



**Rapport sur les technologies quantiques  
pour les applications  
Aéronautique-Spatial-Défense**

**Groupe de Travail  
Technologies Quantiques**

**COMMISSION R&D**

(page laissée intentionnellement blanche)

<b>PREAMBULE .....</b>	<b>4</b>
<b>RESUME AUX DECIDEURS.....</b>	<b>6</b>
<b>LISTE DES PRINCIPALES RECOMMANDATIONS .....</b>	<b>8</b>
<b>1. CAPTEURS QUANTIQUES.....</b>	<b>10</b>
1.1 RESUME AUX DECIDEURS.....	10
1.2 DESCRIPTIF ET CAS D'USAGE.....	11
1.2.1 <i>Atomes froids</i> .....	12
1.2.2 <i>Cellules à gaz pompées</i> .....	15
1.2.3 <i>Centres NV</i> .....	20
1.2.4 <i>Cristaux dopés aux ions terre-rare</i> .....	23
1.2.5 <i>Circuits supraconducteurs</i> .....	24
1.3 CAPTEURS QUANTIQUES, CAS D'USAGE ET HORIZONS ASSOCIES (TABLEAU DE SYNTHESE) .....	24
1.4 RECOMMANDATIONS .....	26
<b>2. COMMUNICATIONS QUANTIQUES.....</b>	<b>28</b>
2.1 RESUME AUX DECIDEURS.....	28
2.2 CONTEXTE ET CAS D'USAGE.....	28
2.3 DESCRIPTION DES SYSTEMES DE COMMUNICATION QUANTIQUE.....	32
2.3.1 <i>Les grands systèmes</i> .....	32
2.3.2 <i>Les technologies habilitantes</i> .....	34
2.4 CONCLUSIONS ET RECOMMANDATIONS .....	35
<b>3. CALCUL QUANTIQUE.....</b>	<b>38</b>
3.1 RESUME AUX DECIDEURS.....	38
3.2 CONTEXTE.....	39
3.2.1 <i>Les applications</i> .....	39
3.2.2 <i>Les Algorithmes</i> .....	40
3.2.3 <i>Les QPUs</i> .....	42
3.2.4 <i>Benchmarking</i> .....	43
3.2.5 <i>Environnement</i> .....	44
3.2.6 <i>Une Roadmap ?</i> .....	45
3.3 LES ACTIONS A POURSUIVRE ET/OU INTENSIFIER.....	46
3.4 CONCLUSIONS ET RECOMMANDATIONS .....	48
3.5 SYNTHESE DES RECOMMANDATIONS.....	50
<b>4. TECHNOLOGIES HABILITANTES.....</b>	<b>52</b>
4.1 RESUME AUX DECIDEURS.....	52
4.2 LISTE DES TECHNOLOGIES HABILITANTES .....	53
<b>5. FORMATION .....</b>	<b>66</b>
<b>GLOSSAIRE .....</b>	<b>68</b>

(page laissée intentionnellement blanche)

# Préambule

Ce rapport a été rédigé à la demande de la commission R&D du GIFAS par un groupe de travail dédié aux technologies quantiques et constitué de représentants des principaux industriels du domaine, sous la coordination de l'ONERA. Ce groupe de travail, créé début 2021, s'est depuis réuni régulièrement (14 réunions plénières entre février 2021 et mars 2023). Fin 2022, il s'est vu confier par la commission R&D la mission suivante, dont le présent rapport relate les principales conclusions :

*Définir les apports majeurs pour la filière des technologies quantiques, les applications ciblées et les horizons calendaires associés ainsi que d'éventuelles recommandations pour la filière et pour le coordinateur national pour la stratégie quantique. Le sous-groupe Technologies quantiques animé par l'ONERA et rassemblant une douzaine de sociétés du GIFAS sera sollicité pour mener ces réflexions en coordination avec la Commission R&D.*

Ce rapport a été conçu pour permettre plusieurs niveaux de lecture. Les lecteurs les plus pressés pourront se limiter au résumé général et à la liste consolidée des recommandations qui suivent. Un deuxième niveau de lecture possible est de ne considérer, dans chacune des 4 parties principales du rapport (capteurs quantiques, communications quantiques, calcul quantique et technologies habilitantes), que le résumé initial qui figure au début de chaque partie et/ou la liste plus détaillée des recommandations qui figure à la fin. Enfin, le lecteur disposant de plus de temps trouvera dans chacune des parties un descriptif détaillé des technologies et des cas d'usage que nous avons identifiés pour les applications intéressant le GIFAS.

## Composition du groupe de travail « technologies quantiques » du GIFAS

Coordinateur : Sylvain Schwartz (ONERA)

### Sous-groupe capteurs quantiques

Coordinateur : Philippe Dejean (SAFRAN)

Participants : Daniel Dolfi et Arnaud Brignon (Thales TRT), Mathilde Portais et Romain Kukla (Naval Group), Oriane Lelièvre et Sébastien Laux (Thales MIS), Alexandre Kotenkoff et Léo Dumas (MBDA), Philippe Millet (Nexter), Alexandre Bresson et Hervé Verrièle (ONERA)

### Sous-groupe communications quantiques

Coordinateur : Mathias van den Bossche (Thales Alenia Space)

Participants : Andrew Thain (ADS), Philippe Millet (Nexter), Jean-Marc Conan (ONERA), Cyrille Laborde (Thales Alenia Space)

### Sous-groupe calcul quantique

Coordinateurs : Alain Refloch (ONERA) et Frédéric Barbaresco (Thales)

Participants : Robert Wang, Olivier Hess et Philippe Duluc (Eviden/Atos), Denys Quesneau (Ariane Group), Edouard Debry et Leo Dumas (MBDA), Gilles Zalamansky (Dassault Aviation), Marc Contat (ADS)

### Sous-groupe technologies habilitantes

Coordinateurs : Gilles Triay (GROUPEADF) et Delphine Roma (Air Liquide)



# Résumé aux décideurs

La mécanique quantique, élaborée au début du XX<sup>ème</sup> siècle et permettant de décrire le comportement des particules à l'échelle microscopique, a donné naissance à partir des années 1960 à une première vague d'applications qui ont radicalement transformé la société moderne. Ainsi les semiconducteurs, les lasers, la résonance magnétique nucléaire ou les horloges atomiques et toutes les applications qui en découlent doivent-ils leur existence à la théorie quantique. On parle parfois à leur sujet de première révolution quantique. En retour, certaines de ces applications technologiques ont permis aux scientifiques puis aux ingénieurs d'acquérir un degré de contrôle de plus en plus important sur les systèmes quantiques élémentaires (atomes, photons et qubits artificiels), ouvrant la voie à une deuxième génération d'applications que l'on qualifie de seconde révolution quantique. La plus emblématique de ces applications potentielles est sans aucun doute l'ordinateur quantique, qui offre la promesse d'un gain exponentiel sur certains algorithmes par rapport aux ordinateurs classiques, mais ce n'est pas la seule. Ainsi les dispositifs quantiques peuvent-ils également apporter un « avantage quantique » dans le domaine des capteurs (gain en sensibilité, auto-calibration, réduction de la taille...) ou dans celui des communications sécurisées.

Si ces trois piliers des technologies quantiques que sont le calcul quantique, les capteurs quantiques et les communications quantiques offrent tous des perspectives intéressantes dans le domaine ASD (aéronautique-spatial-défense), il convient de distinguer d'un côté les capteurs et les communications pour lesquels les industriels du GIFAS sont à la fois constructeurs et utilisateurs potentiels et de l'autre le calcul quantique pour lequel le matériel est majoritairement développé par des start-ups hors GIFAS, le principal apport des industriels du GIFAS devant se situer au niveau du développement des algorithmes adaptés à ces nouvelles machines. Les échéances pour les différents piliers sont également diverses. S'il est difficile de prédire l'avenir d'autant plus pour un secteur qui évolue très rapidement, il semble toutefois clair que les capteurs quantiques sont les plus susceptibles d'apporter à court terme (moins de 5 ans) des avantages concrets pour un certain nombre d'applications ASD. Le déploiement d'un réseau de communications quantiques semble envisageable à moyen terme (5 ans ou plus) tandis que les applications du calcul quantique, plus incertaines, sont plutôt espérées à moyen ou long terme.

Il nous semble donc important, dans le contexte actuel, de renforcer les investissements sur les capteurs et les communications quantiques, tout en développant la recherche de nouveaux algorithmes quantiques pour les applications ASD. En termes de technologies habilitantes, on note un fort recouvrement entre les différents piliers qui fait qu'un investissement initialement dédié aux capteurs quantiques (par exemple le développement d'un détecteur de photons à bas bruit) pourrait ensuite bénéficier aux communications quantiques puis au calcul quantique (calcul quantique photonique dans cet exemple). A cet égard, nous avons identifié un certain nombre de technologies habilitantes clés qu'il conviendrait de soutenir, afin de pérenniser la filière et de garantir un accès aux composants dans les années qui viennent. On pense notamment à la photonique intégrée, aux cryocoolers 4K transportables ou à certains types de lasers et de composants optiques. Il nous semble également important de continuer à soutenir le développement d'une offre de formation pour les futurs ingénieurs et techniciens des métiers du quantique, aussi bien au niveau universitaire qu'en ce qui concerne la formation continue.

Finalement, il convient de souligner que la France dispose d'un écosystème quantique exceptionnel avec des laboratoires académiques de pointe, des start-ups couvrant quasiment l'ensemble des technologies quantiques et un réseau d'industriels prêts à développer et à mettre en œuvre ces technologies, le tout avec un soutien étatique fort. L'objectif des quelques recommandations et du rapport qui suivent est de contribuer à l'essor de cet écosystème, au bénéfice des industriels du GIFAS et de l'ensemble de la communauté nationale.

(page laissée intentionnellement blanche)



# Liste des principales recommandations

Capteurs 1	Encourager, au niveau national, le soutien au développement des capteurs quantiques notamment dans les domaines suivants d'intérêt majeur pour les applications ASD : atomes froids, horloges atomiques compactes, magnétomètres haute performance et capteurs électromagnétiques radiofréquence
Comm. 1	Pour les réseaux d'information quantique, soutenir le développement d'un système de démonstration de la distribution de la ressource d'intrication depuis l'orbite basse vers deux stations sol dans le cadre du programme national QINSAT avec une contribution du plan quantique. Dans ce cadre, soutenir en particulier des démonstrateurs opérationnels de source de photons intriqués spatialisée, terminaux récepteurs d'intrication, systèmes de synchronisation et de datation ultra précis, système d'optique adaptative sol, légère et bas cout, système de contrôle de la polarisation des photons.
Calcul 1	Encourager le développement de la recherche sur les algorithmes quantiques et les cas d'usage ASD associés (par exemple en soutenant des projets impliquant des industriels du GIFAS et des acteurs académiques du domaine). Cette action, en cohérence avec les actions en cours dont le projet Proqcima récemment lancé par la DGA, pourra s'appuyer sur le projet BACQ existant.
Technos 1	Construire pour chacune des technologies habilitantes clés détaillées dans ce rapport une stratégie d'acquisition pérenne, en s'appuyant sur les synergies entre les capteurs, les communications et le calcul quantique. On citera notamment la cryogénie embarquable (2-4K mais aussi 40-80K), des lasers compacts et robustes y compris pour les applications spatiales, des masers embarquables, des cellules à gaz, des cristaux non-linéaires haute brillance, des détecteurs de photons haute efficacité / faible bruit et des modules de photonique intégrée. Soutenir auprès des instances nationales le projet d'une ligne pilote européenne dédiée aux circuits photoniques intégrés pour les technologies quantiques.
Calcul 2	Faciliter l'accès pour les industriels du GIFAS aux machines quantiques déjà disponibles avec le bon niveau de sécurité : à court terme par la subvention d'heures de calcul pour pouvoir tester des algorithmes élémentaires (ne pas forcément se limiter aux machines françaises dans un premier temps), et à long terme par le soutien à la maturation technologique d'un réseau d'information quantique pour permettre de faire tourner des algorithmes sensibles ou confidentiels de façon sécurisée via le cloud (et aussi pour interconnecter les calculateurs quantiques)
Capteurs 2	Inciter les membres du GIFAS à collaborer activement entre eux et avec les autres parties prenantes à l'élaboration de nouveaux cas d'usage pour tirer le meilleur parti des propriétés uniques des capteurs quantiques

Comm. 2	Aider les industriels français à se positionner dans les projets de clés quantiques européens (EuroQCI) en contribuant aux actions européennes sur le sujet lorsqu'elles demandent une coparticipation des états membres, en participant aux comités de standardisation ces systèmes qui ont vocation à être multi vendeurs et devront être interopérables et en promouvant l'intérêt du sujet auprès de l'ANSSI, avec laquelle nous partageons le besoin de sécurité de bout en bout. Dans ce but, on s'attachera notamment au développement des briques technologiques suivantes : terminaux de clés quantiques, sources de photons uniques si possibles non-cryogéniques, générateurs quantiques de nombres aléatoires, systèmes de gestion de clés.
Calcul 3	Encourager les industriels du GIFAS à adopter et à faire évoluer les benchmarks proposés par le projet BACQ et à en publier les valeurs mesurées afin de partager un outil d'évaluation commun pour suivre quantitativement les progrès des machines quantiques disponibles.
Calcul 4	Encourager le développement de piles logicielles de confiance (compilateur, bibliothèque, outils de programmation/ingénierie logicielle), pour aller du langage de haut niveau jusqu'au niveau circuit quantique. Dans ce cadre, on veillera à promouvoir les liens entre HPC classique et calcul quantique, car il est clair que ce dernier ne trouvera d'applications qu'en complément des moyens de calcul classique existants.
Capteurs 3	Explorer dès maintenant avec les parties prenantes l'intégration des capteurs quantiques dans des futurs systèmes afin de maximiser la performance système atteignable et d'accélérer cette intégration.
Comm. 3	Pour la préparation de la phase 2 de QINSAT qui visera à assembler plusieurs liens réseaux à la fin de la décennie soutenir les acteurs qui développent les mémoires quantiques longue cohérence et facilement adressables, les routeurs d'intrication qui utiliseront ces mémoires quantiques et les dispositifs de distillation d'intrication pour améliorer les performances des liens individuels en soutenant les acteurs plus amont qui travaillent sur ces sujets (start-ups, laboratoires publics ou privés, intégrateurs système) par du développement d'équipements ou de démonstrateurs sur table.
Calcul 5	Consolider / veiller à être en mesure de garantir une filière industrielle européenne pour garantir à terme l'accès aux machines et un modèle économique viable pour les constructeurs de machines français (subventions à l'achat...)
Formation 1	Encourager le développement, en complément des formations universitaires, d'une offre importante de formation continue dans le domaine des technologies quantiques à destination des techniciens et des ingénieurs ayant vocation à travailler dans le domaine. Une difficulté peut apparaître liée aux fondements mathématiques de la théorie quantique, qui nécessiteront sans doute de mettre en place plusieurs niveaux dans l'offre de formation continue aux technologies quantiques.
Formation 2	Une bonne connaissance de l'algorithmie classique étant nécessaire pour appréhender les enjeux du calcul quantique, il serait également pertinent de développer de telles formations dans le cadre du plan quantique national.

