sur des systèmes physiques à l'instar des atomes, photons, et ions, soit sur des systèmes artificiels à base de supra et semi-conducteurs (cf. Figure 1).

Ces *qubits*, dits « physiques », sont vulnérables au bruit. Pour créer des *qubits* tolérants aux défauts, appelés également *qubits* logiques, se comportant exactement comme leurs modèles mathématiques, il faut utiliser des méthodes de correction d'erreurs et de tolérance aux fautes, qui utilisent plusieurs *qubits* physiques pour créer un *qubit* logique.

Il en découle deux grands types de calculateurs quantiques :

- Un calculateur quantique « universel » de puissance significative appelé « LSQ » pour « *Large Scale Quantum* » qui serait composé de milliers de *qubits* logiques et aurait la possibilité de réaliser tout type de calcul quantique. Ce type de calculateur surpasserait de manière exponentielle le plus puissant des supercalculateurs actuels pour un grand nombre d'applications. Les premiers calculateurs « LSQ » ne sont pas attendus avant 2030.
- Un calculateur quantique « bruité » de taille intermédiaire appelé « NISQ » pour « *Noisy Intermediate Scale Quantum* », qui serait, *a contrario*, composé de quelques centaines de *qubits* physiques permettant de réaliser un certain nombre de calculs spécifiques. Ce type de calculateurs a vu le jour il y a quelques années dans des machines développées, notamment, par IBM, Google, et RIGETTI avec quelques dizaines de *qubits*.

En dépit de ses promesses de puissances de calcul inégalées, un calculateur quantique n'a pas vocation à remplacer un ordinateur classique ni même un supercalculateur car il ne présente un avantage que pour certains problèmes. Le calculateur quantique doit être vu comme un coprocesseur « *Quantum Processing Unit* » ou QPU<sup>1</sup> qui accélérera certains calculs bien spécifiques au même titre qu'un GPU (processeur graphique) ou un NPU (processeur IA). En revanche, pour ce type de calculs, le gain de temps sera exponentiel (passage de plusieurs milliers d'années à quelques heures), rendant accessibles certains calculs irréalisables en pratique à ce jour : simuler le repliement d'une protéine, concevoir un catalyseur pour la fabrication d'engrais azotés à basse température, concevoir un catalyseur pour stocker le CO<sub>2</sub>, simuler des systèmes complexes (climat, météorologie, aviation), factoriser des grands nombres, etc.

Un calculateur quantique peut être émulé sans apporter d'accélération tangible sur un ordinateur conventionnel, pour lequel le nombre de *qubits* (logiques) à émuler est limité par la mémoire de l'ordinateur. La plus grande émulation réalisée à ce jour a nécessité un supercalculateur de plusieurs pétaoctets de mémoire pour représenter 46 *qubits* (Jülich). Sur un serveur d'entreprise, le record est à 41 *qubits* (Atos QLM). Un vrai calculateur quantique de 50 *qubits* permettrait de réaliser en un temps raisonnable des calculs nécessitant des milliers d'années sur un supercalculateur. **Ce seuil de 50 *qubits* correspond à peu près à celui de la « suprématie quantique ».** A partir de quelques centaines de *qubits*, plusieurs applications pratiques pourraient être envisagées : prédire les interactions entre une protéine et un nouveau médicament, prédire les propriétés macroscopique d'un nouveau matériau, etc.

<sup>1</sup> On parle également d'accélérateur quantique



	<b>supra-conducteurs</b>		<b>Si spin CMOS</b>		<b>ions piégés Yt ou Ca</b>		<b>photons</b>		<b>impuretés diamants</b>		<b>fermions de Majorana</b>		<b>atomes froids</b>
<b>qubits</b>	supra-conducteurs + effet Josephson	spin d'électrons dans semi-conducteur	ions piégés magnéti-quement	photons	spin d'électron dans cavité diamant + azote	quasi-particules faites de paires d'anyons	niveau d'énergie de la cavité	niveau orbital d'électron	micro-ondes, émission de photons	ionisation et recueil d'électron	6 qubits (QDTI)	0	<20
<b>état</b>	phase de résonance ou sens du courant	spins d'électrons	niveau énergétique de l'ion piégé	polarisation, temps, espace, couleur	niveau d'énergie de la cavité	sens de l'anyon	laser	inversions 2D d'anyons	fusion d'anyons	micro-ondes, émission de photons	20 (Chine)	79 (IonQ)	49 qubits (Intel)
<b>portes</b>	micro-ondes 5 GHz et effet Josephson	micro-ondes	laser	interférence quantique	laser	laser	détecteur de photons	6 qubits (QDTI)	0	<20	20 (Chine)	79 (IonQ)	49 qubits (Intel)
<b>mesure</b>	magnétomètre	conversion spins to charge	fluorescence	détecteur de photons	fluorescence	fluorescence	fluorescence	6 qubits (QDTI)	0	<20	20 (Chine)	79 (IonQ)	49 qubits (Intel)
<b># max de qubits</b>	53 qubits (IBM et Google)	conversion spins to charge	fluorescence	détecteur de photons	fluorescence	fluorescence	fluorescence	6 qubits (QDTI)	0	<20	20 (Chine)	79 (IonQ)	49 qubits (Intel)

en rouge : chipsets non caractérisés et benchmarkés.

source : Olivier Ezratty, « Comprendre l'informatique quantique »

Figure 1: panorama des technologies de fabrication de qubits - crédit: O. Ezratty

## 1.2 Capteurs Quantiques

En exploitant la sensibilité extrême des états quantiques, les capteurs quantiques atteignent des précisions de mesure inégalées. Ces capteurs exploitent les propriétés d'intrication des objets quantiques (atomes, molécules, photons etc.) pour améliorer la sensibilité, la reproductibilité et la justesse des mesures.

Il faut distinguer deux principales catégories de capteurs quantiques dont la maturité permet des applications dès aujourd'hui ou à court terme :

- Les atomes et ions refroidis par laser : cette technologie permet de préparer un système quantique présentant des propriétés quasi-idéales pour différents types de mesure de précision. Elle permet en particulier de réaliser des mesures inertielles de très haute performance, et présente un fort intérêt pour le développement d'une nouvelle génération de gravimètres, gradiomètres de gravité, accéléromètres et gyroscopes ainsi que pour des mesures ultimes de temps-fréquence permettant d'avoir des horloges d'une stabilité remarquable.
- Les impuretés dans le diamant : cette technologie présente plusieurs avantages intrinsèques liés d'une part aux performances (cohérence, résolution, sensibilité) et d'autre part pour la facilité de mise en œuvre (état solide, fonctionnement à température ambiante, manipulation tout optique).

Une 3<sup>ème</sup> voie, l'illumination quantique, qui vise à exploiter l'intrication de paires de photons pour améliorer les performances de détection ou d'imagerie active d'objets à distance, fait également l'objet de recherches mais son niveau de maturité plus faible, au stade du concept ou des premières expérimentations en laboratoire, ne permet pas d'envisager des applications industrielles à court terme.

## 1.3 Cryptographie Quantique et Post-Quantique

Les communications quantiques sont des technologies exploitant les propriétés d'intrication et de non-clonage et visent à renforcer la sécurité ou l'efficacité des télécommunications.

La distribution quantique de clés souvent abrégée QKD pour « *quantum key distribution* » est une méthode de communication qui met en œuvre un protocole de cryptographie symétrique classique mais en exploitant les propriétés d'intrication et de non-clonage. Elle permet à deux individus de produire une clé secrète aléatoire partagée par un canal quantique, connue d'eux seuls et qui peut ensuite être utilisée pour chiffrer et déchiffrer des messages en utilisant des canaux traditionnels, assurant, ainsi, leur intégrité et empêchant leur modification par un tiers (cf. Figure 2). La distribution quantique de clés permet d'assurer, sous certaines hypothèses d'implémentation, que la clé commune obtenue n'a pas pu être interceptée, ce qui est quasi-impossible de garantir en cryptographie classique. L'originalité de cette technologie est que cette assurance ne dépend pas de la puissance de calcul ou du savoir-faire mathématique d'un attaquant, contrairement à ce qui se passe en cryptographie classique. Elle repose en revanche sur des postulats de la mécanique quantique (théorème de non-clonage, principe d'incertitude), et sur la qualité de sa réalisation pratique. La QKD est parfois présentée comme rendue nécessaire par l'avènement de l'ordinateur quantique, dans le

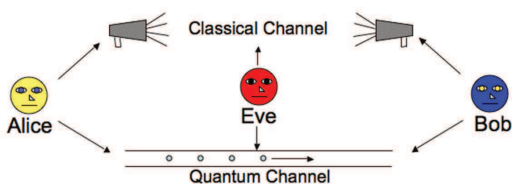


Figure 2: Principe de la distribution quantique de clés

sens où elle permet de remplacer des primitives de cryptographie classique qui sont menacées par les calculateurs quantiques.

La cryptographie post-quantique est une autre réponse possible aux capacités de cryptanalyse (déchiffrement d'un message chiffré) d'un ordinateur quantique. Ce terme désigne des mécanismes de chiffrement asymétrique classiques basés sur des problèmes mathématiques dont la difficulté reste intacte face à un ordinateur quantique.

Des compétitions internationales, sous l'égide du « *National Institute of Standards and Technology* » (NIST), principal organisme de normalisation aux États-Unis, sont actuellement en cours pour identifier de tels mécanismes, et en normaliser les plus prometteurs. Cette approche est similaire à celle ayant normalisé les algorithmes de chiffrement basés sur le logarithme discret et la factorisation utilisés aujourd'hui<sup>2</sup>.

En cryptographie symétrique, l'émetteur et le récepteur du message partagent la même clé pour chiffrer et déchiffrer l'information. Le problème de ce chiffrement est qu'il nécessite un moyen sûr de transmettre la clé mais représente, actuellement, le moyen de chiffrement le plus sûr.

Le chiffrement asymétrique repose sur deux clés. Tout le monde peut encoder avec la première clé (publique), mais seul le récepteur peut décoder avec la seconde clé (privée). La clé privée n'est jamais transmise. La sécurité du chiffrement asymétrique repose sur la difficulté de résolution de certains problèmes mathématiques (factorisation des nombres premiers, courbes elliptiques, etc.)

## 1.4 Écosystèmes mondiaux

Avec un écosystème déjà structuré autour de 40 startups, 50 fonds de capital-risque, 4 grandes entreprises technologiques (Google, IBM, Intel, Microsoft) et 3 agences gouvernementales opérant 1,3 Md\$ d'argent public, les USA disposent d'une avance importante par rapport aux autres pays.

Outre-Rhin, l'Allemagne dispose d'un programme national sur 5 ans doté d'un budget de 650M€.

Outre-Manche, le Royaume-Uni consacre 270 M£ à son programme industriel « Quantum Technologies ».

Forte de ses découvertes pionnières au niveau scientifique, la France dispose en outre de plusieurs atouts pour devenir un compétiteur industriel sérieux dans l'informatique, notamment grâce au positionnement :

- de ses organismes de recherche publique, CNRS, CEA, et INRIA sur différentes technologies quantiques, ce qui offre à ce stade de maturité une gestion des risques adaptée,
- de ses grands groupes industriels utilisateurs de calcul intensif à l'image de Total, Airbus et Edf, qui fournissent des problèmes concrets pouvant bénéficier de l'accélération quantique,
- de ses grands groupes industriels pionniers dans l'utilisation des technologies quantiques qui insufflent un fort dynamisme à l'écosystème français à l'image de Thalès et Atos,
- de ses grands groupes industriels établis dans le domaine technologique et qui ont le potentiel à exploiter et soutenir les innovations quantiques, à l'image de SOITEC, STMicroelectronics, Air Liquide, Orano...,
- de plusieurs startups qui exploitent d'ores et déjà les technologies quantiques à l'image de Pasqal, Muquans, Quandela et VeriQloud,
- du fond de capital risque « *Quantonation* » spécialisé dans les technologies quantiques.

<sup>2</sup> Ces deux classes d'algorithmes sont aujourd'hui réputées vulnérables à la cryptanalyse quantique

## II. Jeux des technologies quantiques

### II.1 Calcul Quantique

**Enjeu 1** Diffuser, dès aujourd'hui, l'usage du calcul quantique dans les secteurs applicatifs prioritaires (chimie, logistique, intelligence artificielle, etc.) afin d'anticiper la rupture que cette technologie apportera, à terme, en matière de temps de mise sur le marché

Depuis quelques années, les machines bruitées de taille intermédiaire ou « NISQ » pour « Noisy Intermediate-Scale Quantum » et les simulateurs quantiques (machines analogiques spécialisées dans la simulation de la chimie moléculaire) exploitables commercialement sont devenues une réalité. Ces machines constituent, dès aujourd'hui, des outils d'apprentissage du calcul quantique. Se saisir, dès aujourd'hui, des outils d'apprentissage du calcul quantique, confèrera, à moyen terme, un avantage stratégique aux acteurs industriels dans plusieurs domaines : pharmacologie, matériaux avancés, fertilisants, catalyseurs, logistique, finance etc.

#### Principales applications à court terme du Calcul Quantique

##### ■ Chimie :

Le Calcul Quantique pourrait permettre la simulation quantique de la chimie moléculaire, ce qui permettrait d'élaborer des nouveaux procédés chimiques avec des gains d'efficacité substantiels : l'élaboration d'un nouveau catalyseur pour la fabrication d'engrais pourrait potentiellement permettre de réduire de 5% la consommation énergétique mondiale.

##### ■ Science des matériaux :

Le Calcul Quantique pourrait être utilisé pour analyser des interactions physico-chimiques complexes, permettant de découvrir plus rapidement des nouveaux matériaux disruptifs dans plusieurs secteurs économiques. La création de **matériaux brevetables** constitue une **source potentielle d'importants profits** pour les premiers utilisateurs finaux dans des secteurs clés.

##### ■ Médecine personnalisée :

Le Calcul Quantique pourrait être utilisé pour modéliser les réactions chimiques à l'échelle moléculaire afin prédire avec plus de précision l'**interaction protéines-médicaments**, ce qui mènerait à de **nouvelles méthodologies pharmaceutiques** qui accélèreraient la mise sur le marché de nouveaux médicaments personnalisés.

##### ■ Biologie :

Le Calcul Quantique pourrait être utilisé pour la simulation de processus tels que la photosynthèse ou pour la modélisation des systèmes énergétiques. Il permettrait d'accélérer l'élaboration de **nouveaux engrais** ou à l'amélioration des engrais existants, contribuant ainsi à améliorer les sources alimentaires mondiales.

##### ■ Optimisation et logistique

Le Calcul Quantique permettrait d'accélérer la résolution de problèmes d'optimisation complexes, notamment pour la distribution d'énergie, contrôle et re-routage du trafic, et la planification des tâches.

##### ■ Apprentissage pour l'Intelligence Artificielle :

Le Calcul Quantique pourrait accélérer considérablement l'**apprentissage à partir de modèles différentiels complexes** : aéronautique, systèmes énergétiques ...

## **Enjeu 2** Se prémunir d'une trop forte dépendance à un acteur et à une voie technologique uniques

Les experts estiment à 200 *qubits* physiques le seuil à partir duquel les machines NISQ prendront l'avantage sur les techniques de modélisation chimique traditionnelles. Or, des écosystèmes très fortement intégrés se constituent, dès aujourd'hui, autour de machines de 50 *qubits* physiques qui, bien qu'elles ne confèrent pas d'avantage quantique avéré, permettent d'anticiper les disruptions futures et fédèrent et fidélisent un écosystème de développeurs autour d'outils de développements *Hardware-dépendants* (dépendants du matériel).

L'avantage quantique désigne la situation dans laquelle l'utilisation de processeurs quantiques apporte, par rapport à une solution classique, pour une application donnée, un avantage économique en matière de coût, de temps de calcul, de consommation énergétique, etc.

Aujourd'hui, ces stratégies d'intégration verticale constituent un frein à l'adoption du calcul quantique par les secteurs aval qui appréhendent le risque d'une dépendance à une voie technologique qui n'aboutisse pas à terme. Cet enjeu s'accompagne d'une opportunité à développer des modèles prédictifs qui pourront extrapoler les résultats des différentes approches technologiques et prévoir leurs performances en avance de phase.

## **Enjeu 3** Garantir, demain, une capacité de développement et d'approvisionnement en calculateurs « LSQ »

Au-delà des machines « NISQ », les perspectives d'un ordinateur quantique corrigé en erreurs « LSQ » ou « *Large Scale Quantum* » promettent :

- un saut qualitatif de plusieurs ordres de grandeur dans les différents domaines cités plus haut ;
- des risques de compromissions sur l'ensemble des informations chiffrées aujourd'hui par cryptographie asymétrique ;
- des usages encore insoupçonnés avec la découverte de nouveaux algorithmes pouvant tirer concrètement profit de ces machines.

Compte tenu du caractère dual lié notamment aux applications de cryptanalyse permises par les machines « LSQ », le club très fermé des pays dotés de la technologie pourraient décider d'interdire l'exportation des machines les plus performantes. Une telle rétention technologique offrirait à ces pays des gains de plusieurs points de leur balance commerciale et de leur PIB, tandis que le reste du monde se trouverait sous la menace d'une compromission généralisée de ses communications avec l'obligation de déployer dans l'urgence des moyens de chiffrement plus sûrs.

La trajectoire menant aux machines « LSQ » est largement plus incertaine que pour les machines « NISQ » notamment à cause des conditions extrêmes dans lesquelles ces machines opèrent : il faut, en effet, lutter contre la tendance naturelle des objets quantiques à être perturbés par leur environnement.

Trois scénarios pourraient alors être envisagés :

- Une découverte inopinée pourrait survenir à n'importe quel moment dans des voies peu explorées, à l'instar des approches « topologiques » défendues principalement par Microsoft et Nokia ;
- Les machines « LSQ » surviennent au cours des deux prochaines décennies grâce à des avancées dans les technologies réputées « scalables » ;
- Les machines « LSQ » ne voient jamais le jour.

Les deux premiers scénarios soulèvent les mêmes enjeux de constitution d'écosystème industriel que dans le cas des NISQ, avec notamment la nécessité d'avoir des stratégies industrielles et d'approvisionnements adaptées permettant à la France de garantir ses intérêts stratégiques.

Dans l'hypothèse où les calculateurs « LSQ » ne voient jamais le jour, l'effort consenti ne serait pas vain pour autant. Les verrous levés auront créé des externalités positives irrigant plusieurs filières technologiques françaises (microélectronique, photonique, vide et froid industriels, câblage, gaz industriels etc.). A titre d'illustration, il convient de rappeler que les efforts consentis à la réalisation du Concorde ont permis à terme de développer les technologies des actuels avions de ligne d'Airbus. Le projet de fusion nucléaire ITER est une autre illustration, qui bien qu'à ce jour, pas encore opérationnel, a permis de lever des verrous dans plusieurs secteurs technologiques dont les impacts sont dès à présent palpables (e.g. électro-aimants, supraconducteurs, matériaux etc.).

Par ailleurs, la recherche sur les calculateurs quantiques a déjà eu des retombées importantes sur l'informatique classique, où les concepts et techniques développées ont permis d'inventer de nouveaux algorithmes classiques dans les domaines de la chimie, de la logistique et de l'IA, ou encore pour développer de nouveaux processeurs de calcul spécialisés, notamment dans l'optimisation combinatoire (i.e. le « *Digital Annealer* »<sup>3</sup> de Fujitsu).

Le 20 septembre 2019, le *Financial Times* affirme que Google aurait atteint la « suprématie quantique » : réalisation, en quelques minutes, d'un calcul qui aurait nécessité 10 000 ans sur un supercalculateur. Si l'information est confirmée, ce sera un grand pas vers les machines « LSQ ».

---

<sup>3</sup> « *Digital Annealer* », dont le design est « inspiré par des phénomènes quantiques » d'après ses concepteurs, est une puce de calcul classique qui se revendique comme concurrent direct de l'unité de traitement de D-Wave, et vise au même titre à résoudre des problèmes d'optimisation combinatoire.

## II.2 Capteurs Quantiques

### **Enjeu 4** S'assurer d'une capacité opérationnelle d'approvisionnement en technologies de capteurs quantiques

Les capteurs quantiques ont plusieurs applications prometteuses dans le domaine de la défense : navigation, interception, détection, sismographie...

De par leur caractère dual, ils pourraient à terme subir les mêmes contraintes à l'export que les calculateurs quantiques.

### **Principales applications de défense des capteurs quantiques**

#### ■ Navigation :

Accéléromètres, magnétomètres et gravimètres quantiques embarqués pourraient répondre à la dépendance des systèmes de navigation critiques à l'égard des signaux satellites du système GPS, qui peuvent être brouillés ou usurpés par un attaquant, rendant les systèmes de navigation inutilisables. Un avion pourrait faire un vol transocéanique et arriver à sa destination avec une précision de quelques mètres sans utiliser le signal GPS.

Les capteurs quantiques de navigation mesurent précisément les variations de certaines propriétés physiques du globe terrestre (champs électromagnétique, champs gravitationnel, etc.) pour lesquels une cartographie à très haute définition est disponible, leur permettant ainsi de se positionner précisément sans avoir recours à des éléments externes comme des satellites.

Les capteurs de navigation peuvent être basés soit sur les atomes refroidis par laser, soit sur les impuretés dans le diamant (cf. I.2).

#### ■ Interception électromagnétique :

Les capteurs à base d'impuretés dans le diamant (cf. I.2) pourraient permettre de réaliser des analyses spectrales des signaux électromagnétiques de plusieurs ordres de grandeurs plus fines que les technologies actuelles. Dans un contexte de guerre électronique et d'écoute des signaux radiofréquence, ces dispositifs pourraient multiplier les performances des systèmes d'interception.

#### ■ Télédétection :

Le radar quantique est une technologie de télédétection émergente fondée sur l'illumination quantique (cf. I.2). S'il est développé avec succès, il permettra de détecter les avions furtifs, de filtrer les tentatives délibérées de brouillage et de fonctionner dans des zones où le bruit de fond est élevé.

### **Enjeu 5** Assurer la viabilité économique à long terme des technologies de capteurs quantiques développées en France

Parmi les différentes familles de technologies quantiques, les capteurs quantiques ont la maturité technologique la plus importante, mais souffrent de difficultés à s'industrialiser dans les secteurs applicatifs civils. La complexité de leur mise en œuvre et l'environnement extrême souvent nécessaire à leur fonctionnement limitent aujourd'hui les débouchés à des marchés très spécifiques, ce qui compromet la viabilité à long terme des entreprises qui les produisent. Le secteur de la défense ne pourra pas, seul, assurer la viabilité économique des entreprises qui les développent.

Dans les applications civiles, les capteurs quantiques, même s'ils sont prometteurs de performances ou fonctionnalités accrues, se trouvent en concurrence avec des capteurs « classiques », dont les performances ne cessent de croître, de manière intrinsèque ou par la mise en réseau et les progrès en traitement des données.

## II.3 Cryptographie Quantique et Post-Quantique

### **Enjeu 6** Garantir, dans l'éventualité même lointaine de l'avènement d'un ordinateur quantique suffisamment performant, l'intégrité rétroactive sur 50 ans des communications et informations sensibles.

S'il est peu probable à court terme, l'avènement post 2030 d'une machine « LSQ », capable de déchiffrer des données protégées par des algorithmes à clé publique, n'est pas exclu. Pour faire face à ce risque, la priorité des autorités françaises consiste à garantir l'intégrité des systèmes d'informations et des communications de l'État de manière rétroactive, en :

L'ANSSI est, dès aujourd'hui, en mesure de labelliser des solutions de sécurité incluant des mécanismes de cryptographie « hybrides » combinant un mécanisme asymétrique éprouvé et un nouveau mécanisme asymétrique offrant une perspective de résistance post-quantique.

- développant et en déployant des schémas cryptographiques asymétriques, appartenant à la « cryptographie post quantique », résistant à une cryptanalyse quantique. Ces schémas de cryptographie, peuvent être ajoutés aux schémas actuels sans s'y substituer, dans un système hybride. Un tel système, combinant la sécurité d'un mécanisme actuel et d'un mécanisme post-quantique, permet de se prémunir contre tout risque de régression face la cryptanalyse classique, occasionné par l'introduction d'algorithmes nouveaux et encore incomplètement étudiés.
- déployant, dans les contextes qui s'y prêtent, des schémas de cryptographie symétrique classique avec des tailles de clés adaptées, sur lesquelles une machine « LSQ » n'a pas d'impact connu pour les communications les plus sensibles.

### **Enjeu 7** Se prémunir contre l'introduction, dans les infrastructures de communication, de composants de cryptographie quantique maîtrisés uniquement par les acteurs non européens.

Bien que la cryptographie asymétrique post quantique et la cryptographie symétrique apportent, de l'avis des autorités compétentes, des garanties *a priori* suffisantes vis-à-vis d'une cryptanalyse quantique, se désengager des voies de recherche dans les communications quantiques pourrait être périlleux.

En effet, il y a un engouement mondial pour le déploiement de la cryptographie quantique en plus des schémas post-quantiques<sup>4</sup>. Nous pourrions, dès lors, nous retrouver, de fait, avec des composants de cryptographie quantique dans les réseaux internet mondiaux. Trois scénarios peuvent, dès lors, être envisagés :

- La France développe, avec le concours d'industriels français, sa propre solution QKD opérationnelle, certifiée par l'ANSSI. Le risque de perte de souveraineté serait négligeable et les industriels impliqués pourraient avoir des débouchés intéressants à l'export pour les technologies développées.
- La France veille à ce qu'une solution QKD européenne voit le jour avec une contribution française limitée. Le risque de souveraineté, déplacé au niveau européen, demeure limité.

<sup>4</sup> La cryptanalyse quantique est un domaine relativement récent étudié par une petite communauté de chercheurs. Les primitives de cryptographie post-quantique, envisagées à ce jour, pourraient être vulnérables à des nouvelles classes d'algorithmes quantiques.



- La France se dessaisit du sujet, et des solutions développées hors Europe s'imposent comme standard de fait. Dans ce cas de figure, des composants non maîtrisés en Europe sont introduits dans les infrastructures de communications<sup>5</sup>.

---

<sup>5</sup> Ce scénario est particulièrement critique d'autant que l'actuel déploiement de la 5G illustre, dès aujourd'hui, les risques en matière de possibilités de compromission du cœur de réseau, d'une perte de savoir-faire en Europe.

## III. Verrous du développement des technologies quantiques

### III.1 Verrous technologiques

#### III.1.1 Calcul quantique

**Verrou 1** Le développement d'un ordinateur « LSQ » nécessite une technologie de fabrication de qubits à faible variabilité.