# 1. Capteurs quantiques

## 1.1 Résumé aux décideurs

On appelle capteur quantique un capteur qui utilise une ressource quantique (photons, atomes, qubits artificiels...) pour mesurer une grandeur physique (temps ou fréquence, forces inertielles, champs électromagnétiques...). L'avantage quantique, expression habituellement utilisée pour le calcul quantique, peut prendre dans le cas des capteurs des formes variées : gain en sensibilité, stabilité long terme et absence de dérive, auto-calibration, réduction de la taille... Il existe à ce jour une grande variété de capteurs quantiques, avec des niveaux de maturité allant de la preuve de concept en laboratoire (ghost imaging, gyroscope à atomes froids...) jusqu'au TRL9 (gravimètre à atomes froids). On trouvera un tableau de synthèse des différentes technologies à la fin de cette partie (section 1.3).

Dans le cadre de la deuxième révolution quantique actuellement en cours, les capteurs quantiques ont une importance particulière pour les industriels du GIFAS, qui en sont à la fois des utilisateurs et des constructeurs potentiels. Parmi ces capteurs, certains pourraient apporter des avantages quantiques clairs pour des applications déjà bien identifiées, l'effort de développement portant de plus en plus sur la tenue à l'environnement et sur l'industrialisation.

Nous avons identifié quatre classes de capteurs quantiques et d'applications associées d'intérêt majeur à court terme (moins de 5 ans) pour le GIFAS :

- Les technologies à base d'atomes froids peuvent apporter des références gravimétriques et gradiométriques (permettant notamment l'établissement de cartes de gravité) ainsi que la réalisation de centrales inertielles absolues. Ces dernières pourraient contribuer à une navigation purement inertielle, précise et résiliente.
- Le partage d'un temps précis est nécessaire pour de nombreuses fonctions des systèmes d'armes, en particulier les communications. Les systèmes de géolocalisation par satellite fournissent cette base de temps, mais leur disponibilité en environnement de guerre électronique ne peut être garantie. L'apparition d'horloges atomiques d'un SWaP-C<sup>1</sup> extrêmement contenu permet d'envisager de nouvelles architectures de partage du temps pour les systèmes d'armes avec des capteurs nombreux et répartis, nécessitant moins de resynchronisation, participant à l'accroissement de la résilience vis-à-vis du brouillage ou de l'interdiction des GNSS.
- Les solutions issues des technologies quantiques pour obtenir des capteurs magnétiques très performants sont nombreuses : centres NV, SQUIDS, cellules à gaz. Leur maturité est élevée, leurs applications au domaine de la défense peuvent être testées rapidement. Les avantages de la navigation magnétique ne font pas l'objet d'un consensus, mais la maîtrise de la signature de bâtiments voire la détection magnétique de cibles maritimes sont à considérer.
- Les capteurs quantiques permettent d'envisager des améliorations majeures en guerre électronique (SIGnal INTelligence). Les technologies envisagées sont les cellules à gaz (atomes de Rydberg), les centres NV, les cristaux dopés aux ions terre-rare et les antennes supraconductrices à interférence quantique (SQUIDS/SQIFs). L'appréciation des performances d'un capteur RF est complexe : la bande passante d'accord, la bande passante instantanée, la dynamique, la sensibilité et le bruit sont les facteurs essentiels, en plus du SWaP-C. Les capteurs quantiques actuels présentent

---

<sup>1</sup> Size Weight and Power - Cost

déjà des niveaux de performances exceptionnels pour certaines de ces caractéristiques. Des travaux sont nécessaires pour couvrir l'ensemble des spécifications.

A noter que le domaine des senseurs optroniques (passifs et actifs) pourrait également bénéficier de l'apport des technologies quantiques, mais le niveau de maturité actuel et celui des démonstrations est plus incertain, du moins à échéance de 5 ans. De fait, ce domaine ne fait pas l'objet d'une recommandation particulière à court terme. A noter également que les composants qui seront développés pour le domaine des communications quantiques (QIN, QKD,..) bénéficieront à celui de l'optronique (et vice-versa) (par ex. compteurs de photons, sources de photons intriqués,..).

Au fur et à mesure que des prototypes embarquables de capteurs quantiques seront disponibles, leur intégration dans des équipements et systèmes d'intérêt GIFAS pourra être mise en œuvre ce qui devrait prendre quelques années supplémentaires afin de transformer l'avantage « capteurs » en avantage « système ». A cet égard, le fait de disposer prototypes embarquables devrait stimuler fortement le développement de ces aspects « système ».

Il convient de rappeler que les coûts de développement des technologies croissent avec leur maturité, et que le coût de la réalisation d'un capteur même industrialisé reste faible vis-à-vis de la réalisation d'un système. Dans ce contexte, les investissements nécessaires au développement des capteurs quantiques peuvent apparaître modérés au regard de leurs enjeux stratégiques.

## 1.2 Descriptif et cas d'usage

Une définition couramment admise pour un capteur quantique<sup>2</sup> est : « un capteur quantique est un instrument de mesure qui recourt à des phénomènes de nature quantique pour mesurer une grandeur physique. Les capteurs quantiques utilisent des effets quantiques comme la superposition ou les interférences pour atteindre une très haute sensibilité ou stabilité long terme, dépassant celle des dispositifs classiques. »

De nombreux capteurs actuellement disponibles répondent à cette définition. Ils sont issus de la première révolution quantique qui découla des premières mises en œuvre de la mécanique quantique. Ils sont nombreux et utilisés même dans des objets destinés au grand public. Pour n'en citer qu'un, les capteurs CMOS qui équipent tous les téléphones et appareils photographiques numériques sont une mise en œuvre de l'effet photoélectrique.

Une seconde révolution quantique est en cours. Cette nouvelle révolution porte une nouvelle génération de capteurs, profitant entre autres des avancées de la première révolution maintenant qui sont matures industriellement (*e.g.* laser semi-conducteur, diodes réceptrices de photon à avalanche, électronique très faible bruit). C'est un cercle vertueux technologique, les capteurs de nouvelle génération bénéficiant des acquis technologiques de la précédente.

Le groupe s'est donc concentré sur les projets de capteurs quantiques de nouvelle génération. Vingt-deux couples technologie-application ont été considérés et instruits.

Le groupe n'en a retenu que quinze après application des critères suivant :

---

<sup>2</sup> Voir par exemple : C. Degen, F. Reinhard et P. Cappellaro, *Quantum sensing*, *Reviews of modern physics* **89** (3), 035002 (2017).

- L'applicabilité à l'aéronautique ou la défense, en particulier l'espoir de pouvoir à terme les embarquer et le gain applicatif attendu vis-à-vis de l'état de l'art ;
- La maturité technologique et par voie de conséquence l'effort de développement à consentir avant une mise en œuvre opérationnelle.

Le résultat de ce panorama et de cette sélection, classé par principe technologique, est :

### **Atomes Froids**

- Gravimètre atomique embarquable
- Accéléromètre et gyromètre atomiques (chute libre)
- Accéléromètre et gyromètre atomiques (piégé sur puce)
- Gradiomètre atomique (en chute libre)

### **Cellules à gaz pompés**

- Capteurs RF à atomes de Rygberg
- Maîtrise de la signature magnétique des bâtiments
- Horloges atomiques et synchronisation de ressources

### **Centres NV**

- Analyse de signaux RF
- Contrôle Non Destructif
- Navigation magnétique

### **Cristaux dopés aux ions terre-rare**

- Analyse spectrale RF très large bande et multiségnal (via transposition en optique)

### **Circuits Supraconducteurs**

- **Antennes Supraconductrice à Interférence Quantique (ASIQ) (réception RF et MAD)** Chaque technologie, ses avantages, son potentiel, les efforts à consentir sont décrits dans ce qui suit.

## **1.2.1 Atomes froids**

### **Quelques généralités sur les atomes froids**

La technologie des atomes froids a été mise au point en laboratoire dans les années 1980. Elle a notamment valu le prix Nobel de physique au français Claude Cohen-Tannoudji en 1996. Concrètement, un dispositif à atomes froids se compose d'une enceinte à vide (typiquement une cellule en verre ou une enceinte en titane avec des hublots) dans laquelle est injectée un gaz de l'espèce d'atome que l'on souhaite refroidir (typiquement du rubidium, du césium ou du strontium, même si de nombreuses autres espèces ont également été refroidies avec cette technique). Le processus de piégeage et de refroidissement des atomes s'effectue ensuite par la pression de radiation exercée par six faisceaux laser (deux contrepropageants dans chaque dimension de l'espace) qui s'opposent aux mouvements des atomes. Il en résulte une « boule » d'atomes localisée à l'intersection des faisceaux lasers, dont la vitesse quadratique résiduelle  $v^2$ , très faible, peut être associée à une température  $T$  (exprimée en Kelvins) par la formule  $mv^2=kT$  où  $m$  est la masse de l'atome et  $k$  la constante de Boltzmann. Typiquement, une source primaire d'atomes froids, appelée piège magnéto-optique, contient de l'ordre de  $10^8$  atomes à une température de l'ordre du milliKelvin. Il est important de rappeler ici que l'ensemble des équipements qui composent un dispositif à atomes froids sont à température ambiante, seuls les  $10^8$  atomes

piégés dans l'enceinte à vide étant refroidis par les lasers. En particulier ces dispositifs ne nécessitent aucun moyen cryogénique. L'intérêt de ces dispositifs à atomes froids est qu'ils permettent d'avoir accès aux propriétés quantiques des atomes, ces derniers étant très bien isolés de leur environnement et très bien contrôlés en vitesse et en position. Cette technologie constitue une base commune aux calculateurs quantiques à atomes de Rydberg (tels que développés par la société Pasqal) et aux capteurs quantiques fondés sur l'interférométrie atomique décrits dans ce qui suit.

### Principes communs aux capteurs inertiels à atomes froids

Une fois les atomes piégés et refroidis par laser, il est possible d'avoir accès expérimentalement à l'onde de matière associée à chaque atome par la mécanique quantique. Cette onde décrit l'amplitude de probabilité associée à la position de chaque atome (l'atome n'étant plus localisé en un point de l'espace comme en mécanique classique mais « délocalisé » sur un certain volume d'autant plus grand que l'atome est froid). Le principe de l'interférométrie atomique est de laisser les atomes se propager selon des chemins différents (plus précisément de faire en sorte que chaque atome se trouve dans la superposition quantique de deux états qui suivent des chemins différents). Quand les chemins se recombient, les ondes de matière s'additionnent et donnent lieu à des interférences permettant de mesurer la phase relative accumulée entre les deux chemins. C'est cette phase qui, en fonction des configurations, peut être rendue très sensible à la gravité, aux accélérations et aux rotations, permettant d'effectuer des mesures inertielles avec ces dispositifs. Elle est habituellement mesurée par fluorescence, en comparant les populations relatives de deux états internes de l'atome. Si les avantages apportés par l'utilisation de l'interférométrie atomique par rapport aux autres types de capteurs inertiels dépendent du type d'implémentation et des applications visées, on peut tout de même citer ici deux grands principes marquants. Le premier est la possibilité d'effectuer des **mesures absolues**, au sens où le facteur d'échelle du capteur peut être relié aux propriétés intrinsèques de l'atome qui sont invariantes dans le temps et l'espace, permettant de supprimer la nécessité de calibration qui existe sur d'autres types de capteurs et garantissant que les performances des capteurs atomiques ne se dégradent pas avec le temps. Le deuxième est la **très grande sensibilité** potentielle des capteurs atomiques dont l'illustration la plus marquante concerne la mesure de rotation par effet Sagnac. En effet, pour une même vitesse de rotation et une même aire inscrite dans l'interféromètre, le déphasage Sagnac pour un interféromètre atomique est 100 milliards de fois supérieur à celui d'un interféromètre optique (type gyromètre à fibre optique). Plus précisément, le rapport entre les facteurs d'échelle est donné par le rapport entre l'énergie de l'atome ( $mc^2$ ) et l'énergie du photon ( $h\mu$  où  $h$  est la constante de Planck et  $\mu$  la fréquence), qui vaut environ  $10^{11}$  pour un atome de rubidium et une fréquence optique. Même si en pratique on ne retrouve pas cet avantage de 11 ordres de grandeur sur les gyromètres atomiques par rapport aux gyromètres optiques car ils sont en partie compensés par un désavantage sur le rapport signal à bruit et sur la taille de l'interféromètre, cela illustre tout de même le potentiel de ces capteurs en terme de sensibilité, le même argument étant également valable dans une certaine mesure pour les gravimètres et les accéléromètres atomiques.