Pour un système avec un grand nombre de *qubits*, les dimensions, les qualités de surfaces, la pureté des matériaux et autres paramètres physico-chimiques devront avoir un niveau de reproductibilité suffisant pour que deux *qubits* se comportent nominale de manière identique. Les domaines de fonctionnement des *qubits* sont hors des champs habituels des technologies de production de masse. Un effort technologique non négligeable sera nécessaire pour passer à une production de *qubits* en grands volumes.

**Verrou 2** Un ordinateur « LSQ » nécessite, au-delà de l'aspect matériel, de développer des codes de correction d'erreurs performants.

À l'exception de la voie « topologique » explorée notamment par Microsoft et Nokia, les *qubits*, toutes technologies confondues, n'ont pas la capacité intrinsèque à rejeter les perturbations extérieures qui peuvent fausser les résultats des calculs. Le rejet de ces perturbations s'effectue par des algorithmes de bas niveau particuliers appelés « codes de correction d'erreurs ». L'augmentation du nombre de *qubits*, toutes technologies confondues, augmente également leur sensibilité au bruit, compliquant davantage la réalisation de codes de correction d'erreur performants<sup>6</sup>.

Conceptuellement, la correction d'erreur consiste à intriquer un nombre élevé de *qubits* physiques de sorte que la perturbation de l'un influe marginalement sur l'état des autres. La performance des codes de corrections d'erreurs se mesure par le nombre minimum de *qubits* physiques nécessaires pour créer un *qubit* logique. Le ratio dépend de la qualité des *qubits* physiques et est actuellement de plusieurs milliers. Pour une réalisation pratique d'un ordinateur « LSQ », il sera nécessaire de réduire ce ratio.

**Verrou 3** Les technologies de qubits les plus performantes passent difficilement à l'échelle et les technologies les plus évolutives affichent des niveaux de bruit trop élevés pour permettre une implémentation efficace des codes de correction d'erreurs.

Pour autant, la réalisation de ordinateurs « LSQ » continuera à nécessiter un nombre important de *qubits* physiques, ce qui suppose une capacité à les fabriquer par des processus industriels existants ou de créer des nouveaux outils industriels qu'il faudra amortir. Or, les voies technologiques capables de passer à l'échelle grâce à un outil industriel déjà amorti, à l'image du Silicium, souffrent d'un faible niveau de maturité car elles ont démarré plus tard que les approches qui pouvaient être explorées avec des techniques de laboratoires. À ce jour, cette voie affiche des niveaux de bruits trop élevés (~0.1%) pour une implémentation efficace des codes de correction d'erreurs. Idéalement, il faudrait améliorer le niveau de bruit pour atteindre 0.01%. Les voies technologiques les plus avancées, à l'instar de la supraconduction, souffrent elles aussi d'un niveau de bruit élevé et semblent peiner à passer à l'échelle au-delà de quelques dizaines de *qubits*.

<sup>6</sup> INRIA est l'un des spécialistes mondiaux de la correction d'erreurs.

#### **Verrou 4 Plus une technologie de qubits est robuste aux perturbations externes, plus il est difficile de créer des portes logiques et réciproquement.**

Un autre verrou à la réalisation de machines « LSQ » réside dans le fait que la sensibilité aux perturbations externes et la qualité des portes logiques sont en réalité **deux manifestations du phénomène d'intrication** (cf. I.1) qui caractérise la capacité d'un *qubit* à interagir avec son voisin. L'amélioration de la qualité des portes logiques s'accompagne systématiquement d'une détérioration du rejet des perturbations externes et vice-versa. Il y a donc un compromis à trouver entre vitesse de manipulation et durée de préservation de l'information quantique.

A ce jour, seule la voie technologique des *qubits* topologiques revendique la capacité de s'affranchir du problème de bruit.

La faisabilité des *qubits* topologiques n'est, à ce jour, pas démontrée.

Ce verrou, connu sous le nom de « décohérence », est généralement peu abordé par les communications marketing des entreprises technologiques qui n'annoncent que le nombre de *qubits*, plus élogieux, sans aborder le sujet de la qualité de ces *qubits* : leur sensibilité au bruit comparativement à la qualité de leurs portes logiques. La levée de ce verrou nécessitera des travaux sur l'amélioration compromis entre capacité de manipulation du *qubit* et décohérence, afin d'augmenter le nombre d'opérations pouvant être réalisées avant que l'information quantique ne soit perdue.

#### **Verrou 5 L'absence de protocole connu permettant un transfert efficace de données massives vers un ordinateur quantique freine la percée des accélérateurs quantiques, y compris NISQ, dans le domaine du Calcul Haute Performance (HPC).**

Bien qu'un ordinateur quantique tire sa puissance de sa capacité à utiliser un petit nombre de *qubits* pour représenter une quantité exponentiellement plus grande de données, il n'existe actuellement pas de méthode connue pour transcrire efficacement un large jeu de données classiques en un seul état quantique.

Il en résulte que pour les problèmes qui nécessitent de grandes quantités de données en entrée, le temps nécessaire à l'initialisation du ordinateur quantique devient prépondérant sur le temps de calcul, réduisant ainsi l'avantage quantique. Cette limite ouvre la voie à des innovations en termes de protocoles et d'interfaces entre le logiciel et l'implémentation matérielle.

#### **Verrou 6 Le manque d'outils de développement et de standards de programmation performants et interopérables freine l'adoption par les secteurs applicatifs.**

L'algorithmie quantique constitue un changement de paradigme de programmation important par rapport à l'algorithmie classique. En effet, les propriétés de « non clonage » des états quantiques interdisent toute possibilité de lire plus d'une fois l'information quantique, sans oublier que l'information quantique « s'écroule » dans un état classique dès la lecture. À cause de cette propriété, des opérations classiques de base telles que les « boucles d'itération », les « résultats intermédiaires », les « copies », les « points d'arrêts », ou encore les « exécutions pas à pas » n'ont plus de sens en algorithmie quantique.

L'exploitation de la puissance du calcul quantique nécessitera, dès lors, de repenser les paradigmes et méthodes de développements algorithmiques. Des nouvelles piles logicielles, langages de programmation, et environnements de développement devront être développés. Plusieurs initiatives commencent à aborder ce sujet à l'instar de

l'environnement d'émulation quantique d'Atos **QLM** basé sur le langage **AQASM** ou de l'intégration du langage **Q#** à **Visual Studio** par Microsoft.

**D'une manière générale, la levée des différents verrous liés au calcul quantique nécessitera le concours de plusieurs domaines de compétences à l'instar de l'informatique théorique, la physique quantique, l'ingénierie système, l'ingénierie des procédés, les matériaux et le contrôle-commande.**

### III.1.2 Capteurs quantiques

**Verrou 7** Les capteurs quantiques doivent être intégrés dans des systèmes où leur plus-value par rapport aux capteurs classiques est tangible.

De par leur maturité, les principaux verrous d'ordre technologique liés aux capteurs quantiques en tant que composants ont été levés. Les verrous technologiques résiduels se situent au niveau de l'intégration dans des systèmes existants en vue de remplir une fonction métrologique : remplacer un jeu d'antennes par un seul capteur à base d'impuretés dans le diamant pour des besoins de détection électromagnétique, développer un système de géolocalisation sans GPS à base de capteurs à atomes froids etc.

### III.1.3 Cryptographie Quantique et Post-Quantique

#### III.1.3.1 Cryptographie Post-Quantique

Traditionnellement, la confiance dans les schémas cryptographiques s'accroît avec le temps : moins il y a d'attaques contre un schéma, plus la confiance qui lui est accordée est grande. Certains schémas post-quantiques, existant depuis un certain temps, sont bien acceptés et considérés comme suffisamment mûrs pour être déployés.

**Verrou 8** En l'absence d'ordinateurs quantiques suffisamment puissants, la confiance dans les schémas post-quantiques ne peut être établie que sur la base d'un modèle théorique de l'ordinateur quantique.

Les algorithmes post-quantiques nécessitent également d'être évalués au regard d'une attaque utilisant des ordinateurs quantiques. Or, il n'y a, à ce jour, pas d'ordinateur quantique suffisamment puissant pour une analyse pratique de la cryptanalyse quantique. Par conséquent, les estimations sur la sécurité des systèmes post-quantiques vis à vis des calculateurs quantiques sont purement théoriques ce qui occasionne deux problèmes :

- si la puissance des ordinateurs quantiques est sous-estimée, les mesures de sécurité choisies risquent d'être trop faibles et les schémas seront brisés avec l'apparition d'ordinateurs quantiques suffisamment puissants ;
- si la puissance des ordinateurs quantiques est surestimée, les mesures de sécurité choisies seront également surestimées, ce qui entravera leur efficacité et leur déploiement à grande échelle.

**Verrou 9** Les algorithmes de cryptographie post-quantique en cours d'évaluation augmentent d'un ou plusieurs ordres de grandeur les ressources en temps et en stockage nécessaires par rapport aux algorithmes actuels.

Les algorithmes post-quantiques actuellement envisagés exploitent généralement des clés au moins 10 fois plus longues que leurs équivalents actuels. Cette taille plus importante

s'accompagne d'un temps de calcul plus important, ainsi que par des besoins en mémoire plus élevés pour les dispositifs qui les mettent en œuvre. Ces changements posent relativement peu de difficultés pour les dispositifs disposant d'une puissance de calcul et d'une quantité de mémoire importantes comme des smartphones ou des ordinateurs de bureau. Pour les dispositifs à ressources limitées, à l'instar des cartes à puces, des circuits spécialisés visant à accélérer de façon sécurisée les calculs liés à ces nouveaux algorithmes devront être développés. Ce travail pourra débuter lorsque les algorithmes standardisés seront connus ou fortement pressentis. Plusieurs travaux académiques, en cours, visent à développer les briques de calcul nécessaires à certains des algorithmes pressentis.

**Verrou 10** Le déploiement effectif de nouveaux systèmes de cryptographie, et donc d'algorithmes post-quantiques, sera un processus lent.

Le déploiement d'algorithmes post-quantiques en remplacement des algorithmes asymétriques actuels sera un processus lent si l'on se fie à ce qui a pu être observé dans le passé pour le déploiement des algorithmes asymétriques actuels. Une décennie sera probablement nécessaire pour une bonne pénétration de ces algorithmes. De façon générale, les applications nécessitant une implémentation matérielle ou semi-matérielle des algorithmes évoluent sur des temps plus longs. Ces estimations de délais dépendent de la pression qui s'exercera sur l'évolution. En cas de vulnérabilité avérée des algorithmes actuels en raison du développement d'algorithmes de cryptanalyse quantique, le déploiement d'algorithmes post-quantiques pourrait être nettement accéléré.

### III.1.3.2 Cryptographie Quantique

Avant qu'une généralisation de la QKD ne soit envisageable, plusieurs défis doivent être relevés :

- **La distance** : la perte de photons et le bruit limitent la distance de transmission. Dépasser ces limites nécessite des relais classiques de confiance induisant des problèmes de sécurité à cause de l'information non protégée qui y circule, des relais quantiques qui nécessitent des mémoires quantiques, et des satellites, avec le coût associé.
- **L'intégration aux infrastructures de télécommunications** : la QKD nécessite, généralement, le déploiement d'infrastructures dédiées ce qui limite son adoption, là où la cryptographie post-quantique se satisfait des infrastructures existantes. La QKD à variables continues, technologie inventée en France, a l'avantage de pouvoir mieux réutiliser des équipements de télécommunications terrestres existants, et donc de pouvoir être déployée plus facilement. Cependant, elle souffre à ce stade d'une plus forte sensibilité aux pertes.

**Verrou 11** Les principales technologies QKD nécessitent un déploiement d'infrastructures spécifiques dont le coût est élevé comparativement au service rendu.

- **La confiance dans la solution cryptographique** : pour être adoptée en pratique, une solution QKD doit apporter des garanties de cyber-sécurité pour une cible de sécurité donnée. La maturité de la QKD étant faible vis-à-vis des catégories de menaces comme les canaux auxiliaires ou les attaques par déni de service (DoS), il sera nécessaire de concevoir des contre-mesures adéquates à ce type d'attaques, avant d'envisager un éventuel usage pour manipuler des informations sensibles. Les contre-mesures utilisées pour les communications classiques, basées en majorité sur des mécanismes de redondance, ne sont pas applicables en l'état, en raison des contraintes de non-clonage des états quantiques.

Une attaque par canal auxiliaire désigne une attaque qui exploite des failles dans l'implémentation d'une méthode de sécurité grâce à une analyse électromagnétique, de la consommation, temporelle, acoustique etc. Une attaque DoS vise à empêcher l'utilisation légitime d'un service, en le saturant de requêtes illégitimes.

**Verrou 12** La QKD manque aujourd'hui de maturité sur le plan de la cyber-sécurité, notamment au regard des relais de confiance et des attaques par canal auxiliaire et par déni de service.

Ces différents axes de développement constituent l'ossature d'une éventuelle certification d'un système QKD permettant son emploi pour manipuler des informations sensibles.

### III.1.4 Technologies habilitantes

**Verrou 13** Les capteurs et les calculateurs quantiques, nécessitent des équipements de servitude complexes, encombrants et aux facteurs de formes peu favorables à une intégration système

Les technologies habilitantes sont des composants non quantiques mais indispensables au bon fonctionnement des capteurs et calculateurs quantiques : cryostats, lasers, ultravide, etc.

L'un des principaux verrous liés à ces technologies réside dans leur encombrement et leur facteur de forme.



Figure 3: cryostat 70°K

Ainsi, si un cryostat à 70 °K tel que développé pour les imageurs infrarouges tient aujourd'hui dans la paume d'une main (cf. Figure 3), cette prouesse n'a pu se concrétiser que grâce à un effort de recherche et développement conséquent de la part des industriels.

Alors qu'un capteur ou un processeur quantique tient dans moins d'un cm<sup>3</sup>, l'électronique de commande et le système de refroidissement capable d'atteindre des températures de quelques milli Kelvins occupent, à ce jour, pas moins de dix mètre cube incluant réfrigérateurs à dilution, baie de commande et accessoires (cf. Figure 4).

Par ailleurs, ces machines cryogéniques, pensées pour des usages génériques en laboratoire, ne permettent, à ce jour, pas une intégration des dispositifs quantiques dans leur environnement système. Le développement technologique doit permettre d'améliorer l'intégration du système et l'optimisation des espaces alloués.



Figure 4: cryostat à dilution

Ainsi, en ce qui concerne les capteurs, les systèmes de commande et de refroidissements devront gagner en compacité avant que ces dispositifs puissent se diffuser largement.

En ce qui concerne les calculateurs quantiques, l'effort de R&D en matière de technologies habilitantes devra aborder à la fois la compacité ainsi que le facteur de forme. Les cryostats cylindriques d'un mètre cube auront du mal à s'intégrer, en l'état, dans un centre de calcul d'une manière *plug-and-play* à l'image des lames d'accélération à base de GPU ou NPU.

Une collaboration étroite entre les secteurs de cryogénie, de l'ultravide et les développeurs de technologies quantiques sera nécessaire pour lever ces verrous.

## III.2 Verrous non technologiques

### III.2.1 Coordination et efficacité de l'écosystème

**Verrou 14** Le fonctionnement en silos des différentes communautés de physiciens, d'algorithmiciens, d'ingénieurs, de cryptographes, et d'utilisateurs finaux limite les percées majeures et les levées de verrous à fort impact en informatique quantique.

Des avancées majeures en matière de capteurs quantiques ont pu être réalisées par le seul effort de la communauté de physiciens, sujet significativement moins complexe que le calcul et les communications.

Concernant le calcul quantique et les communications quantiques, le fonctionnement en silos est beaucoup plus préjudiciable à la levée de verrous à fort impact, dans la mesure où ces technologies sont beaucoup plus complexes et pluridisciplinaires. Plusieurs biais expliquent ces fonctionnements en silos.

Ainsi, en matière de calcul quantique, la communauté de physiciens, motivée principalement par la compréhension fine des phénomènes physiques, a tendance à être sceptique quant aux avancées technologiques possibles tant que cette compréhension n'est pas pleine et entière. Or, le progrès technique a généralement précédé la compréhension fine des lois de la nature. L'humain a créé les premiers alliages cinq millénaires avant la compréhension des sciences des matériaux, et la machine à vapeur un siècle avant la compréhension fine des lois de la thermodynamique.

Les communautés d'informaticiens et d'électroniciens, généralement dotées d'une culture technique forte, ont tendance à minimiser certaines difficultés conceptuelles et fondamentales. Il est ainsi observé que certains modèles sont simplifiés à l'extrême et se heurtent, lors des réalisations pratiques, à des verrous physiques non pris en compte initialement.

Un second biais réside dans une tendance générale à privilégier les démarches techno-push, et à envisager les usages en dernier. Si cette démarche est pertinente lorsque les usages finaux sont diversifiés, dans le cas du calcul quantique, qui vise des secteurs précis, l'association des usagers finaux dès le départ est indispensable. De ces usages pourront découler les bonnes architectures de calcul, et les bons compromis sur les performances techniques des qubits.

En matière de cryptographie quantique, la communauté de physiciens a tendance à s'intéresser davantage à la réalisation d'une tâche de communication quantique qu'à la réalisation d'une fonction de cryptographie avec preuve de sécurité. Ce biais est naturel, dans la mesure où les chercheurs dans ce domaine sont davantage stimulés intellectuellement par la découverte et l'expérimentation scientifique que par la réalisation de dispositifs clé en main qui relève davantage de l'ingénierie.

Enfin, la communauté cryptographique, plus impliquée dans l'ingénierie des dispositifs de sécurité, exprime, pour sa part, un certain scepticisme quant à l'apport réel des communications quantiques en matière de sécurité. Si ce scepticisme est basé sur des raisons légitimes liées aux vulnérabilités d'implémentation non traitées par la communauté physique, le manque d'échange entre ces deux communautés a été exacerbé dans les dernières années par les promesses de « sécurité absolue » des communications quantiques clamées il y a quelques années d'un côté, et de son « inutilité pratique » de l'autre. Les ruptures technologiques en matière de communication quantique nécessiteront indéniablement le concours des deux communautés.



### III.2.2 Développement des compétences

**Verrou 15** L'augmentation du nombre d'ingénieurs, de startups et sociétés de conseil familiarisés avec la logique et le processus de développement en informatique quantique est une condition nécessaire à la diffusion du calcul quantique dans les secteurs applicatifs.

Conscientes des ruptures liées à l'informatique quantique, plusieurs entreprises de différents secteurs applicatifs commencent à explorer l'apport de cette technologie pour leur secteur. Elles se heurtent néanmoins à un manque de compétences de pointe sur le marché de l'emploi. Ce constat concerne aussi bien les ingénieurs, diplômés de masters ou docteurs en sortie de formation supérieure que les startups logicielles et sociétés de conseil.

Contrairement à d'autres technologies à l'image de l'intelligence artificielle, le nombre d'algorithmiciens et développeurs familiers avec la logique quantique ne dépasse pas quelques dizaines à l'échelle du pays.

La constitution d'un écosystème de développeurs en informatique quantique est une attente forte des industriels. Une montée en compétences des développeurs dans le domaine de l'informatique quantique est devenue une condition nécessaire à la diffusion de l'informatique quantique dans les secteurs applicatifs.

### III.2.3 Taille de marché et cycles de Hype

**Verrou 16** Le maintien d'un « cash-flow » Public-Privé de long-terme à destination des entreprises impliquées dans le développement des technologies quantiques est une condition nécessaire au dépassement d'une « vallée de la mort » qui pourrait durer près de dix ans.

La courbe d'apprentissage dans le domaine des technologies quantiques sera particulièrement lente et nécessitera, de ce fait, de nombreux redéploiements technologiques successifs et des réinvestissements importants de la part des secteurs technologiques. Au niveau des secteurs aval, le marché sera également lent à se développer par la pénurie de spécialistes des technologies quantiques au sein du marché actuel de l'emploi. La confiance des décideurs sera, dès lors, lente à atteindre à cause des innombrables aléas rencontrés (cf. Figure 5).

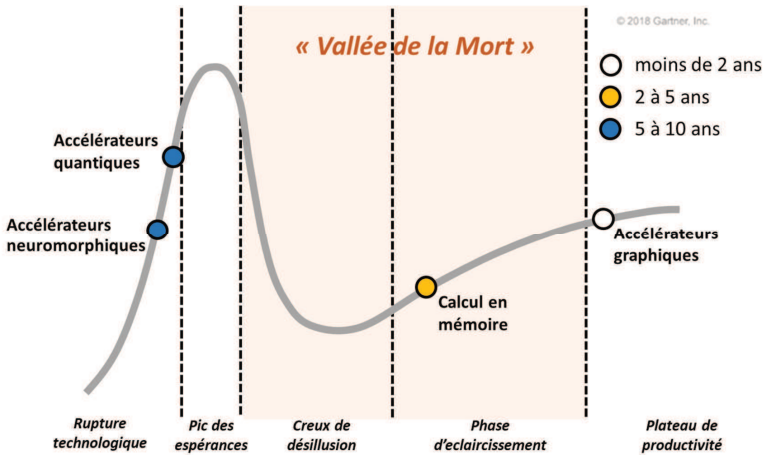


Figure 5: Cycle de "Hype" des technologies de calcul –crédit Gartner

Il conviendra, donc, au même titre que ce qui est pratiqué par les plus grands acteurs mondiaux, d'assurer la viabilité de nos acteurs naissants par un flux de commandes suffisant et à la continuité et visibilité appropriées. Ce flux de commande pourra se faire soit dans le cadre des différentes initiatives européennes en matière de souveraineté numérique, soit sous l'angle des impératifs de souveraineté voire de sécurité nationale.

Enfin, ce flux de commande constituera un levier important en vue de rassurer les investisseurs en capital dont la contribution à la viabilité des acteurs naissants est incontournable, dans la mesure où ces acteurs pourraient, tout en gagnant des parts de marché importantes, ne pas dégager de bénéfice lors des cinq à dix prochaines années.

## IV. Ambitions de la France en matière de technologies quantiques

### IV.1 Calcul Quantique

#### IV.1.1 Devenir l'un des leaders mondiaux en matière de calculateurs « LSQ »

Sur le plan des machines « LSQ », la technologie Silicium jouit d'une capacité de passage à l'échelle supérieure à celle des autres voies technologiques, notamment grâce aux milliards d'euros investis dans le monde sur les capacités de productions industrielles, mais affiche à ce jour, des niveaux de performances plus bas.

**Ambition 1** Créer, avant 2025, la première entreprise *fabless*/hybride européenne proposant des processeurs quantiques à base de Silicium.

La France est l'un des rares pays à l'échelle mondiale disposant, grâce au CNRS-Institut Néel, au CEA-LETI, au CEA-IRIG et à STMicroelectronics, d'un socle de compétences en recherche amont et technologique, ainsi que de l'outil industriel permettant d'explorer sérieusement la voie Silicium. En effet, la réalisation de *qubits* Silicium se satisfait d'une finesse de gravure de 28 nm, ce qui laisse envisager une production à terme sur le site industriel de STMicroelectronics à Crolles.

Néanmoins, les processeurs quantiques resteront au niveau mondial un marché de relativement faible volume, comparable à celui du calcul intensif nécessitant le développement de modèles d'affaires adaptés.

Aussi, une option à privilégier pour permettre le développement d'une filière industrielle nationale est la création d'une entreprise (*NewCo*) capable de porter les développements technologiques vers le marché par une approche *fabless* à l'image de Nvidia ou hybride à l'image de Lynred (ex Sofradir).

Quel que soit le modèle d'affaire retenu, la *NewCo* devra fournir un kit de développement logiciel incluant un jeu d'instructions de base et un compilateur de très bonne qualité. En effet, la diffusion des CPU et GPU d'Intel et de Nvidia ne serait pas celle qu'on connaît aujourd'hui sans les jeux d'instructions X86 et CUDA associés et la communauté de développeurs qui va avec.

#### IV.1.2 Devenir le leader européen en matière de calculateurs « NISQ »

Sur le plan des machines « NISQ » et des simulateurs quantiques, les premières machines commencent à voir le jour depuis deux ans. Faisant abstraction des problématiques de passage à l'échelle, plusieurs voies technologiques cohabitent actuellement dans les offres disponibles : supraconducteurs, ions piégés, atomes froids, photonique etc.

La France dispose d'une masse critique de chercheurs (CNRS et Institut d'Optique) et d'un soutien des syndicats de filières dans le domaine de la photonique et des atomes froids. L'effort de recherche des dernières années, a permis, entre autres, d'essaimer la première startup française de simulation quantique : Pasqal. Au niveau Européen, l'Autriche dispose d'une avance technologique substantielle dans le domaine des ions piégés, une autre voie prometteuse qu'elle explore avec Atos dans le cadre d'un projet *flagship* européen.

## **Ambition 2** Développer et diffuser la première offre commerciale européenne d'accélération quantique pour le marché du calcul intensif.

En capitalisant sur l'expertise d'Atos en matière de conception et d'intégration de supercalculateurs, la France pourrait devenir le premier fournisseur de « lames de calcul quantiques » à destination du marché du calcul intensif. Ces lames de calcul pourront incorporer les émulateurs et accélérateurs quantiques disponibles ou en développement en France et en Europe (atomes froids, ion piégés, supraconducteurs, silicium, etc.).

### **IV.1.3** Devenir l'un des leaders mondiaux en matière de logiciels métiers

Alors que l'offre technologique en calcul quantique est aujourd'hui dominée par les américains, les principaux groupes intéressés par l'usage du calcul quantique sont européens. Il serait souhaitable dans ces conditions de se réappropriier la valeur au niveau européen. Devenir un leader mondial du calcul quantique repose, en plus du développement matériel, sur la capacité à identifier des applications industrielles percutantes où le matériel à disposition apporte un « avantage quantique » tangible.

L'identification de ces applications nécessite un grand nombre d'autres briques technologiques (cf. Figure 6), notamment des cas d'usage pertinents, des algorithmes performants et robustes, des piles logicielles optimisées, une bonne intégration aux systèmes du calcul intensif classique, une décomposition optimale des problèmes pour une exécution efficace sur les accélérateurs quantiques NISQ, des compilateurs et des codes de correction d'erreurs performants, etc.

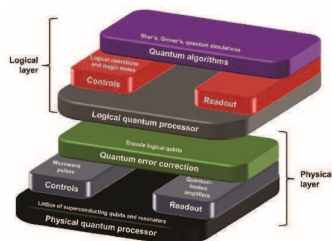


Figure 6: Briques technologiques du calcul quantique

## **Ambition 3** Proposer, en 2023, avec le concours d'autres partenaires européens, la première offre logicielle métier « clé en main », bénéficiant de l'accélération quantique, pour les domaines de la chimie, la pharmacologie, la logistique et l'apprentissage en IA.