### Gravimètre atomique embarquable

Le principe du gravimètre atomique est de laisser tomber les atomes (une fois refroidis) en chute libre et d'utiliser une série d'impulsions laser verticales pour mettre chaque atome dans la superposition de deux états suivant deux trajectoires différentes (l'un des états tombant un peu plus vite que l'autre). Le déphasage mesuré est proportionnel à  $gT^2/\lambda$  où  $g$  est le champ de pesanteur à mesurer,  $T$  le temps de chute des atomes et  $\lambda$  la longueur d'onde du laser. Ces deux dernières quantités pouvant être reliées aux propriétés fondamentales de l'atome (fréquence de transition entre deux niveaux hyperfins de l'état fondamental) par des techniques d'asservissement, on obtient une mesure absolue de  $g$  sans ca-

libration de l'instrument. Une technique développée par l'ONERA pour réaliser des mesures embarquables (c'est-à-dire dans des porteurs en mouvement) consiste à utiliser une plateforme gyrostabilisée pour maintenir la tête de capteur à la verticale malgré les mouvements du porteur. Cette technique a permis de réaliser des mesures en mer et aéroportées (avec des niveaux de sensibilité et d'exactitude de l'ordre du  $\mu\text{g}$ ). L'application la plus prometteuse identifiée à ce stade est l'établissement de cartes de l'anomalie de pesanteur, qui pourront ensuite servir par exemple à de la navigation par corrélation de terrain. Récemment, l'ONERA a obtenu un contrat du ministère des Armées pour fournir, en co-développement avec Exail, plusieurs exemplaires de gravimètres à atomes froids pour équiper les bâtiments du SHOM (service hydrographique et océanographique de la marine). L'avantage opérationnel principal est l'absence de nécessité de calibration. Un deuxième avantage est un gain en sensibilité d'un facteur 2 environ par rapport aux gravimètres classiques habituellement utilisés pour ce type d'application (gravimètre à ressort type KSS32-M). Les gravimètres à atomes froids embarquables actuellement développés ont un volume total de l'ordre du  $\text{m}^3$  (incluant l'ensemble des lasers et de l'électronique nécessaires), une consommation de l'ordre du kW et une masse de l'ordre de 200kg (incluant la plateforme gyrostabilisée). Des recherches<sup>3</sup> en cours en vue de réduire l'encombrement incluent la possibilité de se passer de la plateforme gyrostabilisée dans certains environnements ainsi que la réduction de la partie électronique et optique (possiblement en optique intégrée, voir section 4). Les technologies associées incluent les techniques du vide (pompe ionique, getter, dispenser...), l'optique (lasers RIO à 1560nm actuellement achetés aux USA, cristaux doubleur type PPLN guide d'onde actuellement achetés au Japon), l'électronique bas bruit en DC, RF (100MHz) et MW (6.8GHz).

Acteurs principaux : ONERA, Exail, Vector Atomic, Atomionics, Nomad Atomic + nombreux laboratoires académiques.

### **Accéléromètre et gyromètre atomiques (chute libre)**

Le principe du gravimètre atomique exposé précédemment peut être étendu à la mesure des accélérations et des rotations. En fonction de l'orientation des lasers et de la séquence temporelle mise en œuvre, il est ainsi possible, au cours de la chute, de séparer les chemins suivis par les deux états de chaque atome verticalement, pour être sensible à l'accélération verticale, ou selon une boucle, pour être sensible à la rotation autour de la normale à cette boucle comme pour un gyromètre optique à effet Sagnac. Des démonstrations de telles mesures ont été effectuées en laboratoire sur des appareils statiques. Les performances atteintes pour la mesure des accélérations transverses sont de l'ordre de 200ng (à comparer à une fraction de ng pour la mesure de g ou de l'accélération verticale avec un gravimètre à atomes froids de laboratoire statique). Pour les performances en terme de mesure des rotations, on peut citer l'expérience de Kasevich en 2000 qui a atteint une sensibilité de 0.6 nrad/s/racine(Hz) soit 2  $\mu\text{deg}/\text{racine}(\text{hr})$  avec un jet d'atomes. Une expérience plus récente et plus compacte du SYRTE affiche 30 nrad/s/racine(Hz) soit  $10^{-4}$  deg/racine(hr) avec une stabilité long terme de 0.3 nrad/s soit  $6 \cdot 10^{-5}$  deg/hr. D'importants efforts de recherche sont en cours pour tenter de rendre ces capteurs embarquables et suffisamment compacts sans dégrader leurs performances. En cas de succès, l'application principale pourrait être la navigation inertielle de haute précision sans GPS. Toutefois les difficultés techniques liés à ces capteurs ainsi que les très bonnes performances des capteurs classiques concurrents (gyromètres à fibre optique, gyromètres vibrants par exemple) rendent incertaine l'émergence à court terme de cette application.

Acteurs principaux : ONERA, SYRTE et d'autres laboratoires académiques à travers le monde.

---

<sup>3</sup> À noter que dans les deux cas des alternatives européennes sont envisageables dans la mesure où ces deux technologies y sont maîtrisées au même niveau qu'aux USA et au Japon. C'est plus une question d'opportunité de marché que de maîtrise technologique.

### **Accéléromètre et gyromètre atomiques (piégé sur puce)**

Le principe des accéléromètres et gyromètres piégés sur puce consiste à garder les atomes piégés à l'aide d'une puce, appelée puce atomique, pendant toute la durée de la mesure. Ainsi les atomes ne sont plus en chute libre pendant la mesure permettant de réduire drastiquement la taille du capteur. La séparation spatiale des deux états atomiques utilisés pour la mesure est alors réalisée par une séquence de différents pièges. Pour réaliser un accéléromètre, les deux états sont séparés suivant une trajectoire rectiligne, l'accéléromètre mesure alors une différence d'énergie potentielle d'accélération. Pour réaliser un gyromètre, les deux états sont déplacés dans deux sens contraires le long d'une trajectoire fermées incluant une aire permettant de mesurer l'effet Sagnac. L'objectif de ces développements est la compacité (de l'ordre du litre), comparable aux centrales inertielles actuelles, tout en permettant de meilleures sensibilité et stabilité pour les mesures d'accélération et de rotations ( $0,1 \mu\text{g}$  et  $0,1 \text{ mdeg/h}^{1/2}$ ) que les dispositifs classiques. L'application visée est la navigation inertielle long terme sans GPS. D'importants efforts de recherche sont en cours pour atteindre ce niveau de performance et de compacité. Plusieurs technologies sont requises comme les circuits photoniques intégrés pour la réalisation de la source laser nécessaire au refroidissement et à la détection des atomes mais aussi pour la réalisation de pièges magnéto-optiques compacts ou encore la fabrication des puces atomiques et leur intégration sur des enceintes à vide de tailles réduites.

Acteurs principaux : THALES, SYRTE et d'autres laboratoires académiques à travers le monde.

### **Gradiomètre atomique (en chute libre)**

Il est également possible, sur le principe des accéléromètres à atomes froids en chute libre, de réaliser des gradiomètres atomiques. Pour cela l'approche typique consiste à utiliser deux boules d'atomes froids séparées spatialement par un même laser permettant d'effectuer des mesures de  $g$  en deux points séparés avec une référence commune (ce qui permet d'augmenter encore la sensibilité par rapport à deux gravimètres). Les expériences de laboratoire ont pu démontrer des niveaux de stabilité de l'ordre de quelques Eotvos ( $1\text{E}=10^{-9} \text{ s}^{-2}$ ). Les applications potentielles de la gradiométrie concernent la navigation par corrélation de terrain (en complément des centrales inertielles) et la détection de structures enfouies. Une limitation majeure toutefois est que la plupart des applications nécessitent la mesure des 6 composantes du tenseur gradiométrie

$$(dg_x/dx, dg_x/dy, dg_x/dz, dg_y/dy, dg_y/dz, dg_z/dz)$$

alors que les démonstrations actuelles ne mesurent qu'une ou deux composantes particulières. A noter que la société Exail développe actuellement une version transportable de gradiomètre à atomes froids. Sa mise en œuvre correspond schématiquement à celle de deux gravimètres en chute libre, placés l'un au-dessus de l'autre. Ils partagent l'ensemble des lasers et asservissements et donc seule la « colonne » de chute est typiquement deux fois plus haute, dans un volume global qui reste celui du  $\text{m}^3$ .

## **1.2.2 Cellules à gaz pompées**

### **Capteurs RF à atomes de Rydberg**

Cela fait maintenant une cinquantaine d'années que les atomes de Rydberg, qui sont des atomes avec un très grand nombre quantique principal  $n$ , ont attiré l'attention des scientifiques. La grande taille de ces atomes (proportionnelle à  $n^2$ ), et donc un moment dipolaire potentiellement élevé, ont suscité un



intérêt d'abord fondamental, les propriétés de ces atomes permettant par exemple d'étudier des phénomènes de décohérence<sup>4</sup>.

La détection de champs micro-ondes se base sur une mesure optique sur une cellule de gaz atomique (Rubidium ou Cesium) en utilisant des lasers d'interrogation (lasers de pompe et de sonde). La détection se fait par la mesure du signal de transparence électromagnétiquement induite (EIT) établi dans le système atomique<sup>5</sup>. Si l'état de plus haute énergie est un état de Rydberg, couplé à d'autres états par un signal RF, le phénomène EIT<sup>6</sup> est alors perturbé : il se dédouble par effet Autler-Townes et on obtient deux résonances EIT au lieu d'une. Ainsi, la mesure de l'amplitude ou de l'intensité du champ RF à détecter se fait au moyen d'une mesure de fréquence (l'écart séparant les deux résonances EIT).

Comparées aux antennes dipôles métalliques actuellement utilisées pour ce genre d'applications, les cellules diélectriques d'atomes de Rydberg, fonctionnant à température ambiante, permettent d'envisager des mesures indépendantes de la longueur d'onde, précises, avec de très grandes sensibilité ( $1 \mu\text{V}/\text{m}/\text{VHz}$ ) et dynamique (120 dB), une stabilité intrinsèque et une auto-calibration et une large bande d'accord pouvant fonctionner de 1 GHz à 500 GHz en ajustant la longueur d'onde d'un des lasers. De plus, la partie sensible du capteur est purement diélectrique et ne perturbe par conséquent pas le champ à mesurer. L'encombrement visé pour ce type de dispositif est de quelques  $\text{cm}^3$  pour le capteur et quelques décilitres pour les lasers et la détection optique.

La détection de la phase du champ électrique nécessite actuellement d'ajouter une antenne émettrice d'un oscillateur local qui peut par exemple perturber le fonctionnement d'une antenne. Des investigations sont actuellement menées afin de pouvoir mesurer cette phase en effectuant des mesures tout optiques. Des travaux sont à réaliser pour concevoir des cellules fibrées déportées optiquement du bloc opto-électronique. Les lasers compacts, stables et agiles dans le visible constituent une technologie habilitante pour ce type de capteurs.

Les principaux acteurs sont Thales, Rydberg Technology (USA), Quantum Valley (Ca), le NIST et l'université de Stuttgart. Des prototypes sont déjà disponibles. A noter que certains acteurs dont l'ONERA étudient également l'apport de la technologie des atomes froids aux capteurs de champ électromagnétiques à atomes de Rydberg, pour des applications où la résolution et la stabilité à long terme (auto-calibration) sont importantes.

### **Maîtrise de la signature magnétique de bâtiments**

On peut schématiser les dispositifs à vapeurs atomiques comme étant l'assemblage de trois fonctions : une source de lumière polarisée excitatrice (laser), une cellule de gaz, et un système de détection. Les espèces d'atomes habituellement choisies pour constituer le gaz sont des métaux alcalins (potassium, rubidium ou césium). En effet, ceux-ci ont une faible température de fusion qui permet d'atteindre facilement l'état gazeux, et les différences entre leurs niveaux d'énergie correspondent à des fréquences de lumière excitatrice pour lesquelles la technologie laser est parfaitement maîtrisée. L'utilisation d'hélium-4 est également envisagé, celui-ci étant déjà dans l'état gazeux à température ambiante. Quel que soit le type d'atomes choisi, ceux-ci sont placés dans une cellule dont la température est portée au-delà de leur température de fusion. Le gaz ainsi obtenu est plongé dans un champ magnétique et éclairé par un laser de polarisation et de fréquence adaptées de manière à ce que les électrons de valence des

---

<sup>4</sup> J.M. Raimond, M. Brune et S. Haroche, Colloquium: Manipulating quantum entanglement with atoms and photons in a cavity, *Rev. of Mod. Physics*, 73, 565 (2001).

<sup>5</sup> J. A. Sedlacek, A. Schwettmann, H. Kübler, R. Löw, T. Pfau et J. Shaffer, Microwave electrometry with Rydberg atoms in a vapour cell using bright atomic resonances, *Nature Phys.*, 8, 819 (2012).

<sup>6</sup> Electromagnetically Induced Transparency

atomes le composant atteignent un état d'énergie excité en absorbant les photons incidents. Leur désexcitation peut les ramener soit à l'état fondamental initial soit à un état fondamental de nombre quantique plus faible. Un régime s'établit progressivement dans lequel chaque électron est périodiquement désexcité, puis repoussé vers l'état d'excitation précédent par l'absorption régulière de photons jusqu'à ce qu'il se fixe dans l'état le plus faible<sup>7</sup>. Différentes méthodes peuvent être utilisées pour relier l'évolution de l'absorption du laser incident par la cellule (ou d'un laser secondaire) à la variation de la norme du champ magnétique. Dans le cas d'une mesure qui n'est pas réalisée en champ nul, le phénomène de résonance magnétique est exploité : l'application d'un champ radiofréquence provoque une remontée des électrons dans l'état fondamental initial et crée une oscillation mesurable dans l'absorption du laser exciteur lorsqu'il est de nouveau sollicité. En scannant les fréquences RF, une résonance correspondant à la vitesse maximale de déplétion de l'état faible donne une lecture directe de la norme du champ magnétique extérieur. En fonction du type d'atomes utilisés, il existe des contraintes plus ou moins fortes sur l'intensité minimale et l'orientation du champ détectable. Dans le cas de la vapeur d'hélium-4, des travaux exploitent des techniques de modulation qui dégradent la précision et la bande passante, au profit d'une estimation vectorielle du champ.