Partant du principe que le calcul quantique ne résout efficacement qu'une catégorie spécifique de problèmes, la France pourrait capitaliser sur son savoir-faire en développement de logiciels métiers pour développer, avec le concours de ses partenaires européens notamment allemands, une offre logicielle métier bénéficiant de l'accélération quantique dédiée aux domaines de la modélisation chimique, de la logistique et de l'apprentissage en IA. Cette offre inclurait les couches d'abstractions matérielles (codes de corrections d'erreur, langages assembleurs, et compilateurs), les environnements de développements et les langages de programmation dédiés aux domaines identifiés.

Pour développer une telle offre, la France pourra capitaliser sur :

- les développements passés d'Atos en matière de langages de programmation bas-niveau interopérables (kit logiciel AQASM) et d'intégration du calcul quantique dans un environnement HPC (émulateur d'ordinateur quantique « Quantum Learning Machine »),
- les savoir-faire et la capacité d'accès au marché d'INRIA en matière de piles logicielles et d'IA<sup>7</sup>,

<sup>7</sup> En IA, la librairie SciKitLearn développé par l'INRIA occupe la 3<sup>ème</sup> place en nombre d'utilisateurs dans le monde.

- les compétences du CNRS en matière d'algorithmie quantique,
- les compétences du CEA-LIST en matière d'architectures logicielles et systèmes,
- les savoir-faire et la capacité d'accès au marché de Dassault Système en matière de logiciels de modélisation chimique et de l'allemand SAP en matière de logiciels de modélisation logistique,
- les spécifications métier des end-users français et européens à l'image de TOTAL, Airbus, Dassault Aviation, EDF, SANOFI, BASF, BAYER et BOSCH.

## IV.2 Capteurs Quantiques et Technologies Habilitantes

### IV.2.1 Jouir d'une large autonomie industrielle sur les technologies habilitantes

**Ambition 4** Faire émerger, en 2025, au moins deux acteurs industriels européens de rang mondial, dont au moins un français, pour chacune des technologies habilitantes critiques : cryogénie, ultravide et lasers.

En matière de lasers, la France dispose d'un historique industriel important et compte plusieurs laseristes de rang mondial fournissant les intégrateurs nationaux et européens<sup>8</sup>.

En matière de cryogénie et d'ultravide, la France dispose également de plusieurs atouts pour devenir un acteur mondial du domaine. La présence d'acteurs institutionnels et industriels de la cryogénie et de l'ultravide à l'image de l'IRIG, l'institut Néel, *CryoConcept*, *MyCryoFirm*, *Absolute System*, *Thales* et *AirLiquide* contribue à la levée des verrous liés à l'intégration des systèmes de cryogénie dans leur environnement tel qu'abordé au chapitre précédent.

### IV.2.2 Jouir d'une large autonomie industrielle dans les capteurs à base d'impuretés dans le diamant

Les capteurs à base d'impuretés dans le diamant sont l'une des technologies de capteurs quantiques les plus prometteuses car elle permet d'entrevoir des applications concrètes à court et moyen terme. Il existe un effort très important dans ce domaine au niveau mondial (US, Chine, UE, Australie, etc.). La France bénéficie d'atouts importants en matière de capteurs à base d'impuretés dans le diamant mais déploie des moyens plus modestes par rapport à ses principaux concurrents mondiaux.

A titre d'exemple, Thales mène des travaux de R&D visant à explorer le potentiel de cette nouvelle technologie de capteurs et à identifier l'opportunité de l'intégrer dans les futurs systèmes Thales.

**Ambition 5** Devenir un fournisseur mondial de premier plan de diamants pour les capteurs à base d'impuretés dans le diamant, à horizon 2026.

En France, il existe des capacités de productions au niveau académique (CEA-LIST, LSPM etc.) qui suffisent pour les travaux à un stade de recherche, mais ne permettent pas de répondre en l'état aux demandes industrielles.

Un soutien à cette filière permettrait de renforcer et de développer les applications qui en découleront. Il pourrait, ainsi, être envisagé de profiter du repositionnement en cours de la société *Element Six*, pour structurer une filière industrielle française des capteurs à base d'impuretés dans le diamant, notamment en matière de fabrication de diamants de grande qualité.

Pour mettre en place une telle filière, la France pourra bénéficier, en plus de Thales, de l'expertise de ses laboratoires publics.

---

<sup>8</sup> En matière de lasers, le risque se situe au niveau de protection des laseristes français par rapport à une OPA hostile.

## IV.3 Cryptographie Quantique et Post-Quantique

### IV.3.1 Maintenir une indépendance stratégique sur les technologies de cryptographie post-quantique

**Ambition 6** Proposer, en 2022, la première offre de cryptographie post-quantique pour dispositifs de sécurité de haute performance et à ressources de calcul limitées.

La France est l'un des acteurs industriels mondiaux de la cyber-sécurité, notamment en matière de dispositifs de sécurité tel que les modules HSM<sup>9</sup> et cartes à puces. En développant ses propres produits de cryptographie post-quantique et en les diffusant grâce à ses capacités d'accès aux marchés existantes et une stratégie de normalisation appropriée, la France confirmera sa position de leader mondial de cyber-sécurité.

Pour développer son offre, la France pourra bénéficier des savoir-faire techniques et commerciaux de ses grands groupes et startups à l'instar de Thales, Atos, Orange, *Secure-IC* et *CryptoNext*.

Maintenir une indépendance stratégique sur les technologies de cryptographie quantique

**Ambition 7** Proposer, en 2024, la première solution QKD européenne, déployable à coût d'infrastructures marginal et résistante aux attaques par canaux auxiliaires et par déni de service.

Sur le plan des communications quantiques, la France dispose d'un tissu de recherche spécialisé en communications quantiques à variables continues et à variables discrètes qui sont deux voies technologiques qui laissent envisager un déploiement à coût d'infrastructures marginal. À plus long terme, les solutions QKD à base de variables hybrides, pour lesquelles la France compte parmi les pays pionniers, devrait permettre d'exploiter le meilleur des deux approches.

En capitalisant, par ailleurs, sur son expertise en cyber-sécurité, la France pourrait prendre le leadership européen sur le développement de solutions de QKD robustes du point de vue de la cyber-sécurité, et ne nécessitant pas de lourds investissements d'infrastructures.

---

<sup>9</sup> Un module HSM ou « *Hardware Security Module* » est un dispositif électronique, réputé inviolable, visant à générer, stocker et protéger des clés cryptographiques.

## V. Recommandations de la mission pour une stratégie nationale

### V.1 Une infrastructure de pointe pour la recherche et l'industrie

#### V.1.1 Calcul Quantique

**Proposition 1** Héberger, au « Très Grand Centre de Calcul » (TGCC), une plateforme de Calcul Quantique diversifiée, évolutive et accessible aux communautés de chercheurs et développeurs académiques et industriels.

A travers une vision de convergence entre le calcul quantique et le HPC, la France pourrait héberger au TGCC, principal centre de calcul public français, la première infrastructure au monde d'accélérateurs quantiques intégrés d'un point de vue logiciel à un système de supercalculateurs classique. La mise en place, sur le sol français, d'une infrastructure de rang mondial, intégrant différents émulateurs et accélérateurs quantiques basés sur des principes technologiques divers, représentera un levier d'action fort permettant de répondre à plusieurs enjeux, verrous et ambitions abordés dans les chapitres précédents :

- **Développer l'écosystème logiciel et les usages** : L'émulation créée par la mise à disposition de cette plateforme auprès d'une communauté de chercheurs et d'utilisateurs industriels pionniers à l'image de Total ou Airbus permettra de constituer un écosystème de développeurs familiarisés avec la logique quantique et indépendants d'une implémentation matérielle particulière, ce qui répond à une attente forte des industriels usagers. Une dynamique de création de startups et de services de conseil tirant profit de la plateforme du TGCC pourra voir le jour, à l'instar ce qui est observé dans d'autres pays, notamment le Canada et le Royaume-Uni ;
- **Développer la légitimité et le rayonnement de la France à l'international** : La diversité des plateformes matérielles constitue un argument *marketing* fort pour attirer sur le sol français des sommités mondiales du calcul quantique. Les capacités de test, d'expérimentation et de comparaison entre les différentes voies technologiques permises par cette infrastructure contribueront à donner à la France, la légitimité d'un leadership sur le développement d'une suite logicielle quantique « *hardware-agnostique* » ;

Des rapprochements entre le TGCC et le centre de calcul allemand *Jülich* pourraient permettre de développer une offre commune et un portail commun permettant l'accès à l'ensemble des technologies de calcul quantique européennes.

**Proposition 2** Ouvrir un appel à contributions permanent à destination des startups et laboratoires français et européens développant des processeurs d'accélération quantique en vue d'une intégration à l'infrastructure de calcul.

Afin de maintenir sa légitimité et son attractivité, l'infrastructure doit se maintenir au niveau le plus élevé de l'état de l'art mondial et devra, de ce fait, renouveler ses équipements de manière à bénéficier des accélérateurs quantiques les plus avancés (plus de *qubits*, plus d'opérations, moins de bruit etc.).



Pour ce faire, elle pourra ouvrir un appel à contribution à destination des startups, laboratoires et consortiums français et européens développant des processeurs et émulateurs quantiques : *Atos, Pasqal, AQT Innsbruck, CEA, CNRS, OpenSuperQ* etc. L'opportunité d'ouvrir l'infrastructure à des fournisseurs hors Europe pourra également être étudiée.

Une intégration, à l'infrastructure de calcul, de lames de calcul quantique développées par les différentes startups ne nécessitera pas une maturité technologique élevée<sup>10</sup> et pourra être envisagée à partir d'une preuve de concept (TRL4) de 5 *qubits* et d'une feuille de route de montée en performance validée par un comité d'experts.

Au même titre que pour le HPC, la gestion de l'achat et du renouvellement des lames d'accélérateurs quantiques pourra être confiée à la société civile GENCI.

### **Proposition 3** Développer une offre public-privé de QCaaS ou « Quantum Computing as a Service » compétitive.

Afin de sécuriser leurs investissements, la majorité des usagers finaux privilégient, tel que préconisé par les cabinets de conseil *Gartner* et *McKinsey*, l'utilisation de ressources de calcul quantique en mode SAAS ou « *Software As A Service* » à l'investissement dans une infrastructure propre. La singularité de l'infrastructure proposée devrait s'accompagner d'une offre de service adaptée destinée à la fois au monde de la recherche et de l'entreprise.

Cette offre serait constituée d'un accès partagé aux ressources de calcul et d'un service d'accompagnement à l'expérimentation.

Deux niveaux d'accompagnement pourraient être proposés :

- Un niveau d'accompagnement de base à destination des nouveaux utilisateurs qui souhaitent découvrir les bases du calcul quantique ;
- Un niveau d'accompagnement avancé à destination des utilisateurs avertis cherchant une expertise pointue pour un sujet précis.

La mise en place de cette offre QCaaS, qui en première estimation pourra nécessiter une dizaine d'ingénieurs à temps plein compte tenu du nombre d'utilisateurs visés, ainsi que la définition d'un business model viable pourra être confié à des acteurs tels que *Teratec, Airbus, Atos* et *INRIA* qui ont de l'expérience dans l'animation d'écosystème HPC et des offres SaaS. Un Appel à Manifestation d'Intérêt (AMI) pourra être lancé par l'État afin de développer cette offre QCaaS.

## V.1.2 Communications quantiques

### **Proposition 4** Déployer une plateforme de test pour différents dispositifs de communications quantiques.

Afin de lever les verrous technologiques relatifs à la cryptographie quantique, les chercheurs académiques et industriels auront besoin d'une infrastructure d'expérimentations permettant de valider leurs différents dispositifs. En pratique, il s'agit de disposer d'un moyen de communication par fibre optique sur de longues distances où les chercheurs pourront

---

<sup>10</sup> L'accès aux infrastructures de calcul se fait à travers un accès Cloud. La faible maturité d'un accélérateur quantique se traduira principalement par un coût de maintenance plus élevé et une fonction de disponibilité potentiellement plus réduite. L'indisponibilité pour maintenance est observée dans les offres commerciales de calcul quantique à l'instar de l'IBM-Q.

tester différents dispositifs, y compris des systèmes à variables continues et discrètes, les relais classiques et quantiques ou éventuellement l'interopérabilité avec des liens satellite. Il pourrait être envisagé d'exploiter l'infrastructure de fibres optiques du réseau RENATER reliant Paris à Saclay, ou de faire appel à un opérateur de télécommunications pour déployer des nouvelles fibres optiques à mettre à la disposition des équipes de recherche selon un modèle d'affaires à déterminer.

Cette infrastructure, ainsi que les infrastructures présentes entre Nice et Sophia-Antipolis permettront, par ailleurs, aux chercheurs français de participer plus efficacement à différentes initiatives européennes à l'image du projet OpenQKD ou de l'initiative EuroQCI.

L'étude de l'opportunité d'investir dans un déploiement d'une infrastructure de communications quantiques de plus grande envergure sera conditionnée par la levée des verrous technologiques relatifs à l'utilisation de la QKD (cf. Verrou 11 et Verrou 12) pour manipuler les informations sensibles. L'intérêt d'un déploiement d'infrastructures plus large pourra être étudié par les autorités à l'issue de la levée de ces verrous.

## V.2 Un programme de soutien au développement technologique

### V.2.1 Soutien transversal à l'ensemble des technologies quantiques

#### V.2.1.1 Recherche amont

**Proposition 5** Reconduire, à partir de 2021, les appels à projets (AAPR) de l'axe « Technologies Quantiques » de l'Agence Nationale de la Recherche (ANR) visant à financer annuellement vingt projets exploratoires.