Une source de variation du champ magnétostatique est la présence d'un bâtiment de guerre non immunisé, celui-ci étant composé de matériaux ferromagnétiques denses. Dans le cadre de la détection aéroportée d'anomalies magnétiques réalisée par les patrouilleurs maritimes en France, un avion sonde une zone avec son MAD<sup>8</sup>. Les ATL2 sont actuellement dotés d'un capteur scalaire de type Overhauser basé sur la résonance magnétique nucléaire (RMN). Une application des magnétomètres à pompage optique serait d'augmenter la précision (et donc la portée) de la mesure pour la détection en champ lointain, par l'installation d'un réseau de capteurs de sorte à éviter tout cône d'angle mort de mesure et à obtenir un gain de sensibilité entre 1 et 3 ordres de grandeur. Ces technologies, essentiellement portées par la communauté des géophysiciens, sont pour l'instant disponibles sur le marché, chez des fournisseurs américains, anglais ou canadiens. Il n'existe pas de point dur pour déployer ces capteurs en base fixe ou en embarqué, mais quelques efforts de conception sont nécessaires pour les faire évoluer vers des besoins d'intégration système et de robustesse aux conditions opérationnelles. La grande maturité de ces capteurs en fait une solution d'évolution rapide des capacités de détection, qui pourraient ensuite laisser place à la génération suivante de capteurs vectoriels (centres NV, SQIF). Aucun fournisseur industriel français n'a émergé pour l'instant, bien que le CEA-LETI ait poussé cette technologie jusqu'à un TRL >7, le problème de l'encombrement total restant un frein important à l'embarquabilité en aéroporté.

### **Horloges atomiques et synchronisation de ressources**

Le principe des horloges atomiques réside dans l'utilisation d'une transition atomique entre deux niveaux d'énergies  $E_1$  et  $E_2$  (ex : Césium Cs, Rubidium Rb ou même Hydrogène H). Ces niveaux étant quantifiés en énergie, le passage de l'un à l'autre état n'est possible qu'au travers de l'absorption d'ondes électromagnétiques de fréquence  $\nu_{12}$  qui satisfait la relation  $E_1 - E_2 = h \nu_{12}$ ,  $h$  étant la constante de Planck. Ces niveaux d'énergie ne dépendent que des caractéristiques physiques de l'atome, ceci confère à la transition atomique  $\nu_{12}$  une stabilité extrême.

Le schéma classique d'une horloge atomique exploite cette caractéristique asservissant la fréquence d'un oscillateur classique (ex : OXCO<sup>9</sup>, TCXO<sup>10</sup>) sur la fréquence de transition atomique  $\nu_{12}$  (9.2 GHz pour le césium) au travers d'une boucle d'asservissement telle que l'illustre le schéma suivant :

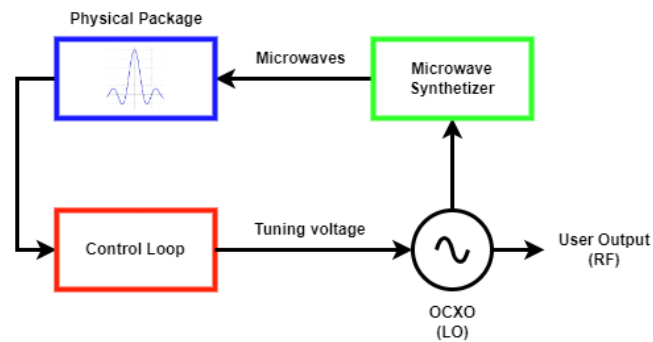
---

<sup>7</sup> Principe de fonctionnement très proche des horloges atomiques

<sup>8</sup> Magnetic Anomaly Detector

<sup>9</sup> Oven Controlled X-tal (Crystal) Oscillator

<sup>10</sup> Temperature Compensated X-tal (Crystal) Oscillator



L'OCXO, délivrant une fréquence  $\nu$ , pilote un générateur microondes qui génère une onde électromagnétique de même fréquence sondant la vapeur d'alcalin. Une photodiode en sortie de la cellule mesure l'absorption d'un laser incident. Ce taux d'absorption dépend de l'écart en fréquence  $\delta = \nu - \nu_{12}$  et atteint un extremum lorsque  $\delta=0$ , c'est-à-dire quand  $\nu=\nu_{12}$ . La boucle d'asservissement sert à obtenir cette condition sur le signal de détection en pilotant la fréquence de l'OXCO.

Dans les horloges atomiques de type CSAC (Chip Scale Atomic Clock) notamment, le principe de « coherent population trapping (CPT) » est exploité. Ce phénomène est obtenu par l'irradiation de la cellule par un seul et même laser splitté en deux faisceaux et dont l'écart en fréquence est modulable. Lorsque l'écart en fréquence entre les deux faisceaux est égal à  $\nu_{12}$ , correspondant à la transition de l'horloge, l'absorption par la vapeur d'atome devient nulle. C'est la condition recherchée par la mise en œuvre, pilotant l'écart en fréquence, pour caler la fréquence de l'OXCO sur la transition atomique.

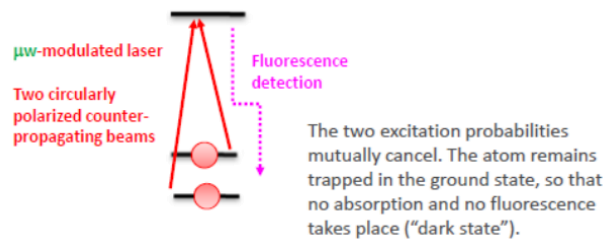
**Double optical-microwave resonance:**

$\mu\text{w}$  cavity needed



**Coherent population trapping:**

$\mu\text{w}$ -modulated laser needed



L'exploitation de ce phénomène est très avantageuse car il permet d'éviter l'utilisation du générateur micro-ondes améliorant ainsi la compacité et diminuant la consommation le tout permettant de minimiser le CSWAP<sup>11</sup>.

Le principal avantage de cette technologie est donc de pouvoir être miniaturisée très fortement. Pour les solutions ultra-compactes, les cellules peuvent être réalisées sur les lignes technologiques silicium et peuvent ainsi conduire à des MEMS dont les coûts chutent drastiquement avec les quantités. Le SWAP est également considérablement réduit ce qui permet d'ouvrir à de nouvelles applications notamment portables.

Les applications visées sont toutes celles nécessitant une synchronisation bien meilleure qu'une résonateur quartz mais ne requérant pas une horloge haute performance comme les technologies déflexion magnétique Césium ou MASER. Les performances de stabilités visées sont pour les développements à insertion courte sur le marché de l'ordre de  $1\mu\text{s}$  par 24h et jusqu'à quelques ordres de grandeur de mieux pour les développements qui visent une insertion à moyen terme (typiquement 1ns par 24h).

<sup>11</sup> Cost Size Weight and Power

Cette stabilité est nécessaire pour les applications suivantes :

- Référence de temps sans GNSS
- Synchronisation de senseurs RF (radars multistatiques, systèmes d'écoute distribués, systèmes de communication...) ou optroniques sans GNSS
- Synchronisation de réseaux informatiques sans GNSS
- Détection d'interférence GNSS (Anti Jamming / Anti Spoofing)

Ces applications adressent de nombreux domaines. En premier lieu, et notamment avec le conflit Ukrainien, l'absence de GNSS et donc de synchronisation temporelle, entraîne un intérêt certain dans le domaine de la défense (Serveurs de temps pour les réseaux et les communications, détection de spoofing GNSS, ...).

Dans le domaine spatial, les constellations de type LEO PNT requièrent une stabilité de référence de temps très bonne pour des tous petits satellites.

Dans le domaine ferroviaire, les infrastructures de signalisation doivent être synchronisées et donc nécessitent des horloges précises pour être robustes à des pertes de GNSS malveillantes.

Dans le domaine terrestre civil, les infrastructures de communications de type 4G/5G nécessitent une synchronisation résiliente à la perte de GNSS.

Dans le domaine maritime, des balises sous-marines peuvent nécessiter une synchronisation en temps sans avoir accès au signal GNSS.

C'est donc tout le domaine industriel, spatial et défense qui est concerné par cette technologie.

Le prérequis de cette technologie est donc de disposer de composants d'un volume de la classe quelques  $\text{cm}^3$ , d'une masse de quelques grammes et consommant suffisamment peu de manière à fonctionner sur batterie pendant plusieurs jours de façon à ce que l'horloge les intégrant soient compatibles des besoins cités.

Les principes physiques et leurs implémentations sont connus. Ces horloges reposent sur les technologies lasers, de fabrication de cellules de vapeurs d'atomes, d'électroniques analogiques, numériques et hyper-fréquences (RF) et de détecteur optique rapide. Les démonstrations actuelles présentent des volumes et consommations de la classe d'un équipement de laboratoire.

Les enjeux sont la validation des performances en volume contraint mais aussi une industrialisation assurant la souveraineté.

En ce qui concerne les micro-horloges, un premier niveau d'effort est en cours et doit permettre d'atteindre un produit répondant aux besoins d'ici 3 ans. Toutefois, compte tenu du champ d'application (notamment portable), il semble essentiel de poursuivre la miniaturisation et le niveau d'industrialisation pour obtenir un très haut niveau de compétitivité sur le CSWAP à une échelle de 5 ans. Ces efforts porteront notamment sur la cellule silicium et le passage en ASIC d'électroniques discrètes.

Un troisième niveau d'amélioration doit être également réalisé autour de l'amélioration de la performance. Car la demande en résilience sera de plus en plus élevée. Il sera nécessaire de la maintenir au plus haut niveau de performance. Cela peut demander en fonction des axes d'amélioration (électronique ou cellule) de 3 à 7 ans.

Toutes ces améliorations visent à proposer des solutions en compétition avec l'acteur principal qui est aujourd'hui américain : Il s'agit de MicroChip avec le CSAC (Chip Scale Atomic Clock). Cet acteur utilise une technologie qui a été très fortement soutenue par la DARPA. Au-delà du financement initial que cet

acteur a bénéficié, il profite aujourd’hui de commandes US très importantes permettant un soutien industriel fort.

Les micro-horloges ne permettant pas à elles seules de disposer de solutions souveraines pour l’ensemble des besoins précédemment cités. D’autres développements autour de la technologie CPT sont en cours<sup>12</sup>. Ils bénéficieront partiellement des travaux associés aux micro-horloges (ex : électronique). L’objectif est de disposer d’horloges avec un niveau de performance et de SWAP intermédiaire entre les micro-horloges et autres solutions commerciales françaises basées sur des technologies plus maîtrisées.

Les acteurs principaux en France sur cette technologie sont THALES, Safran Electronic et Defense via sa filiale SYRLINKS, TRONICS, le SYRTE, le FEMTO-ST.

### 1.2.3 Centres NV

Les centres NV sont physiquement des diamants dans lesquels deux atomes de carbone voisins dans la structure cristalline ont été substitués l’un par un atome d’azote et l’autre par un vide créant ainsi un couple azote-vacance. Ces défauts sont intéressants car ils présentent des propriétés quantiques singulières, notamment un temps de cohérence de spin extrêmement long.

Le principe de fonctionnement des centres NV repose sur l’interaction entre le spin des électrons piégés dans le centre et un champ magnétique externe. Un champ magnétique externe modifie l’énergie des états de spin du centre NV. Cela peut être mesuré par une interrogation par un laser vert stimulant la fluorescence du centre NV. Plus précisément, la longueur d’onde de cette fluorescence rouge renseigne sur l’état de spin du centre et indirectement sur le champ magnétique externe.

D’autres contraintes externes peuvent aussi modifier l’état de spin du centre et de fait, les centres NV peuvent être utilisés pour mesurer les paramètres physiques suivant :

- Les champs magnétiques, avec une sensibilité extrêmement élevée.
- Les températures, avec une résolution spatiale nanométrique.
- Les contraintes mécaniques, avec une résolution spatiale micrométrique.
- Les champs électriques, avec une résolution spatiale nanométrique.
- Les courants électriques, avec une résolution spatiale micrométrique.

Les centres NV présentent de nombreux avantages :

- Une mesure absolue, sans calibration ;
- Une sensibilité élevée ;
- Une possibilité d’interrogation et lecture par une fibre optique ;
- Une résistance aux environnements difficiles ;
- Une taille potentiellement nanométrique.
- Une mise en œuvre aisée.

Les centres NV reposent sur quelques technologies :

- Les diamants dopés ;
- Les lasers verts compacts et stables, semi-conducteurs en priorité ;

---

<sup>12</sup> [Quantique : Thales et SYRLINKS, PME rennais, s’associent pour développer des horloges atomiques de nouvelle génération pour applications civiles et militaires | Thales Group + syrlinks - Des horloges atomiques de nouvelle génération avec Thales](#)

- Les photodétecteurs (dans le domaine visible et donc présentant à la fois une grande sensibilité et une grande dynamique) ;
- Les électroniques de commande, de mesure et traitement.

Pour réussir leur mise en œuvre, des précautions doivent être prises pour éviter les contraintes externes parasites (voir plus haut).