Les technologies quantiques ne disposent à ce jour pas d'un historique de développement suffisamment long permettant à une voie technologique donnée de prendre l'ascendant sur les autres. Dès lors, il est indispensable de maintenir un socle suffisant de recherche amont exploratoire. Ce socle de recherche concerne aussi bien les technologies de calcul quantique que celles des capteurs et communications quantiques.

Afin de pérenniser ce socle de recherche, il pourra être envisagé de reconduire les appels à projets de l'axe « Technologies Quantiques » de l'ANR qui s'arrêtera en 2020.

**Proposition 6** Renforcer l'axe « Technologies Quantiques » de l'ANR par une enveloppe financière visant à soutenir trois projets exploratoires ciblant les voies technologiques prioritaires identifiées.

En complément d'un socle de recherche transversal, un soutien plus ciblé sur les voies technologiques pour lesquelles la France bénéficie d'un avantage en matière d'acteurs académiques et industriels<sup>11</sup>, à travers des projets moins nombreux mais bénéficiant d'un financement plus important, permettra d'atteindre les seuils critiques de R&D nécessaires à la levée des principaux verrous scientifiques. Les projets à financer selon cette modalité devront comporter une forte composante de recherche amont exploratoire (*flying qubits*, relais quantiques, isolateurs topologiques, liens satellites, hétérojonctions Si/SiGe etc.) visant à renforcer la compréhension et à lever les incertitudes scientifiques autour des voies technologiques prioritaires<sup>12</sup>.

**Proposition 7** Inciter les laboratoires et entreprises français à répondre aux appels à projets européens Flagship « Quantum Technologies ».

Au niveau européen, les équipes de recherche académiques et industrielles françaises pourraient être encouragées à déposer davantage de propositions au *Flagship* Européen « Quantum Technologies » et aux futurs programmes Horizon Europe et Digital Europe, afin de compléter l'effort national. Un objectif de 12 à 15 M€ de co-financements européens annuel serait cohérent avec les taux de réussite constatés jusqu'à présent. Un alignement d'une partie de l'aide nationale sur les subventions européennes obtenues pourra être envisagé.

---

<sup>11</sup> Atomes froids, photonique et Silicium

<sup>12</sup> Le niveau de prise de risque scientifique devra constituer un critère d'évaluation de cet appel à projets

### V.2.1.2 Recherche partenariale

#### **Proposition 8** Inclure une priorité sur les technologies quantiques dans les futurs appels PSPC et Concours d'innovation.

En complément du soutien à la recherche académique, différents instruments d'aide à l'innovation et à la recherche partenariale entre les laboratoires publics et l'industrie pourraient être mobilisés :

- Concours d'Innovation i-Lab : concours de création de startups à destination des chercheurs.
- Concours d'Innovation i-Nov : concours d'aide aux startups et PME souhaitant développer une offre innovante.
- PSPC-Région : Projets collaboratifs visant à structurer des chaînes de valeurs industrielles.

S'agissant d'instruments existants ayant prouvé leur efficacité, il pourrait être envisagé d'introduire une priorité sur les technologies quantiques dans les prochains appels à projets. Un objectif de soutien à quinze concours i-Lab, cinq concours i-Nov et dix PSPC-Région<sup>13</sup> sur une période 5 ans pourrait être envisagé.

## V.2.2 Soutien aux ambitions françaises en matière de Calcul Quantique

### V.2.2.1 Ambitions sur les calculateurs « LSQ »

Un important effort de recherche a été déployé, à ce jour, par les équipes du CNRS et du CEA en vue de développer des *qubits* à base de semi-conducteurs, notamment sur le <sup>28</sup>Si.

Une équipe de cinquante chercheurs constituée d'ingénieurs en microélectronique (LETI) et de chercheurs en physique quantique (NÉEL, IRIG) a été constituée et a permis d'atteindre un certain nombre de jalons relatifs à la réalisation de *qubits* et de portes logiques (cf. Figure 7) : 6 *qubits* et de portes logiques (cf. Figure 7) : 6 *qubits* en Arséniure de Gallium, 1 *qubit* en Silicium, 1 porte à 2 *qubits*, etc.

La levée des verrous relatifs à la réalisation de calculateurs « LSQ » (cf. III.1.1) nécessitera, en plus des travaux sur les « Composants Technologiques », d'aborder les aspects « Micro Architecture » et « Architecture Système »<sup>14</sup> (cf. Figure 7) **de façon globale.**

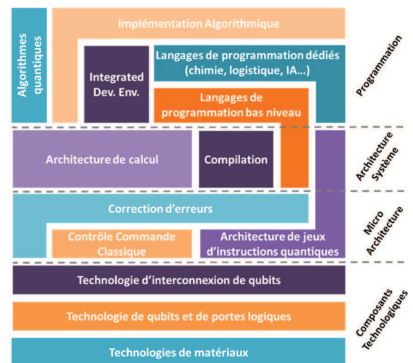


Figure 7: Briques technologiques d'un calculateur "LSQ"

<sup>13</sup> Les PSPC sont davantage adaptés aux projets à faible incertitude technologique. On limitera leur usage aux seuls projets de ce type.

<sup>14</sup> L'aspect programmation est abordé au V.2.2.2

### **Proposition 9 Renforcer les équipes microélectroniques grenobloises par des compétences en logiciels et architectures de calcul.**

Il sera indispensable de renforcer cette équipe tout en équilibrant la répartition des compétences. Disposer d'une masse critique d'ingénieurs et de chercheurs répartis de manière équilibrée entre composants technologiques et architectures est une **condition nécessaire** à l'atteinte des ambitions françaises en matière de « LSQ ».

Par ailleurs, les incertitudes scientifiques et technologiques qui jalonnent la réalisation d'un calculateur « LSQ » nécessitent une gestion de risque adaptée au cycle long du projet. Il sera, en effet, **particulièrement risqué de faire un pari unique sur une voie technologique donnée.**

### **Proposition 10 Déployer une gestion de projet agile afin de réduire progressivement les incertitudes et les coûts tout au long du projet.**

Une gestion du risque en « *fast fail* » permet de réduire les incertitudes et le coût au cours du temps. Grâce à cette méthode, plusieurs voies technologiques pourront être explorées en parallèle. Les options technologiques les moins prometteuses pourront être progressivement abandonnées.

### **Proposition 11 Déployer, au moyen d'une action du PIA<sup>15</sup> et d'un PPR<sup>16</sup>, un programme de R&D-Capitalisation visant à développer des accélérateurs quantiques scalables.**

De par les enjeux souverains, les incertitudes, les horizons de temps longs, et l'intensité capitalistique qui lui sont associés, le développement de capacités de calcul « LSQ » devra s'accompagner d'une action dédiée au niveau de l'État en partenariat avec les acteurs privés. Une action « accélérateurs quantiques » au niveau national, à laquelle pourrait s'ajouter un cofinancement européen des JU ECSEL et EuroHPC, permettrait de couvrir les besoins en dépenses de personnel et en lots technologiques.

Cette action pourra être menée en coordination avec la seconde phase du plan IA afin d'aborder le sujet des accélérateurs de calcul (XPU) de manière plus globale : accélérateurs quantiques, tensoriels, neuromorphiques, etc.

Les besoins de financement de ces actions complémentaires pourront faire l'objet d'une instruction plus approfondie par les services de l'État.

### **Proposition 12 Soutenir, à travers les AAPR de l'axe « Technologies Quantiques » de l'ANR, un programme de recherche visant à explorer des voies Silicium audacieuses.**

Dans l'esprit de la Proposition 10, des actions de recherche exploratoires et ambitieuses pourront bénéficier de l'AAPR « Technologies Quantiques » de l'ANR (cf. Proposition 6). Ces actions pourront, entre autres, concerner les jonctions Silicium/Germanium, les *qubits* topologiques sur Silicium, le Silicium dopé trous, les Nitrures de Silicium, les impuretés dans le Silicium pour *qubits* à température plus élevées, les couplages électron-photon, etc.

Ces actions exploratoires contribueront à **réduire le risque d'un engagement prématuré et irréversible** sur une voie technologique risquée.

<sup>15</sup> Programme d'Investissement d'Avenir

<sup>16</sup> Programme Prioritaire de Recherche

## V.2.2.2 Ambitions sur les calculateurs « NISQ » et les logiciels

**Proposition 13** Mettre en place, en 2020, un Grand Défi de l'Innovation « NISQ » visant à développer, avant 2023, une pile logicielle métier interoperable pour les secteurs de la chimie, de la logistique et de l'IA.

Afin de se prémunir d'une forte dépendance à un acteur unique, et répondre aux ambitions françaises en matière de leadership européen sur les calculateurs NISQ et les logiciels, la France pourra envisager de mettre en place un Grand Défi du Conseil de l'Innovation<sup>17</sup> relatif au thème suivant :

**« Comment utiliser du calcul quantique pour accélérer l'innovation dans la chimie, la logistique et l'intelligence artificielle »**

Ce Grand défi du Conseil de l'Innovation débouchera sur des solutions novatrices au profit des entreprises et des particuliers pour :

- Tirer le plus grand bénéfice des accélérateurs quantiques dans un contexte plus global du calcul haute performance en développant des solutions algorithmiques hybrides, en améliorant l'échange de données entre les calculateurs quantiques et calculateurs classiques et en développant des compilateurs mixtes performants.
- Diffuser l'usage du calcul quantique dans les secteurs prioritaires en développant des piles logicielles et des environnements de développement *hardware-agnostiques* sur la base de langages de programmations dédiés aux domaines de la chimie, de la logistique et de l'IA (*Domain Specific Languages*) et pouvant devenir à terme des standards.

Ce défi pourra s'appuyer sur les domaines d'excellence scientifique de la France, en matière d'algorithmie quantique et d'informatique théorique, ainsi que sur un terreau riche d'entreprises et d'écosystèmes d'innovation parmi lesquels :

- pour les académiques, le CNRS (PCQC, IRIF, LIP6, LORIA, etc.), l'INRIA, et le CEA (LIST) ;
- pour les grands groupes, Atos, TOTAL, EDF, SANOFI et AIRBUS ;
- pour les PME, PASQAL ;
- pour les pôles de compétitivité et IRT, le pôle Systematic et l'IRT SystemX.

Il pourra s'appuyer sur certaines communautés d'étudiants spécialisées dans l'informatique quantique et organiser des *hackathons* de développement algorithmique pour les usages clé ;

Il pourra, également, s'appuyer sur l'existence de plateformes technologiques disponibles ou en construction permettant de tester dans des conditions réalistes les innovations développées, notamment au TGCC (cf. V.1.1).

**Proposition 14** Inscrire le Grand Défi dans un cadre de collaborations avec d'autres pays européens.

Ce grand défi pourra, enfin, trouver **une résonance internationale**, que ce soit au niveau européen, notamment à travers l'entreprise commune EuroHPC, bilatéral avec l'Allemagne, par exemple en lançant le grand-défi d'une manière conjointe avec l'Allemagne qui vient

---

<sup>17</sup> Le conseil de l'innovation, instance de pilotage stratégique, orientera l'action du Gouvernement en matière d'innovation.

de créer son agence d'innovation de rupture, ou bilatéral avec l'Autriche qui dispose d'un leadership sur la conception de *qubits* à base d'ions piégés. Ce grand défi conjoint pourra, dès lors, bénéficier, côté allemand et autrichien, des expertises de :

- Innsbruck, Fraunhofer et Jülich pour la recherche publique ;
- BAYER, BASF, BOSCH et SAP pour les industriels *end-users*.

**Proposition 15 Renforcer les moyens de recherche en algorithmes et logiciels dans le domaine du calcul quantique.**

Dans le cadre de son contrat d'objectifs et de performance 2019-2023, INRIA a proposé que « les algorithmes et l'information quantiques » ainsi que « la cryptologie post-quantique » figurent parmi ses thèmes prioritaires.

Dans le cadre de ce programme, INRIA pourra constituer quinze équipes-projets communes avec les partenaires académiques et industriels qui recouvrent :

- à court et moyen terme : l'exploitation du hardware existant à travers le développement d'outils d'ingénierie logicielle et d'algorithmes adaptés;
- à plus long terme : le support au développement de nouveaux *hardware* (cf. V.2.2.1) à travers le développement de codes de correction d'erreurs et l'échange de données entre calculateurs classiques et quantiques.

**Proposition 16 Mettre en place, en 2022, un Grand Défi de l'Innovation visant à développer une solution de calcul quantique complète, sous réserve de résultats intermédiaires probants pour le Grand Défi « NISQ » et pour l'action PIA « accélérateurs quantiques ».**

Sous réserve que le Grand Défi lancé en 2019 et l'action « accélérateurs quantiques » aient fourni des résultats intermédiaires probants, il pourra être envisagé de lancer un second Grand Défi en 2022 visant à diffuser le plus largement possible une offre de calcul quantique complète incluant en plus des couches logicielles « *hardware-agnostiques* », les couches logicielles « *hardware-dépendantes* », ainsi que les composants matériels français et européens les plus avancées.

**Proposition 17 Inclure des spécifications pour l'acquisition d'accélérateurs quantiques expérimentaux dans certains appels d'offres de GENCI relatifs à l'acquisition, au renouvellement et à l'extension du parc de supercalculateurs français.**

Sous réserve de résultats intermédiaires satisfaisants pour le Grand Défi « NISQ » et d'une maturité suffisante (TRL4) des premiers dispositifs d'accélération quantique (*Pasqal*, *AQT Innsbruck*, consortium *OpenSuperQ...*), aussi bien d'un point de vue matériel que logiciel et intégration dans un environnement HPC classique, les différents appels d'offres de GENCI, relatifs à l'acquisition, au renouvellement et à l'extension de supercalculateurs du parc français, pourront être l'occasion d'inclure une spécification relative à un « bac à sable » d'accélérateurs quantiques.