### **Analyse de signaux RF**

L'utilisation du centre NV du diamant pour l'analyse spectrale de signaux RF repose sur un encodage spatial de la fréquence de résonance de spin d'un ensemble de centres NV au moyen d'un gradient de champ magnétique. Le contenu spectral instantané d'un signal RF circulant dans une antenne aux voisinage des centres NV est alors directement transposé spatialement sur l'intensité du signal de photoluminescence de l'ensemble de centres NV et peut alors être obtenu au moyen d'une simple image avec une probabilité d'interception de 100% sur la bande spectrale sondée.

L'analyse spectrale des signaux RF par le biais des centres NV repose sur une méthode analogique. La taille de la bande d'analyse spectrale est donnée directement par l'intensité du gradient, le rapport gyromagnétique du centre NV ( $28 \text{ GHz} \cdot \text{T}^{-1}$ ) et la taille de l'ensemble de centre imagée par la caméra sur lequel le gradient est appliqué.

Sa mise en œuvre extrêmement simple ne nécessite aucun traitement de type FFT, ni d'échantillonnage rapide, limitant la consommation énergétique de l'ensemble. D'une part, ce système ne nécessite aucune servitude en termes de cryogénie et fonctionne parfaitement à température ambiante, d'autre part, le gradient magnétique peut être obtenu au moyen d'aimants permanents. La compacité de l'ensemble est ainsi fortement réduite. Cette technique peut être notamment envisagée pour des problématiques de type capteurs embarqués pour le renseignement d'origine électromagnétique (ELINT), sur des porteurs de type drone par exemple.

Un autre aspect important concerne la résistance à l'éblouissement d'un tel analyseur basé sur les centres NV. L'application aux centres NV d'une forte excitation RF se traduit simplement par une saturation du contraste de résonance et par l'élargissement de la réponse spectrale dans le domaine RF des centres en résonance avec le champ RF excitateur sans impacter les centres NV non résonants. Le fonctionnement parallèle de l'analyseur permet donc de préserver la mesure sur les canaux adjacents. Concernant les aspects civils, ce système permet également d'adresser potentiellement le domaine des communications sans fil, dans le domaine de la 5G par exemple.

Une version éclatée à TRL 3-4 de ce système a récemment permis en employant un cristal de diamant commercial faiblement dopé en centres NV avec une taille utile pour l'analyse de  $500 \mu\text{m}$ , un aimant permanent en NdFeB de taille centimétrique comme source de gradient magnétique et une source laser Nd-YAG doublée en continu pour l'illumination de réaliser l'analyse de signaux RF de typiquement quelques MHz à 27 GHz avec une bande d'analyse instantanée jusqu'à 5 GHz et une résolution temporelle de l'ordre de la ms.

Des travaux autour de ce dispositif sont en cours à Thales pour atteindre un TRL 7 à horizon 2028 pour l'analyse temps réel de signaux RF sur une bande de fréquence allant jusqu'à 20 GHz, dans un volume de l'ordre de  $3 \text{ dm}^3$  et une consommation électrique de 30 W.

### **Contrôle Non Destructif (CND)**

Certains contrôles non destructifs sont destinés à détecter des criques à la surface ou légèrement sous la surface de pièces métalliques. La mesure des anomalies de champ magnétique est une méthode de détection possible. C'est le principe de la magnétoscopie ou des courants de Foucault. Plus précisément :

- La pièce est soumise à un champ magnétique extérieur ou à son propre champ ;
- La mesure du champ magnétique à proximité de la surface de la pièce permet de détecter un éventuel champ de fuite ou des variations de champ, symptôme de la présence d'une discontinuité dans le matériau, donc d'une crique.

Cette méthode peut aussi être employée pour la vérification de traitement thermo-chimique, la mesure de corrosion, etc.

La mesure du champ magnétique peut être faite par un centre NV. Vis-à-vis de la performance attendue en CND, le centre NV apporte les avantages suivants :

- Sa faible taille lui permet d'être utilisée sur des géométries complexes ;
- Son très faible bruit en basse fréquence et sa sensibilité améliore la précision de mesure ;
- Sa résistance à l'environnement le rend utilisable dans les ateliers industriels ;
- Sa capacité à effectuer une mesure tri-axiale avec une bonne précision angulaire améliore aussi la capacité de détection.

La technologie est disponible dans des laboratoires industriels pour une démonstration de principe, sa maturité actuelle est faible, estimée à TRL2. 5 ans de travaux seraient nécessaires pour atteindre un TRL suffisant pour un premier déploiement industriel. Ces travaux portent sur d'une part la qualification de la méthode et d'autre part sur la réalisation d'un prototype industriel.

### **Navigation magnétique (et détection d'anomalie magnétique)**

La possibilité pour un sous-marin de naviguer sans GNSS – donc sans dépendance envers un système externe, et sans nécessité de retour régulier à la surface – est importante en matière de stratégie militaire, et la navigation magnétique est l'une des solutions envisageables pour contribuer à un tel objectif. Le principe serait d'avoir, en sus de centrales inertielles de très haute précision et avec une dérive minimale (voir paragraphe sur les accéléromètres et gyromètres atomiques), une mesure tridimensionnelle du champ magnétique ambiant afin de corriger l'erreur résiduelle sur la position du porteur par un recalage sur une carte de champ magnétique préétablie. Pour envisager un tel fonctionnement, il faut disposer de capteurs de champ magnétique de très haute précision, autant pour établir les cartes que pour la navigation en elle-même, et pouvoir disposer ceux-ci en réseau sur le porteur afin d'avoir les données nécessaires pour pouvoir soustraire la signature du porteur à la mesure du champ ambiant. Les magnétomètres à centre NV offrent une mesure tridimensionnelle de haute précision, et leur compacité permet d'envisager la mise en réseau de plusieurs capteurs sur le porteur, ce qui en fait des bons candidats pour cette technologie. A noter que les mêmes caractéristiques des centres NV peuvent être exploitées pour la détection d'anomalies magnétiques (MAD/magnetic anomaly detection), c'est-à-dire pour la détection de masses métalliques perturbant le champ magnétique terrestre environnant. Une telle détection est évidemment de première importance pour la détection de mines enfouies ou immergées ainsi que pour la détection de sous-marins. Les freins potentiels à ces applications sont cependant nombreux. Comme pour la détection MAD, le positionnement des capteurs dans le repère de référence du porteur devra être parfaitement maîtrisé, et l'impact des vibrations, ou des changements de pression ou de température reste à étudier. Le traitement des mesures pour soustraire la signature du porteur est un point dur technologique. Même si on peut l'espérer, il n'est pas avéré aujourd'hui que la sensibilité améliorée de la mesure ait un impact significatif sur la précision du recalage sur carte car on ne possède pas de cartes avec la précision que pourrait offrir les capteurs à centre NV, et il est difficile d'évaluer les ordres de grandeurs des variations locales du champ magnétique que l'on obtiendrait, ainsi que leur stabilité. Les acteurs à suivre concernant cette technologie sont ceux qui travaillent sur le développement de capteurs à centre NV, l'application à la navigation étant pour le moment une application potentielle assez lointaine, et à bas TRL (2). Cette application dépend complètement de la dispo-

nibilité de cartes magnétiques précises et à jour (de responsabilité du SHOM) ou de l'existence d'anomalies géomagnétiques bien référencées – ce qui peut en soi annuler tout avantage opérationnel car de tels points géographiques de recalages pourraient devenir des zones sous surveillance.

De façon générale, les acteurs européens principaux sur cette technologie des centres NV pour les applications présentées ci-dessus sont Thales, Kwan-Tek, Univ. Stuttgart, ENS-Paris Saclay, Diehl, Fraunhofer Inst.

## 1.2.4 Cristaux dopés aux ions terre-rare

### **Analyse spectrale RF très large bande et multisignal (via transposition en optique)**

Cette technologie repose sur la possibilité de creuser un trou spectral (Spectral Hole Burning, SHB) dans les bandes d'absorption des cristaux dopés aux ions de terres rares. Ce trou est créé par l'excitation d'un ensemble d'atomes par un laser. A température cryogénique, ces atomes mettent un temps important pour revenir à leur état fondamental. C'est ce niveau fondamental dépeuplé qui crée un trou dans l'absorption lumineuse du cristal, qui peut alors servir de filtre optique très fin.

Cette propriété les rend particulièrement attractifs pour le traitement large bande de signaux RF. Cette technologie est aussi citée pour la réalisation de mémoires quantiques.

Pour l'exploitation en RF, la première étape consiste à transposer les signaux RF dans le domaine optique via un modulateur électro-optique. Le faisceau ainsi formé traverse un cristal Tm<sup>3+</sup>:YAG refroidi à 3K. Plus précisément, deux architectures principales ont été proposées :

- l'architecture arc-en-ciel, repose sur la programmation de réseaux spectro-spatiaux qui permet de diffracter angulairement le faisceau d'intérêt selon les fréquences RF. Cette architecture est bien adaptée aux besoins de l'ELINT (Electronic Intelligence). On peut atteindre des résolutions temporelles de l'ordre de la microseconde et des résolutions fréquentielles de l'ordre de la dizaine de MHz ;
- dans l'architecture photographique, les signaux RF transposés dans le domaine optique s'inscrivent dans la raie d'absorption inhomogène du cristal. Un laser balayé en fréquence permet de relire les spectres et en particulier les raies d'absorption, avec des résolutions temporelles de l'ordre la milliseconde avec des résolutions fréquentielles de l'ordre de la dizaine de kHz, compatibles des besoins COMINT (Communication Intelligence).

L'avantage de cette technologie est d'assurer des traitements de signaux sur des bandes passantes instantanées supérieures à 20 GHz et des dynamiques multiségnaux supérieures à 60 dB, avec de faible temps de latence, inaccessibles par conversion analogique-numérique directe. Les démonstrateurs transportables actuels sont de deux racks 19 pouces et une consommation électrique de 2.5 kW dimensionnée par la cryogénie.

Les enjeux actuels sont de mutualiser la cryogénie et les lasers pour plusieurs fonctions et/ou plusieurs voies adressant plusieurs antennes, augmentant ainsi les performances (accès à la direction d'arrivée des signaux etc...) tout en réduisant considérablement le volume/consommation par voie et fonction. La cryogénie 2-4K compacte, compatible de porteurs embarqués et optimisée en consommation est une technologie habilitante clé à développer en Europe.

Les acteurs principaux sont S2corporation aux États-Unis et Thales en France.



## 1.2.5 Circuits supraconducteurs

### Antennes Supraconductrice à Interférence Quantique (ASIQ) (réception RF et MAD)

Une antenne supraconductrice à interférence quantique, aussi appelée SQIF (Superconducting Quantum Interference Filter), met l'effet Josephson pour détecter la composante magnétique de l'onde électromagnétique sans résonance. Les antennes résonantes classiques, capte la composante électrique du champ électrique. Pour ces antennes classiques, la taille est proportionnelle à la longueur d'onde captée. De plus, la mise en œuvre de l'effet Josephson est possible jusqu'à plusieurs centaines de GHz. Cela rend les ASIQt fondées sur des composants de type SQUIDs/SQIFs efficaces du régime continu jusqu'à au moins quelques dizaines de GHz, tout en gardant une taille très compacte (quelques cm).

Ces propriétés font des ASIQt des excellents candidats pour :

- la réception de communications stratégiques ;
- la détection de la signature magnétique d'un bâtiment ou sa détection
- l'écoute dans une gamme très large de fréquences, essentielle pour la guerre électronique.

Sa versatilité fait que plusieurs pays travaillent sur ce type de détecteurs, notamment l'Australie, les États-Unis, l'Allemagne et la Chine.

L'emploi d'un matériau supraconducteur à haute température critique ( $T_c$ ) permet un fonctionnement à une température relativement élevée de l'ordre de 70 K, ce qui permet l'utilisation d'une cryogénie « légère » rendant l'antenne embarquable.

Ces matériaux à haute  $T_c$ , principale technologie habilitante ne sont pas totalement matures,. Leur fabrication n'est maîtrisée que par une source commerciale au monde, i.e. Ceraco GmbH, Allemagne. De plus, une antenne SQIF nécessiterait plusieurs milliers d'éléments nanométriques tous identiques. Actuellement, l'amélioration de l'homogénéité et la répétabilité reste le challenge principal. La levée de ce verrou technologique ainsi que l'intégration dans une machine à froid compacte devraient être accomplies dans un horizon de 5 à 7 ans.