### V.2.3 Soutien aux ambitions françaises en matière de Capteurs Quantiques

**Proposition 18** Structurer au moyen d'une succession de projets i-Lab, i-Nov et PSPC-Région une chaîne de valeur industrielle de production de capteurs à base d'impuretés dans le diamant.

Afin de répondre aux ambitions françaises sur les capteurs à base d'impuretés dans le diamant, la création, à partir des savoir-faire académiques, d'une startup, spécialisée dans la fabrication de diamants de haute qualité, sera un vecteur privilégié pour la création d'une chaîne de valeur industrielle complète de production de capteurs à base d'impuretés dans le diamant en France. Cette action pourra bénéficier successivement des aides i-Lab et i-Nov ainsi que d'un PSPC région, après la levée des principaux verrous technologiques.

### V.2.4 Soutien aux ambitions françaises en matière de Cryptographie

**Proposition 19** Soutenir, à travers les concours i-Nov et les dispositifs de soutien et d'accélération de l'innovation des ministères concernés, le développement, avant 2022, d'une offre compétitive de cryptographie post-quantique pour systèmes à ressources de calcul limitées.

Afin de répondre aux ambitions françaises en matière de cryptographie post-quantique pour dispositifs de sécurité à haute performance et à ressources de calcul limitées, les concours i-Nov, et plus généralement les outils d'accélération de l'innovation des ministères concernés pourront bénéficier aux industriels français, notamment les startups, développant ces technologies. Les appels à projets devront inclure un critère d'évaluation lié à la gestion du risque relatif au planning du concours du NIST visant à standardiser un certain nombre de primitives de cryptographie post-quantique.

**Proposition 20** Elaborer une stratégie d'évaluation des systèmes QKD s'appuyant sur le schéma de certification français et européen.

Sans certification par les organismes nationaux chargés de la sécurité des systèmes d'information, la QKD ne pourra pas être utilisée pour manipuler des informations sensibles. Un schéma de certification au niveau national et européen pourra être développé avec différents horizons de temps.

A court terme, l'analyse pourra porter sur les vulnérabilités de nature non quantique. Dans un second temps, le schéma de certification pourra s'intéresser à l'analyse des protocoles quantiques employés, de la cryptographie classique sur laquelle ils s'appuient, ainsi que des possibilités d'exploitation de canaux auxiliaires.

**Proposition 21** Soutenir, à travers les AAPR de l'axe « Technologies Quantiques » de l'ANR, une action de recherche relative à la maturation de la technologie QKD (systèmes à variables continues et à variables discrètes, relais quantiques, liens satellite, etc.) impliquant les experts des communications quantiques, les experts de la cybersécurité et les équipementiers télécom.

Les AAPR de l'axe « Technologies Quantiques » de l'ANR seront, dans un premier temps, le vecteur privilégié pour lever les verrous technologiques relatifs principalement à l'utilisation de la QKD à variables continues et à variables discrètes pour manipuler des informations



sensibles, ainsi qu'à l'intégration de dispositifs QKD, aux réseaux de communications existants, sans surcoût d'infrastructure prohibitif. Afin de maximiser les chances de réussite de ces travaux de recherche, l'interdisciplinarité devra constituer un critère d'éligibilité important dans le processus d'évaluation des dépôts de projets.

Sous réserve de résultats probants, les résultats de ces recherches pourront faire l'objet d'une valorisation industrielle à travers les concours i-Lab, i-Nov et PSPC.

## V.2.5 Soutien aux ambitions françaises en matière de Technologies habilitantes

**Proposition 22** Soutenir, à travers les concours i-Lab, les concours i-Nov et projets PSPC, le développement d'une offre française compétitive en matière d'ultravide et de cryogénie compacts pour les températures de 1 à 40 K.

Plusieurs voies de technologies quantiques prometteuses, à l'instar de la photonique et potentiellement le Silicium<sup>18</sup>, se satisfont de températures supérieures à 1 K. A ces niveaux de température, les systèmes cryogéniques sont de plusieurs ordres moins complexes et plus compacts que ceux nécessaires à la cryogénie sub-K (inférieure à 1 K).

Le développement d'une offre de cryogénie compacte compétitive pourra être soutenue par les concours i-Lab, les concours i-Nov et les appels à projets PSPC et bénéficier de l'écosystème industriel et de recherche français en matière de cryogénie sur-K : Thales , *CryoConcept*, *MyCryoFirm*, *Absolute System*, Institut Néel, IRIG, etc.

**Proposition 23** Soutenir, à travers les concours i-Lab, les concours i-Nov, les projets PSPC et les dispositifs de soutien et d'accélération de l'innovation du Ministère des armées, ou d'une action du PIA, le développement d'une offre française compétitive en matière de cryogénie extrême pour les températures sub-K.

Les besoins de cryogénie extrême sont, aujourd'hui, couverts principalement par trois acteurs mondiaux : *Bluefors* en Finlande, *Oxford instrument* au Royaume Unis et *JANIS* aux États-Unis. Ces entreprises répondent aux besoins des chercheurs avec des réfrigérateurs à dilution qui permettent d'atteindre des températures de quelques mK mais avec des puissances de refroidissement très faibles (~30  $\mu$ W).

La faible puissance de ces machines sera, à terme, un facteur limitant du développement du calcul quantique avec un grand nombre de *qubits*. En effet, ce nombre élevé de *qubits* nécessitera une puissance de refroidissement beaucoup plus conséquente (de 100 mW à quelques dizaines ou centaines de W).

Une action de R&D, associant *AirLiquide*, CEA, CNRS et l'écosystème de startups français permettra d'anticiper les enjeux du changement d'échelle des calculateurs quantiques, et de développer une nouvelle génération de réfrigérateurs avec une puissance augmentée d'un facteur 30 ou plus.

---

<sup>18</sup> Les *qubits* Silicium fonctionnent de manière nominale à 100 mK avec premières preuves de fonctionnement à 1 K.

## V.3 Un programme de soutien au développement des usages

### V.3.1 Calcul Quantique

**Proposition 24** Diffuser l'usage du calcul quantique, à travers des « Challenges » et « Hackathons » proposés par les industriels des secteurs applicatifs les plus avancés. Le « Airbus Quantum Computing Challenge » pourra être pris comme modèle.

A l'image des « Challenges IA », des « Challenges » et « Hackathons » quantiques pourraient être proposés par les acteurs industriels les plus avancés : Airbus, Atos, Thales, Total, Edf, Bosch, Bayer, SAP etc.

Profitant de l'infrastructure de calcul quantique du TGCC et de l'offre QCaaS associée, des startups et sociétés de service pourront répondre à ces « Challenges ». Ces actions permettent, ainsi, de développer l'écosystème de développement quantique, de diffuser et de vulgariser le calcul quantique, et d'inciter les chercheurs dans le domaine du calcul quantique à développer des startups et ainsi maximiser l'impact économique de leurs travaux de recherche.

### V.3.2 Capteurs Quantiques

**Proposition 25** Accompagner, à travers des « Challenges » proposés par les secteurs applicatifs, les fabricants de capteurs quantiques dans la recherche de débouchés auprès des secteurs applicatifs.

Des challenges proposés par des industriels utilisateurs finaux pourraient permettre aux startups et industriels proposant des capteurs quantiques de trouver des nouveaux débouchés de marché. Ces challenges sont particulièrement critiques pour le développement de l'écosystème des capteurs quantiques afin que cette technologie trouve sa place au côté des capteurs classiques dont les performances ne cessent de croître.

## V.4 Un environnement d'innovation efficace

### V.4.1 Instituts Interdisciplinaires

**Proposition 26** Créer, à Paris, à Saclay ainsi qu'à Grenoble, trois « Instituts Interdisciplinaires en Information Quantique » (3IQ) rassemblant chercheurs en physique quantique, chercheurs en informatique théorique et appliquée, ingénieurs, industriels des filières technologiques, et utilisateurs finaux.

80% de l'écosystème français du quantique est réparti entre Paris-centre, Saclay et Grenoble. Rassembler géographiquement les acteurs de cet écosystème dans trois « instituts Interdisciplinaires en Information Quantique » (3IQ) à l'image des instituts 3IA contribuerait à l'émulation entre chercheurs et industriels de différentes disciplines ainsi qu'à la visibilité et l'attractivité de l'écosystème à l'étranger. En effet, la concentration des ressources est un élément clé de l'efficacité des écosystèmes d'innovation.

A travers un volet foncier, soutenu par l'État et les collectivités, permettant de densifier les échanges entre des acteurs qui d'ordinaire ont très peu d'interactions, ainsi qu'une dotation de 23 M€/an à partir de 2021, les 3IQ pourront :

1. faciliter la recherche collaborative et interdisciplinaire entre les organismes publics et les industriels ;
2. mettre la recherche fondamentale au service des axes technologiques les plus stratégiques ;
3. créer une visibilité internationale multi-sites pour attirer les meilleurs talents à travers les chaires internationales, les « *frunchtech* visas » et les infrastructures de pointe (cf. V.1) ;
4. faire émerger et financer les phases de création des startups ;
5. accompagner les créateurs d'entreprises ;
6. faciliter la collaboration entre les startups et les clients industriels en faisant émerger des cas d'usage à travers une approche « *use-case-driven* » plutôt que « *techno-push* », notamment à travers les « Challenges » (cf. V.3) ;
7. mettre à disposition des moyens de tests et de validations : environnement de programmation quantique, accès à des accélérateurs quantiques, prototypes de réseau de communications quantiques etc.
8. développer des nouvelles filières de formation initiales et continues de chercheurs, d'ingénieurs et de techniciens en soutien à l'écosystème quantique ;
9. publier des analyses et recommandations à l'attention des décideurs économiques et des institutions publiques, tout en sensibilisant davantage la population académique et non académique aux enjeux, aux compétences, etc.

A Saclay, l'État pourra soutenir la dynamique déjà enclenchée par l'Université Paris Sud, les organismes de recherche, les industriels à l'instar de Thales, et la région, visant à créer un institut quantique d'envergure.

A Paris, le PCQC, regroupant depuis 2014 les chercheurs du CNRS, Sorbonne Université, et Université de Paris, en association des équipes d'INRIA Paris, des startups et des industriels parisiens, pourra préfigurer le prochain institut 3IQ de Paris.

A Grenoble, le rapprochement en cours entre l'INRIA, le CEA-LETI, le CEA-LIST sur le thème des architectures de calcul pour l'IA, en plus des synergies déjà très fortes entre CNRS-NEEL, CEA-LETI, CEA-IRIG et UGA ainsi que la présence d'Atos, pourra préfigurer l'institut 3IQ de Grenoble.

Pour la mise en place de ces instituts, **l'État pourra demander aux organismes de recherche publics, CEA, CNRS et INRIA, de proposer un programme cohérent pour la mise en place de ces instituts permettant d'avoir trois sites forts et visibles au niveau international aussi bien sur le plan de la recherche que sur le transfert à l'industrie.**

Si la logique de concentration géographique est vertueuse pour l'innovation de rupture et justifie la création d'un nombre limité d'Instituts 3IQ, **les trois instituts seront appelés à mettre en place des stratégies d'inclusion permettant de mobiliser l'ensemble des compétences nationales.**

**Proposition 27** Intégrer un critère d'évaluation relatif à l'interdisciplinarité dans les appels à projets collaboratifs de l'ANR et de la BPI.

Afin d'inciter les différentes communautés à travailler ensemble (cf. Verrou 14) sur la levée des verrous scientifiques et technologiques de l'information quantique, les différents appels à projets de l'ANR et de la BPI relatifs aux technologies quantiques pourront explicitement demander à ce que les projets soumis soient interdisciplinaires : physique et technologies de l'information, physique et ingénierie, physique et cryptographie, etc.

Le niveau d'interdisciplinarité pourra faire l'objet d'un critère d'évaluation dans le processus de revue des projets soumis.

#### V.4.2 Développement des compétences

**Proposition 28** Inclure 6 ECTS<sup>19</sup> d'algorithmie quantique dans les vingt principaux cycles d'ingénieurs et masters en informatique et 6 ECTS de cryptographie post-quantique et quantique dans les masters de cryptographie.

Sans vouloir faire de tous les ingénieurs et diplômés de masters informatiques des experts de l'informatique quantique ou de tous les cryptographes des experts de la cryptographie post-quantique et quantique, que l'actuel marché de l'emploi n'est de toute manière pas en mesure d'absorber, une introduction à ces disciplines dans les principaux parcours de formation en informatique et en cryptographie s'impose. En effet, bien que ces disciplines soient naissantes, on observe dès à présent une difficulté de recrutements dans les entreprises qui souhaitent s'investir dans ces technologies aussi bien sur le plan du développement technologique que sur le plan de l'usage.

**Proposition 29** Concevoir des parcours de formation avec une spécialisation en ingénierie et en informatique quantique et anticiper la croissance du besoin en ingénieurs et techniciens des filières industrielles.

En nombre plus limité, des parcours de formation plus spécialisés pourront être développés afin d'alimenter le besoin pointu des entreprises technologiques, notamment les startups, aussi bien en ingénierie quantique à proprement parler qu'en technologies habilitantes comme de la cryogénie avancée.

---

<sup>19</sup> Système de crédits développé par l'Union européenne dans le cadre du processus de Bologne

### V.4.3 Mobilité des chercheurs

#### **Proposition 30** Sensibiliser les acteurs de l'écosystème aux nouvelles dispositions de la loi PACTE relatives à la mobilité des chercheurs et l'accès aux moyens des laboratoires par les startups.

Avant la loi PACTE, la participation d'un chercheur du CNRS ou de l'INRIA à un projet entrepreneurial visant à valoriser ses résultats de recherche s'accompagnait d'une contrainte majeure liée aux règles de déontologie incombant à la fonction publique. S'il décidait de rejoindre l'entreprise entrepreneuriale, le chercheur perdait son statut de fonctionnaire et la sécurité de l'emploi qui en découle ainsi que l'accès aux infrastructures de recherche de son laboratoire d'origine.

Il s'agit de deux freins majeurs à la transformation d'une découverte ou d'une invention disruptive dans le domaine des technologies quantiques en projet industriel et en avantage compétitif pour le tissu économique.

Dans d'autres pays, à l'image des États-Unis, du Royaume-Unis ou de l'Allemagne, il est courant de voir les chercheurs créer des startups tout en gardant leurs postes dans leurs laboratoires et universités d'origine et tout en bénéficiant des équipements de recherche de ces derniers, ce qui constitue un avantage compétitif important pour la startup.

Ces deux verrous ont été levés par la loi PACTE du 22 mai 2019 qui a introduit de la flexibilité dans les modalités de coopérations entre les chercheurs, les startups qui valorisent leurs travaux et les laboratoires académiques.

Les nouvelles dispositions de la loi PACTE et la flexibilité qu'elle introduit ne sont pas encore bien connues d'une majorité des chercheurs de la communauté académique.

Des actions de sensibilisation auprès des chercheurs et directeurs de laboratoires, y compris en dehors de la communauté quantique, sont nécessaires afin de lever les blocages des chercheurs désireux de valoriser leurs travaux de recherche mais inquiets par rapport aux anciennes dispositions du code du travail.

### V.4.4 Capital Risque

#### **Proposition 31** Accompagner la création d'une cinquantaine de startups du quantique jusqu'en 2024.

Dans le prolongement du plan « DeepTech » mis en place début 2019, l'État pourra demander à la BPI d'accompagner la création de startups du quantique selon un rythme de 5, 10, 10, 15 et 15 startups entre 2020 et 2024. Cet accompagnement pourra se faire soit en aide directe aux startups (i-Lab, i-Nov, Capitalisation...), soit à travers l'investissement de la BPI en « fonds de fonds ». Les startups accompagnées pourront bénéficier de l'excellence de l'écosystème de recherche français pour adresser différents marchés du calcul, des capteurs et des communications quantiques.

La création de startups du logiciel sera facilitée par la mise en place de l'infrastructure nationale de calcul quantique (cf. Proposition 1) et de l'offre QCaaS associée (cf. Proposition 3). En effet, il est observé, aux États-Unis et au Canada, que depuis la mise en place des accès Cloud aux calculateurs d'IBM et de D-Wave, la dynamique création de startups logicielles s'est accélérée (e.g. simulation de protéines, smart-grid, mobilité intelligente, etc.).

**Proposition 32** Faire émerger un fond d'investissement « late-stage » de confiance de 300-500 M€ dédié aux startups du quantique.

Comme pour toutes les startups françaises, les levées de fonds en série B et C (50 – 200 M€) nécessitent généralement de faire appel à des investisseurs non européens avec des impacts négatifs sur la souveraineté technologique, freinant ainsi l'émergence de licornes françaises. La constitution d'un fond d'investissement « late stage » **de confiance**<sup>20</sup> est indispensable pour accompagner les startups quantiques françaises au-delà des phases de seed et de série A (1 – 20 M €). Ce fond devra, néanmoins, être disjoint des fonds dédiés au numérique, compte tenu des horizons temporels différents : 2-3 ans pour le numérique, 5-8 ans pour le quantique. Ce fond de confiance pourra lever 300 à 500 M€ auprès d'industriels français à l'instar d'Atos, de Thales, de Total, d'Edf ou d'Airbus, d'institutionnels comme AXA ou la BNP ainsi qu'auprès de la BPI.

---

<sup>20</sup> Ce fond pourra s'appuyer sur la stratégie de l'État en matière de « ScaleUp », annoncée par le gouvernement, le 17 septembre 2019.

## V.5 Une stratégie de sécurité et d'intelligence économique adaptée

### V.5.1 Protection du patrimoine scientifique et technologique

Les perspectives d'évolution annoncées par les technologies quantiques encouragent certains organismes ou États à s'intéresser à l'écosystème français et à cibler les acteurs les plus vulnérables, qui par ailleurs sont en pointe au niveau mondial. Les enjeux de souveraineté liés au développement d'une offre en matière de technologie quantique et le profil des acteurs clés de cette stratégie appellent une stratégie de sécurité économique adaptée.

**Proposition 33** Sensibiliser les différents acteurs les plus stratégiques aux risques de pillage technologique et aux outils disponibles permettant d'y faire face.

La protection du patrimoine scientifique n'est pas une notion à laquelle les chercheurs académiques sont naturellement réceptifs. Des actions de sensibilisation à la sécurité économique seront nécessaires pour faire face aux risques de pillage technologique.

**Proposition 34** Repérer et surveiller les actifs et activités stratégiques et déployer, au besoin, le dispositif de Protection du Potentiel Scientifique et Technologique (PPST).

Des dispositions à l'instar de la sécurisation des systèmes d'information ou de la mise en place de zones à régime restrictif pourront être déployées pour protéger les actifs scientifiques et technologiques les plus stratégiques aussi bien dans les laboratoires publics que dans les startups issues de la recherche publique. Le conditionnement des financements publics à l'adhésion au dispositif PPST pourrait être envisagé.

D'autres mesures plus innovantes ou contraignantes sont proposées dans le rapport de l'IGF sur les outils de sécurité économique (remboursement avec très lourdes pénalités des aides publiques versées en cas de vente à un acteur étranger par exemple). Enfin, la généralisation du dispositif des investissements étrangers en France aux secteurs les plus stratégiques couplée à la détection précoce des investissements jugés problématiques participe à une meilleure défense de ce secteur.

### V.5.2 Diplomatie Economique

**Proposition 35** Identifier les espaces de coopérations et les synergies possibles avec les partenaires internationaux de la France en matière de technologies quantiques.

Plusieurs pays européens et extra-européens actifs en matière de technologies quantiques pourraient devenir des partenaires de premier plan de la France en matière de technologies quantiques.

Des prises de contact à bon niveau pourraient permettre d'identifier des synergies entre les stratégies nationales de la France et de ses partenaires internationaux.

## V.6 Une gouvernance efficace

### **Proposition 36** Constituer un Comité Stratégique chargé de prendre les décisions d'orientation des actions de recherche.

Le niveau élevé d'incertitudes relatif à certaines voies de développement des technologies quantiques, les horizons de temps longs des actions à mener (2030) et l'intensité capitalistique nécessaire implique que la stratégie de l'État ne peut pas être immuable et se doit de réorienter, au besoin, ses actions sur la durée du plan national. Pour ce faire, l'État aura besoin d'une gouvernance **agile** et dotée d'un **pouvoir décisionnel**. Une situation analogue a été observée dans le domaine de l'aérospatial et du calcul intensif. L'État y a répondu en constituant des comités stratégiques regroupant les représentants de l'État, des organismes de recherche et de l'industrie. D'une manière analogue, un Comité Stratégique pourra être constitué afin de piloter chacune des actions structurantes du PIA.

Le Comité pourra se réunir une à deux fois par an et aura pour objet de :

- impulser les options technologiques structurantes (soutien à une voie technologique plutôt qu'une autre, décider du développement d'une brique technologique ou de l'importer, etc.) ;
- coordonner les actions de recherche depuis la recherche fondamentale jusqu'aux démonstrateurs TRL6 ;
- suivre l'exécution budgétaire.

### **Proposition 37** Nommer un coordinateur interministériel du plan national, chargé de veiller à la cohérence globale des actions des différents acteurs publics et privés au niveau national.

Au même titre que pour la stratégie nationale en intelligence artificielle, un coordinateur interministériel pourra être nommé. Ce dernier aura un rôle plus opérationnel que le Comité Stratégique. Il sera notamment chargé de :

- veiller à la bonne exécution de la stratégie nationale par les acteurs ;
- veiller à la bonne structuration de la filière naissante ;
- veiller à la bonne coordination et articulation des actions menées par les organes de l'État, les organismes de recherche et les industriels.

Le coordinateur interministériel rendra compte de son action au gouvernement.



## La mission



### **Paula Forteza** députée LREM des Français de l'Étranger (2<sup>e</sup> circonscription)

Agée de 33 ans, Paula Forteza est née à Paris de parents argentins, et a passé plus de 20 ans de sa vie en Amérique Latine. Après plusieurs expériences au sein du gouvernement de la ville de Buenos Aires, de l'administration française (Etablissements), ou encore dans l'entrepreneuriat, elle souhaite avant tout mettre le numérique, la transparence et la participation citoyenne au cœur du débat politique en France. Depuis le début de la mandature, Paula Forteza s'est notamment impliquée dans le projet de loi de moralisation de la vie politique, la transposition du règlement général sur la protection des données personnelles (RGPD), ainsi que dans le projet de réforme de l'Assemblée Nationale. Elle a également contribué à faire avancer le débat public sur de nombreux autres sujets liés au numérique tels que la lutte contre les Fake News, la gouvernance du net, la régulation et la fiscalité des géants du web, la place des femmes dans le numérique ou encore l'impact environnemental du numérique.

En avril 2019, Paula Forteza a été mandatée par le Premier ministre pour une mission de quatre mois sur les technologies quantiques.



### **Jean-Paul Herteman** Président d'Honneur du GIFAS, Président-directeur général du Groupe SAFRAN entre septembre 2007 et avril 2015

Jean-Paul Herteman débute sa carrière d'ingénieur de l'armement en 1975 au Centre d'essais aéronautiques de Toulouse (Ceat) et rejoint Snecma en 1984. Successivement Responsable recherche en matériaux, Directeur de la Qualité puis du bureau d'Etudes, il devient en 1995 Directeur des programmes CFM 56 et vice-Président de CFM International. Il assurera la Direction Technique de Snecma de 1996 à 1999 puis se verra confier la Direction Générale de la Division Moteurs-fusées jusqu'en 2002. Il est nommé Président-directeur général de Snecma Moteurs en février 2002. En 2004 il accède à la fonction de Directeur Général Adjoint de Safran, en charge de la Branche Propulsion. Il est nommé Président-directeur général de Sagem Défense Sécurité (2006-2007) et chargé de la Branche Défense Sécurité. Il devient en 2007 Président du Directoire du groupe Safran, puis Président-directeur général de 2011 à 2015.



### **Iordanis Kerenidis** Directeur de recherche au CNRS

Iordanis Kerenidis a obtenu, en 2004, un doctorat du département d'informatique de l'Université de Californie, à Berkeley. Après un contrat de deux ans au Massachusetts Institute of Technology (MIT), il a rejoint le Centre national de recherche scientifique (CNRS) à Paris en tant que chercheur permanent. Il a remporté une bourse européenne Marie Curie, un financement « Jeunes chercheuses – Jeunes chercheurs » de l'Agence nationale de la recherche (ANR) et un financement de l'European Research Council (ERC Starting Grant). Ses recherches sur les algorithmes et les communications quantiques ont fait l'objet de plus de soixante-dix publications dans des revues renommées et des actes de conférence à comité de lecture. Ses derniers travaux ont pour but de trouver des applications concrètes aux ordinateurs quantiques dans les domaines de l'optimisation et de l'apprentissage automatique. Il est directeur du « Paris Centre for Quantum Computing », centre de recherche interdisciplinaire qui constitue le fer de lance des technologies quantiques en Europe.

## Personnes auditionnées

Adrien Facon • Alain Aspect • Alain Schuhl • Annaïg Andro • Anthony Leverrier • Arnaud Landragin • Bernard Giry • Bernard Hamelin • Bernard Ourghanlian • Bertrand Monthubert • Bruno Sportisse • Charles Beigbeder • Christophe Jurczak • Christophe Strobel • Cyril Allouche • Cyril Baudry • Daniel Estève • Daniel Verwaerde • Delphine Roma • Diane Dufoix-Garnier • Dominique Thomas • Eleni Diamanti • Elisabeth Giacobino • Eric Jaeger • Éric Vacaresse • Florent Muller • Franck Pereira dos Santos • Franck Schlie • François Alter • François Jacq • Frederic Magniez • Frederic Valette • George-Olivier Reymond • Georges Ulzbelger • Gilles Ceyssat • Guillaume Colin de Verdiere • Henri Calandra • Hervé Mouren • Hisham Abou Kandil • Hubert Fraysse • Ivan Testart • Jean-Jacques Rabeyrin • Jean-Charles Faugere • Jean-Christophe Gougeon • Joffrey Célestin-Urbain • Khalil Rouhana • Laure Le Bars • Ludovic Perret • Martine Garnier • Mathieu Landon • Maud Vinet • Nolwenn Rozen • Olivier Ezratty • Pascale Senellart • Patrice Bertet • Philippe Duluc • Philippe Grangier • Pierre Perrot • Raphaël Jammes • Roberto Viola • Romain Alléaume • Sebastien Kunz-Jacques • Sébastien Tanzilli • Serge Haroche • Stéphane Bajard • Thierry Debuisschert • Thierry Lahaye • Thierry Petit • Tristan Meunier • Valérie Gacogne • Valérian Giesz • Vincent Mages • Xavier Vasques • Xavier Waintal • Yannick Devouassoux • Zaki Leght