## 1.3 Capteurs quantiques, cas d'usage et horizons associés (tableau de synthèse)

Technologie	Cas d'emploi	Echéance
<b>Gravimètre à atomes froids (chute libre)</b>	Etablissement de cartes de pesantEUR pour la navigation par corrélation de terrain, géophysique	Opérationnel, même embarqué sur navires (ONERA-EXAIL-VECTOR ATOMIC). Solution strapdown en cours de développement
<b>Gradiomètre à atomes froids (chute libre)</b>	Détection de structure souterraine, prospection minière, navigation, cartes de gravité	Preuve de principe démontrée en laboratoire pour certaines composantes du gradient seulement, TRL 7 possible en 2028
<b>Accéléromètre et gyromètre à atomes froids (chute libre)</b>	Navigation inertielle, géodésie spatiale	Preuve de principe démontré en laboratoire, TRL 7 possible en 2028
<b>Accéléromètre et gyromètre à atomes froids (sur puce)</b>	Navigation inertielle, potentiellement plus compact et résistant aux accélérations	Preuve de principe en cours de démonstration en laboratoire, TRL 7 possible en 2030
<b>Capteur de champ radiofréquence (MHz - THz) à atomes de Rydberg en cellule de gaz à température proche de l'ambiante</b>	Communications RF, guerre électronique, calibration des équipements RF, contrôle non-destructif par imagerie THz	Prototypes opérationnels pour calibration d'équipements RF disponibles (Rydberg Technologies), autres cas d'usage en cours de développement et par exemple, TRL 7 possible pour l'application RADAR en 2030

<b>Capteur de champ radiofréquence (MHz - THz) à atomes de Rydberg froids</b>	Guerre électronique, calibration des équipements RF, contrôle non-destructif par imagerie THz	Preuve de principe démontrée en laboratoire, cas d'usage en cours de développement
<b>Horloges atomiques compactes - Volume de l'ordre du litre et très hautes performances (supérieures à la journée).</b>	Référence de temps sans GNSS, synchronisation de réseaux informatiques sans GNSS, détection d'interférence GNSS (Anti Jamming / Anti Spoofing)	TRL 5 possible en 2027, TRL 7 possible en 2030
<b>Horloges atomiques compactes (chip-scale) - Volume de l'ordre d'une puce et hautes performances (inférieures à la journée).</b>	Intégrable sur carte en substitution d'un quartz : Synchronisation de senseurs RF (radars multistatiques, systèmes d'écoute distribués, systèmes de communication...) ou optroniques sans GNSS, détection d'interférence GNSS (Anti Jamming / Anti Spoofing)	TRL 4-5 actuel, TRL 7 possible en 2027
<b>Cellules à gaz pompées optiquement</b>	Maîtrise de la signature magnétique de bâtiments et détection de bâtiments par anomalie magnétique (Magnetic Anomaly Detection ou MAD)	Technologie disponible sur le marché (fournisseurs US, Canada, UK, CEA-LETI), TRL 7 atteint en Amérique du nord, efforts intégration système et robustesse aux conditions opérationnelles à poursuivre
<b>Centres NV - Analyse de signaux RF</b>	Guerre électronique. Mesure de la composante magnétique et image du spectre, accordable par variation du champ magnétique	Preuve de principe démontrée en laboratoire, TRL 7 possible en 2030
<b>Centres NV - Magnétométrie</b>	Contrôle Non Destructif par magnétoscopie: détection d'une discontinuité de surface par la détection d'un champ magnétique de "fuite", caractérisation des propriétés mécaniques (dureté, contraintes résiduelles)	Preuve de principe démontrée en laboratoire, intérêt à confirmer
<b>Centres NV - Magnétométrie</b>	Maîtrise de la signature magnétique de bâtiments et détection de bâtiments par anomalie magnétique (Magnetic Anomaly Detection ou MAD). Gains en sensibilité	Preuve de principe démontrée en laboratoire, TRL 7 possible en 2028
<b>Centres NV - Magnétométrie</b>	Aide à la navigation par magnétométrie	L'intérêt démontré est limité
<b>Ions terre-rare dans cristaux (Spectral Hole Burning)</b>	Analyse spectrale très large bande et multiségnal de signaux RF, via une transposition en optique	Preuve de principe démontrée en laboratoire, TRL 7 possible en 2030. Travaux à conduire pour améliorer la dynamique
<b>SQUID - SQIF - Magnétométrie</b>	Maîtrise de la signature magnétique de bâtiments et détection de bâtiments par anomalie magnétique (Magnetic Anomaly Detection ou MAD), très forte sensibilité, fonctionnement actuel à 77 K	Preuve de principe démontrée en laboratoire, TRL 7 possible en 2030
<b>SQUID - SQIF - Réception RF</b>	Guerre électronique, réception de signal large bande (pas d'analyse)	Preuve de principe démontrée en laboratoire, TRL 7 possible en 2030
<b>Gyromètre optique à effet Sagnac augmenté par utilisation d'états quantiques (ex : squeezing)</b>	Navigation inertielle (FOG, GyroLaser)	Preuve de principe en cours de démonstration, intérêt à confirmer
<b>Particules en lévitation laser pour mesure de forces inertielles</b>	Navigation inertielle	Preuve de principe en cours de démonstration, intérêt à confirmer
<b>Imagerie quantique</b>	LIDAR, spectroscopie, ghost imaging, en modes passif ou actif	Preuve de principe en cours de démonstration, intérêt à confirmer

## 1.4 Recommandations

1. Encourager, au niveau national, le soutien au développement des capteurs quantiques notamment dans tous les domaines identifiés : atomes froids, horloges atomiques compactes, magnétomètres haute performance et capteurs électromagnétiques RF
2. Inciter les membres du GIFAS à collaborer activement entre eux et avec les autres parties prenantes à l'élaboration de nouveaux cas d'usage pour tirer le meilleur parti des propriétés uniques des capteurs quantiques
3. Explorer dès maintenant avec ces parties prenantes l'intégration des capteurs quantiques dans des futurs systèmes afin de maximiser la performance système atteignable et d'accélérer cette intégration.
4. Construire pour chacune des technologies habilitantes clés une stratégie d'acquisition pérenne, en s'appuyant sur les synergies avec le calcul et la communication quantiques (voir la partie 4 du rapport, consacrée aux technologies habilitantes) et notamment une cryogénie embarquable (2-4K mais aussi 40-80K), des lasers aux longueurs d'onde nécessaires, compacts et robustes, des masers embarquables, des cellules à gaz, des modules de photonique intégrée. Soutenir le développement d'une ligne pilote européenne dédiée aux circuits photoniques intégrés pour le quantique
5. Identifier et mettre en œuvre les synergies technologiques avec les autres applications du calcul et communication quantique.

(page laissée intentionnellement blanche)

## 2. Communications quantiques

### 2.1 Résumé aux décideurs

Les communications quantiques sont une technologie qui concerne les membres du GIFAS en tant que fabricants/intégrateurs et non simplement en tant qu'utilisateurs

Il existe deux types de systèmes – les plus ambitieux sont des réseaux qui transportent de l'information quantique entre ordinateurs ou capteurs quantiques. Moins ambitieux et plus mûrs sont ceux qui permettent une sécurisation des liens d'un réseau qui communiquent par ailleurs par des moyens classiques.

La mise en réseaux de dispositifs quantiques va permettre d'une part leur accès à des utilisateurs qui ne pourraient se les offrir, mais va surtout décupler les performances de ces objets.

C'est un sujet d'infrastructure, qui ne prend son sens que s'il est déployé à grande échelle – il a besoin d'autres moyens d'investissement que ceux nécessaires pour les calculateurs quantiques.

A terme, le marché sera dual, et les acteurs qui tiendront la corde seront ceux qui auront été le plus supportés tôt et sur le long terme par des acteurs institutionnels.

La Chine a une avance considérable, et il faut se donner des objectifs ambitieux financés au bon niveau pour permettre de rejoindre le peloton de tête que nos compétiteurs asiatiques mènent.

Une feuille de route industrielle en plusieurs étapes est disponible, ainsi que la liste des technologies à faire murir pour permettre à la France et à l'Europe de rester dans le peloton de tête de ce domaine.

Le premier objectif est de déployer un système 'QINSAT' de démonstration de la distribution de la ressource d'intrication depuis l'orbite basse vers deux stations sol, puis dans un second temps d'enchaîner plusieurs liens réseau.

Contrairement aux autres domaines des technologies quantiques (capteurs, calcul et technologies habilitantes) pour lesquels la grande diversité des technologies et des applications ne permet un chiffrage global de l'effort nécessaire, il est possible dans le cas des communications quantiques d'estimer financièrement le coût de la mise en œuvre des actions proposées. Le montant estimé pour ce projet est de **120M€ sur 5 ans** pour l'équipe de France industrielle et académique, pour lequel il est souhaitable que la stratégie nationale d'accélération des technologies quantiques contribue à hauteur de **60M€**, les autres financements venant de l'Europe, et des autres agences de R&D nationales.

### 2.2 Contexte et cas d'usage

#### Communication quantiques

On désigne par *communications quantiques* un ensemble de technologies qui exploitent les propriétés offertes par la physique quantique dans le monde des télécommunications. Communiquer signifie transférer de l'information d'un endroit à un autre. L'objet des communications quantiques est principalement de transférer de *l'information quantique* d'un endroit à un autre.

L'information quantique est la ressource que produisent et manipulent les ordinateurs quantiques et certains capteurs quantiques. Pouvoir transférer une telle information ouvre la porte à la mise en réseau de tels dispositifs. Ce qui motive la mise en réseau est l'important accroissement de performance qu'une telle mise en réseau permettra, mais aussi la démocratisation de l'accès des utilisateurs à de tels dispositifs. En outre, de par les propriétés fondamentales de la physique quantique, ces communications sont confidentielles par construction, ce qui apporte un nouvel ingrédient au monde des communications sécurisées.

On va distinguer dans ce document deux catégories de technologies de communications quantiques : les *réseaux d'information quantique* (RIQ, en anglais Quantum-information networks QIN) et les *réseaux sécurisés par voie quantique* (RSQ, en anglais quantum-secured networks, QSN). Ce sont des applications de niveau de maturité, mais aussi d'enjeux très différents. Il faut par contre noter qu'un grand nombre de leur technologies élémentaires sont communes aux deux catégories, et qu'avancer sur l'une fait avancer sur l'autre.

### Réseaux d'information quantique (RIQ)

Les réseaux d'information quantique proposent d'exploiter toutes les possibilités que la physique quantique met à disposition, c'est-à-dire transférer de l'information quantique d'un endroit à un autre. L'information quantique est ce qui permet de décrire l'état d'un système quantique. On sait que lorsqu'on mesure une quantité sur un système quantique (par exemple son énergie ou sa polarisation) si le mécanisme de mesure forme un contexte qui est incompatible avec le contexte dans lequel le système a été préparé, les résultats de mesure sont aléatoires et l'on ne peut prédire que les probabilités de chaque résultat de mesure. Par exemple, si un photon est préparé dans un état de polarisation verticale, et qu'on cherche à mesurer les composantes diagonale ou anti-diagonale de sa polarisation, les probabilités de ces deux issues vont être 50%. Ceci se formalise en disant que l'état vertical  $|V\rangle$  est la combinaison linéaire des états diagonal  $|D\rangle$  et anti-diagonal  $|A\rangle$  :

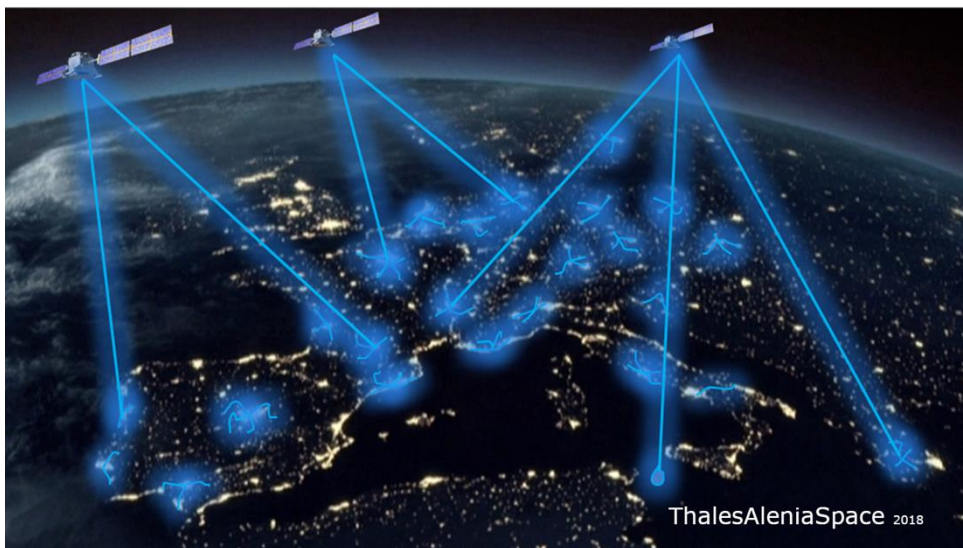
$$|V\rangle = (|D\rangle + |A\rangle)/\sqrt{2}$$

L'information quantique ici est que la composante sur  $|D\rangle$  est  $+1/\sqrt{2}$  et sur  $|A\rangle$  également  $+1/\sqrt{2}$ . Les probabilités sont le module au carré de ces facteurs.

Cette information est ce que les ordinateurs quantiques et certains capteurs quantiques vont produire et manipuler pour calculer ou mesurer (les états  $|H\rangle$  et  $|V\rangle$  peuvent être vus comme des états de base de q-bits,  $|0\rangle$  et  $|1\rangle$ , et l'état  $|D\rangle$  comme le résultat de l'application de la porte logique de Hadamard sur un q-bit dans l'état  $|V\rangle$ ). Le fonctionnement des ordinateurs quantiques indique que leur puissance de calcul croît comme l'exponentielle du nombre de qbits qu'ils peuvent utiliser. On voit donc rapidement qu'associer deux tels ordinateurs en réseau ne va pas additionner, mais bien multiplier entre elles leur puissances de calcul. De façon similaire, mettre  $N$  capteurs quantiques en cohérence va permettre d'améliorer le rapport signal à bruit non pas en  $1/\sqrt{N}$  mais en  $1/N$ , donc bien plus rapidement. On voit donc que dans les deux cas, la mise en réseau est un moyen d'améliorer significativement les performances de ces deux autres technologies quantiques. En outre, cette information peut être utilisée pour générer des clés de chiffrement.

Les cas d'usage sont donc faciles à imaginer : distribuer du calcul entre plusieurs ordinateurs quantiques, donner accès à des utilisateurs distants à des fermes de calcul quantique, construire des moyens de détection étendus et cohérents de haute performance, etc. ceci sans compter ce que la créativité des décennies à venir réserve – comme c'était le cas lors de l'invention d'internet vers 1960.

Pouvoir transporter une telle information d'un endroit à un autre nécessite un nouveau type de réseau. En effet, la ressource de communication – l'équivalent du spectre électromagnétique des communications classiques – va être l'intrication, c'est à dire des corrélations de nature quantique entre éléments distants (propriété dont la mise en œuvre expérimentale en 1980 a valu son prix Nobel 2022 à Alain Aspect). Cette ressource va permettre de réaliser des opérations de téléportation d'information quantique (mécanisme dont la première réalisation en 1997 a valu son prix Nobel 2022 à Anton Zeilinger). Et dans ces réseaux, même si on peut utiliser de la fibre optique déjà déployée, on aura besoin de connexions par satellite pour couvrir des distances supérieures à quelques dizaines de kilomètres. En effet, on ne peut amplifier les signaux quantiques et il faut donc vivre avec les pertes du milieu de propagation – dans la fibre elle sont exponentielles, alors qu'en espace libre elles sont que quadratiques, ce qui pose les satellites en acteurs incontournables.



*Architecture typique d'un réseau de communications quantiques :  
fibré à l'échelle de métropoles, connectées par satellite*

### **Réseaux sécurisés par voie quantique (RSQ)**

Une utilisation plus simple des possibilités offertes par la physique quantique dans le monde des télécommunications consiste à exploiter le fait que les mesures quantiques peuvent avoir des résultats aléatoires ou déterministes en fonction de la compatibilité des contextes de préparation et de mesure des systèmes que l'on manipule. Les protocoles dit de « distribution de clé quantiques » (Quantum Key Distribution, QKD) – qui sont en fait des protocoles de négociation de séquences aléatoires à la confidentialité contrôlée – permettent à deux utilisateurs aux deux extrémités d'un canal optique (fibre, espace libre) de disposer de moyens de chiffrement qui ne peuvent être compromis. Mais les cas d'usages se limitent à la sécurisation des communications par ailleurs classiques.

La ressource du réseau est ici le hasard préalablement établi, qui est disponible pour des opérations de chiffrement. Comme pour les réseaux d'information quantique, les liens longue distance vont nécessiter la mise en œuvre de nœuds de réseau en orbite – la fibre optique absorbant trop les signaux quantiques.

Dans les réseaux terrestres, cette technologie est mûre dans le sens où des produits commerciaux que l'on branche sur des fibres optiques sont disponibles. Par contre, il n'y a pas encore de produit Européen – des développements sont en cours, y compris en France.

A ce stade, il faut aussi mentionner qu'en absence de RIQ, les communications sont sécurisées seulement sur le lien qui relie deux nœuds de réseau. En effet, les nœuds servent de relai des clés qui sont transmises de proche en proche, et elles sont stockées en clair sur matériel du nœud. La sécurité est de proche en proche et non de bout en bout, ce qui réduit son intérêt. En outre, le protocole requiert une authentification préalable qui doit aussi se passer de clés établies par le protocole. Par contre, il faut mentionner que lorsque qu'un RIQ sera disponible, on saura établir des clés de bout en bout, et c'est ainsi que la sécurité deviendra un sous-produit de ces réseaux d'information quantiques présentés ci-dessus.

Enfin, comme pour les RIQ, les satellites sont un moyen incontournable d'assurer les liens à longue distance.

### Les enjeux pour la France

Un certain nombre d'enjeux s'articulent autour des communications quantiques pour les acteurs du GIFAS.

- *Le GIFAS fabriquera* : contrairement aux ordinateurs quantiques dont les acteurs du GIFAS seront principalement des utilisateurs, les communications quantiques sont une technologie sur laquelle plusieurs membres du GIFAS se sont positionnés en tant que fournisseurs d'infrastructures – au moins sur leur volet spatial incontournable. C'est donc naturellement un sujet prioritaire pour notre communauté.
- *Dual* : les communications quantiques intéressent les militaires pour augmenter la complexité des problèmes qu'ils pourront traiter ou la sensibilité de leurs capteurs, autant que le monde commercial qui va pouvoir profiter de ces moyens pour des utilisations logistiques, pharmaceutiques, financières, etc. Il en résulte qu'il faut s'attendre à *une compétition économique dure* sur ces objets, et que ceux qui auront le plus progressé grâce à de l'aide publique sur le long terme en récolteront le plus de dividendes.
- *Chine* : les acteurs chinois ont pris une avance considérable dans le domaine. Un satellite de démonstration a été lancé en 2016, un réseau terrestre étendu sécurisé par voie quantique est en place. Huawei produit des équipements QKD. Les progrès sur les ordinateurs quantiques chinois alimentent la feuille de route de leurs réseaux.
- *USA* : Le gouvernement US a bien compris qu'autant les ordinateurs quantiques seraient des objets qui se vendraient à l'unité et donc pouvaient être confiés à des acteurs privés qui ont une ambition à long terme, autant *les réseaux de communication quantiques sont une infrastructure d'équipement du pays* et ne trouveraient pas le même type d'acteurs financiers pour les porter. Dans ce contexte, le Department of Energy américain a pris le sujet en main, et après avoir publié un 'Quantum Internet Blue Print', dispose de 600 M\$ pour l'exécution d'un plan de R&D et d'équipement. Si l'Europe avait de l'avance sur les USA dans le domaine il y a quelques années, *il faut s'attendre à un rapide rattrapage* si des moyens similaires ne sont pas mis sur la table.

### Technologies critiques et proposition d'actions

La suite de ce document donne plus de détail d'une part sur les deux grandes applications, introduites plus haut, mais détaille également les technologies qu'il va convenir d'assembler pour construire les infrastructures, et s'organiser de façon raisonnée pour constituer la chaîne de la valeur des communications quantiques.



## 2.3 Description des systèmes de communication quantique

### 2.3.1 Les grands systèmes

Technologie / Application	Réseau d'information quantique – RIQ
Quantité produite / Principes de production	Ressource d'intrication, produite par des sources de photons intriqués et commutée par des routeurs d'intrication, avant d'être consommée par des protocoles de transfert d'information quantique.
Avantage attendu par rapport à l'état de l'art classique	Possibilité de mettre en réseau des dispositifs quantiques pour de plus hautes performances - N'a pas d'équivalent classique
Description la technologie mûre Volume, consommation électrique, poids, résistance à l'environnement, etc.	Technologie en cours de maturation – faisabilité démontrée en fibre (Nice, Delft) et en espace libre (Chine - Micius) N/A : infrastructure globale
Degré de maturité actuel (TRL actuel) Date de mise œuvre opérationnelle envisageable (TRL 8)	Source et système de réception/consommation de la ressource TRL4 chez Thales 1 <sup>er</sup> lien 2028 – réseau démonstration sol/orbite QINSAT – Equipe de France RIQ Réseau multi-liens validé en 2030 avec ajout de mémoire quantique
1. Prochaines TRL/étapes 2. Ordre de grandeur du coût pour mener la technologie à maturité (ou prochains TRLs/étapes) 3. Points durs technologiques ou scientifiques	1. Démonstration de la distribution d'intrication en 2028 2. 120M€ pour 2028 en France 3. Sources d'intrication, récepteurs, synchronisation, mémoires tampon quantiques, terminaux de téléportation d'états.
Acteurs principaux (France et international)	F : TAS, Airbus, Aurea, SigmaWorks, OGStech, Bertin, ALPAO, Weling, InPhyNi, ONERA Int : SpeQtral, Qconnect, QTlabs, IQOQI, TU Delft, USTC, ICFO
1. Applications CIDEF potentielles (Défense, Aéronautique militaire et civile, Naval, Terrestre). 2. Avantage technologique attendu (Défense), caractère « stratégique » 3. Autres applications hors CIDEF pouvant influencer le développement (l'accélérer). 4. Volume de marché attendu ? (Total, Aéronautique, Défense) 5. Type de client attendu (public, défense, etc.)	1. Connecter des calculateurs pour plus de performance (optimisation de mission, etc), connecter des capteurs quantiques pour créer des capteurs quantiques étendus (écoute, etc). 2. Moyens plus performants que l'adversaire par la capacité à démultiplier les performances des dispositifs quantiques par leur mise en réseau. Calcul distribué ou délégué pour résoudre des problèmes complexes avec bénéfice de la mutualisation des ordinateurs quantiques, capteurs quantiques étendus pour une meilleure performance. 3. Pharmaceutique, matériaux, finance, science opérationnelle, infrastructures critiques 4. 120M€ pour 2028 en France – marché type internet dans la phase opérationnelle post 2030. 5. Opérateurs télécom, défense
Technologies habilitantes  Compatibilité des fournisseurs à des applications défense (souveraineté, modèle industriel, modèle financier).	Terminaux optiques satellite, systèmes de contrôle de polarisation, Systèmes de synchronisation et de datation ultra précis, cryocoolers autonomes et portables, Mémoires quantiques <sup>13</sup> longue cohérence et facilement adressables, Détecteurs de photons haute efficacité / faible bruit, Lasers télécom bande étroite spatialisés, Cristaux non-linéaires haute brillance pour sources d'intrication. Besoin de développer en UE27 des lasers, compteurs de photons, cristaux non-linéaires, mémoires

<sup>13</sup> Entendu comme système de stockage temporaire d'états qui transite par un nœud de réseau.

Technologie / Application	Réseau sécurisé par voie quantique – RSQ
Quantité produite / Principes de production	Vrai hasard confidentiel partagé par les deux nœuds adjacents d'un lien réseau. L'assemblage des liens réseaux en un réseau sécurisé demande, soit de sécuriser ces nœuds intermédiaires, soit d'utiliser un RIQ pour une sécurité quantique de bout en bout (rubrique précédente).
Avantage attendu par rapport à l'état de l'art classique	Contrairement au chiffrement asymétrique, n'est pas vulnérable à la cryptanalyse. Avantages de principe : Pas d'hypothèse sur les faiblesses de l'attaquant, sessions indépendantes, sécurité persistante, organisable en pile protocolaire pour défense en profondeur.
Description la technologie mûre  Volume, consommation électrique, poids, résistance à l'environnement, etc.	Les protocoles dits « prepare & measure » disposant d'une preuve mathématique de sécurité sont commerciaux dans la fibre optique et leur faisabilité en espace libre a été démontrée. Terminal pour fibre lien dans un rack 19" et consomme quelques watts. Les terminaux spatiaux sont en cours de développement
Degré de maturité actuel (TRL actuel) Date de mise œuvre opérationnelle envisageable (TRL 8)	Sol : TRL8 chez Huawei, IdQuantique, Toshiba, TRL6 chez Thales depuis 2008 Espace : TRL 5 chez AIRBUS et Thales, 6 chez SES Opérations spatiales en 2028 (IRIS <sup>2</sup> , Eagle-1)
1. Prochaines TRL/étapes 2. Ordre de grandeur du coût pour mener la technologie à maturité (ou prochains TRLs/étapes) 3. Points durs technologiques ou scientifiques	1. Phase B2/C/D/E de SAGA pour l'ESA/UE, puis projet F EC IRIS <sup>2</sup> 2. 120M€ pour 2028 en Europe 3. Synchronisation, sources haut débit, récepteurs haute efficacité, moyens d'authentification pour l'amorçage, sécurisation des nœuds (vulnérabilité principale), terminaux optiques satellite. Moyens de certification : Critères communs/profils de sécurité spécifiques, CESTI
Acteurs principaux (France et international)	F : Airbus, Thales, Exail, Nokia, IOGS, LIP6, ONERA Int : Huawei, Toshiba, IDQuantique, QTLabs, SES, Deutsche Telekom, ICFO, AIT, USTC, OHB
1. Applications CIDEF potentielles (Défense, Aéronautique militaire et civile, Naval, Terrestre). 2. Avantage technologique attendu (Défense), caractère « stratégique » 3. Autres applications hors CIDEF pouvant influencer le développement (l'accélérer). 4. Volume de marché attendu ? (Total, Aéronautique, Défense) 5. Type de client attendu (public, défense, etc.)	1. Sécuriser les communications entre acteurs sensibles, pas de menace quantique sur les moyens de chiffrement militaires profonds 2. Pas de vulnérabilité computationnelle (démontrée RSA/DH ou possible PostQuantique) 3. Toutes communications sécurisées : Banques, système de santé, infrastructures critiques 4. 120M€ pour 2028 en Europe 5. Opérateurs telecom, défense
Technologies habilitantes  Compatibilité des fournisseurs à des applications défense (souveraineté, modèle industriel, modèle financier).	Terminaux optiques satellite, Systèmes de contrôle de polarisation, Systèmes de synchronisation et de datation ultra précis, cryocoolers autonomes et portables, Détecteurs de photons haute efficacité / faible bruit, Lasers télécom bande étroite, spatialisés, systèmes de gestion de clés, générateurs quantiques de nombres aléatoires, optique adaptative. Pour l'instant, pas de produit commercial européen, et peu de composants. Besoin de développer en UE27 des lasers, compteurs de photons, générateurs quantiques d'aléa, systèmes de gestion de clés

## 2.3.2 Les technologies habilitantes

### Synthèse

La table ci-dessous recense les principales technologies qu'il convient de mettre en œuvre dans un réseau de communications quantique.

Pour chaque technologie, elle identifie l'élément système du niveau supérieur auquel elle va contribuer.

Le détail de chaque technologie habilitante (la fonction qu'elle remplit, son niveau de maturité actuel vis-à-vis des besoins spatiaux, le principe de fonctionnement, les verrous à lever et les actions proposées) est à retrouver, technologie par technologie, dans la section 4 de ce document.

Niveau / Technologies	Utilisateur
1 / Sources de photons intriqués haut débit	Réseau d'information quantique
1 / Terminaux de clés quantiques	Réseau sécurisé par clés quantiques
1 / Sources de photons uniques, si possibles non-cryogéniques	Terminaux de clés quantiques
1 / Routeur d'intrication	Réseau d'information quantique
1 / Terminaux récepteurs d'intrication	Réseau d'information quantique
1 / Générateurs quantiques de nombres aléatoires	Réseau sécurisé par clés quantiques
1 / Systèmes de gestion de clés	Réseau sécurisé par clés quantiques
2 / Cristaux non-linéaires haute brillance	Sources de photons intriqués haut débit
2 / Lasers télécom bande étroite, spatialisés	Sources de photons intriqués haut débit, Sources de photons uniques
2 / Détecteurs de photons haute efficacité / faible bruit	Récepteurs d'intrication, Terminaux de clés quantiques
2 / Systèmes de synchronisation et de datation ultra précis	Réseau d'information quantique, Réseau sécurisé par clés quantiques
2 / Mémoires quantiques longue cohérence, facilement adressables	Routeur d'intrication, Récepteurs d'intrication
2 / Cryocoolers autonomes et portables	Routeur d'intrication, Récepteurs d'intrication
2 / Optique adaptative	Terminaux de clés quantiques, récepteurs d'intrication (spatiaux)
2 / Systèmes de contrôle de polarisation	Sources, récepteurs
2 / Dispositifs de distillation d'intrication	Routeur d'intrication, Récepteurs d'intrication
3 / Circuits photoniques intégrés	Sources de photons intriqués haut débit, Routeur d'intrication, Terminaux récepteurs d'intrication, Optique adaptative

*Synthèse des différentes technologies à mettre en œuvre dans un réseau de communications quantique, en fonction du niveau de profondeur de la chaîne de la valeur.*

## 2.4 Conclusions et recommandations

Les enjeux des communications quantiques consistent essentiellement à préparer les réseaux spécifiques qui connecteront les ordinateurs quantiques et/ou les capteurs quantiques entre eux : les réseaux d'information quantique (RIQ). En outre, une nouvelle façon de sécuriser les communications pourra en être dérivée. Plusieurs acteurs du GIFAS se positionnent sur la *réalisation* de ces systèmes – en particulier leur composante spatiale qui assurera la longue distance.

Il est attendu que le marché de ces systèmes soit un marché d'infrastructure (et non d'équipement comme les capteurs et les ordinateurs) d'usage commercial ou double. Une concurrence forte est à attendre entre acteurs mondiaux, et comme les défis techniques sont réels, ceux qui tiendront le marché dans les années 2030 *seront ceux qui auront commencé tôt et auront été bien soutenus* en attendant les retours sur investissement long terme.

Il faut noter que la Chine a une décennie d'avance sur l'Europe en la matière, et que les USA viennent de débloquer un budget de 600M\$ pour travailler spécifiquement sur les RIQ, ce qui devrait leur permettre de progresser rapidement. Il est donc clé que la puissance publique s'implique dans le soutien de ce domaine afin que les acteurs français qui ont une position initiale *favorable ne soient pas rapidement débordés par la concurrence mondiale*.

Pour cette implication, nous proposons les familles d'actions suivantes, qui s'inscrivent dans la perspective globale d'un démonstrateur en orbite QINSAT de lien longue distance de réseau d'information quantique.

### 1) Dans le cadre des technologies critiques du démonstrateur QINSAT phase 1

1.a) soutenir des démonstrateurs opérationnels de

- Source de photons intriqués spatialisée
- Terminaux récepteurs d'intrication
- Systèmes de synchronisation et de datation ultra précis
- Système d'optique adaptative sol, légère et bas cout
- Système de contrôle de la polarisation des photons

1.b) soutenir le développement du système de démonstration complet avec un satellite et deux stations sol (y compris ingénierie système, intégration et phase d'expérimentation système) le tout dans le cadre du programme national QINSAT avec une contribution du plan quantique.

### 2) Dans un plan plus général et mutualisé avec d'autres usages, faire progresser les technologies habilitantes comme

- Cristaux non-linéaires haute brillance - sur le composant cristallin, mais aussi son conditionnement thermique et optique
- Lasers télécom bande étroite, spatialisés
- Détecteurs de photons haute efficacité / faible bruit, probablement supraconducteurs pour les meilleures performances.
- Cryocoolers autonomes, a faible maintenance et portables

### 3) Pour le positionnement des industriels français dans les projets de clés quantiques européens (EuroQCI)

- Terminaux de clés quantiques
- Sources de photons uniques, si possibles non-cryogéniques
- Générateurs quantiques de nombres aléatoires
- Systèmes de gestion de clés

en contribuant aux actions européennes sur le sujet lorsqu'elles demandent une coparticipation des états membres.

en participant aux comités de standardisation ces systèmes qui ont vocation à être multi vendeurs et devront être interopérables.

en promouvant l'intérêt du sujet auprès de l'ANSSI, avec laquelle nous partageons le besoin de sécurité de bout en bout.

**4) Pour la préparation de la phase 2 de QINSAT** qui visera à assembler plusieurs liens réseaux à la fin de la décennie soutenir les acteurs qui développent

- Les mémoires quantiques longue cohérence, facilement adressables

- Les routeurs d'intrication qui utiliseront ces mémoires quantiques

- Les dispositifs de distillation d'intrication pour améliorer les performances des liens individuels

en soutenant les acteurs plus amont qui travaillent sur ces sujets (start-ups, laboratoires publics ou privés) par du développement d'équipements ou de démonstrateurs sur table.

(page laissée intentionnellement blanche)

# 3. Calcul quantique

## 3.1 Résumé aux décideurs

Le calcul quantique offre la promesse de résoudre certains problèmes (inversion d'un système linéaire, optimisation d'une fonction de coût, factorisation de grands nombres premiers...) plus rapidement que les meilleurs ordinateurs actuels. Ces dernières années, un grand nombre d'acteurs se sont lancés dans la construction de machines pour le calcul quantique, sur la base de financements publics et privés. Il existe une grande variété de plateformes physiques pour implémenter ces calculateurs quantiques : photons, atomes neutres, circuits supraconducteurs, spins sur silicium, nanotubes de carbone... Il existe également plusieurs approches en fonction du niveau de bruit des machines, avec des horizons associés différents : d'un côté le *quantum annealing* et le *noisy intermediate scale quantum computing* (NISQ), qui peuvent s'accommoder de machines bruitées avec un espoir d'application à court ou moyen terme, et de l'autre le *fault tolerant quantum computing* (FTQC) qui nécessite des qubits logiques corrigés des erreurs (et donc mobilisant un grand nombre de qubits physiques par qubit logique), avec un horizon plus lointain. Pour le moment, il n'existe pas de démonstration d'un 'avantage quantique' sur un problème pratique d'intérêt industriel, et il est très difficile à ce stade de prédire quand cet avantage quantique arrivera et quels sont avec certitude les domaines d'application qui pourraient bénéficier d'un tel avantage. Toutefois, le secteur étant très dynamique et les choses pouvant évoluer très rapidement, il semble important pour les utilisateurs potentiels y compris les industriels du GIFAS de se préparer au calcul quantique.

Les activités du GIFAS pourraient bénéficier de ces machines sur un certain nombre de cas d'usage déjà identifiés : planification de mission, simulation de la combustion ou équations aux dérivées partielles pour la simulation électromagnétique ou la mécanique des fluides par exemple. Il semble toutefois important d'augmenter l'effort en cours sur l'identification des cas d'usage pour notre secteur, et sur la recherche de nouveaux algorithmes pour ces cas d'usage, trop peu nombreux pour le moment. Une autre problématique critique pour notre domaine d'activité est l'accès aux machines à distance de façon sécurisée (ces machines étant a priori trop coûteuses pour être acquises par un utilisateur unique). Si des techniques de sécurisation classiques existent et doivent être consolidées, il semble également pertinent dans une vision à long terme de s'appuyer sur un réseau de communication quantique pour garantir de façon inconditionnelle la sécurité et la confidentialité des algorithmes utilisés. Dans une première phase où les industriels accèdent aux machines existantes pour tester des algorithmes ou des manipulations élémentaires, il semble judicieux de ne pas se limiter aux machines françaises, mais d'étendre l'accès aux machines européennes, pour ne pas exclure de technologie a priori (même si de très nombreuses technologies sont déjà couvertes par les acteurs français du domaine). Il serait intéressant également de partager, au niveau des industriels du GIFAS, les méthodes et les résultats de benchmark des différentes machines quantiques, en se coordonnant avec le projet BACQ du LNE, afin de pouvoir suivre de façon collégiale les progrès de ces dernières au cours des prochaines années. Enfin, sur le long terme, il semble important d'être en capacité de disposer de piles logicielles de confiance (possiblement open source), couvrant l'ensemble de la problématique du développement logiciel, allant des langages de programmation jusqu'à la compilation en circuit quantique, de façon agnostique vis-à-vis du hardware. Il faudra également veiller à être en mesure le moment venu de disposer d'une filière industrielle européenne pérenne pour garantir l'accès aux machines, et d'un modèle économique viable pour les constructeurs de machines français. Enfin, il faudra mettre en plus des formations initiales et continues afin de répondre aux besoins en compétences en algorithmie quantique des industriels.

## 3.2 Contexte

Ce qui est recherché par les utilisateurs industriels c'est un avantage quantique pour leurs applications avant une quelconque suprématie quantique qui peut tarder à se manifester dans le domaine du calcul. L'avantage visé reste une accélération exponentielle sur le temps de calcul permettant de traiter aujourd'hui des problèmes inaccessibles (certaines classes de problèmes NP complet), cependant, une accélération même quadratique pourrait être bonne à valoriser, car elle conduirait à réduire les coûts et à donner un avantage de compétitivité. L'avantage quantique peut aussi se rechercher en terme de précision de la solution à temps de calcul constant, par exemple pour les problèmes d'optimisation combinatoire. En attendant l'avantage quantique, il est mis aujourd'hui en avant un avantage énergétique, donc un avantage sur le coût de fonctionnement de ces machines et la prise en compte du défi sociétal sur le réchauffement climatique. Cependant, si la consommation des QPU (Quantum Processor Units) est très faible en comparaison des futures machines Exascale, le débat est encore ouvert sur la consommation globale de machines de plusieurs millions de qubits, l'électronique associée étant potentiellement très consommatrice d'énergie (suivant les technologies, les stratégies de contrôle des qubits requièrent plusieurs câbles radiofréquence de haute-fidélité par qubit). L'initiative #QEI (Quantum Energy Initiative) doit répondre à ces questionnements.

### 3.2.1 Les applications

Sur le papier, toute application déjà utilisatrice de moyens de calcul haute performance est susceptible de tirer parti du calcul quantique, mais ceci implique trois prérequis. Le premier est de disposer d'algorithmes quantiques pouvant apporter un avantage, le second est de disposer de la machine pouvant les implémenter de façon efficace, le troisième est d'avoir des outils d'ingénierie pour valider/qualifier ces algorithmes

Capacité	Domaine d'emploi
Equation différentielle, résolution de systèmes linéaires	Simulations électromagnétique, mécanique des fluides, mécanique des structures, pyrotechnie, combustion, climat, ...
Simulation Monte Carlo, simulation probabiliste en très grande dimension, filtrage particulaire, analyse valeurs extrêmes, tests statistiques	IVVQ (Intégration, Vérification, Validation, Qualification) reconfiguration, rayonnement, ...
Design de molécules, conception de matériaux, compréhension de réactions chimiques	Prédiction et génération de nouveaux polymères, matériaux énergétiques, biocarburants, poudres pyrotechniques, ...
Étude de risques, détection d'anomalies	Cyber sécurité
Optimisation combinatoire, ordonnancement, recherche opérationnelle, allocation de ressources, logistique, plus court chemin	<ul style="list-style-type: none"> <li>• Optimisation du design des capteurs (radars, ...)</li> <li>• Aide au déploiement et à la reconfiguration</li> <li>• Gestion des missions et du trafic (avions, drones, satellites, ...)</li> </ul>
IA-Apprentissage Machine, apprentissage par Renforcement et IA générative.	<ul style="list-style-type: none"> <li>• Système de recommandation</li> <li>• Reconnaissance d'images</li> <li>• Allocation de ressources des capteurs et des armes</li> <li>• Génération de données simulées plus réalistes, ...</li> </ul>
Aide à la prise de décision, planification de missions	Rover, allocation de ressources, reconfiguration de missions,....



Robotique	Diagnostic, perception, ...
Cryptographie	Crypto-Analyse, attaque de code

Tableau 1 : Capacité

L'un des premiers domaines qui pourrait tirer parti du calcul quantique est celui des problèmes d'optimisation et du QML (Quantum Machine Learning). On peut mentionner ensuite la simulation des molécules et le calcul EDP. Globalement, les applications qui se prêteront le mieux à l'avantage quantique sont celles qui nécessitent beaucoup de calcul pour très peu d'entrées-sorties (ce qui n'est malheureusement pas le cas des problèmes de mécanique des fluides).

### 3.2.2 Les Algorithmes

Le choix des algorithmes n'est pas découplé des machines qui vont les exécuter, en effet, la taille des circuits que l'on peut exécuter est limitée par le bruit, on est donc amené à considérer ce qui est faisable à court, moyen, long terme, que l'on décline en technologies:

- QA (Quantum Annealer) : ordinateur quantique analogique pour résoudre les problèmes QUBO (Quadratic Unconstrained Binary Optimization)
- NISQ (Noisy Intermediate Scale Quantum) : ordinateur quantique à portes bruités utilisant des algorithmes variationnels avec formalisation hamiltonienne du problème
- FTQC (Fault Tolerant Quantum Computing) : ordinateur quantique à portes disposant de codes correcteurs d'erreur et de feedback quantique de régulation

Le nombre d'algorithmes quantiques disponibles est encore restreint (<https://math.nist.gov/quantum/zoo>), mais il faut noter que beaucoup d'algorithmes s'appuient à plus bas niveau sur la QFT (Quantum Fourier Transform) qui demande des qubits non bruités. De ce fait, très peu d'algorithmes existants sont utilisables dans la période NISQ actuelle (notamment les algorithmes variationnels).

Actuellement, on cherche à identifier les capacités à l'échelle en s'appuyant sur des algorithmes utilisant moins de 50 à 100 qubits physiques et qui seraient résistants au bruit. A court terme, on cherche à traiter des problèmes utilisant des algorithmes peu profonds, mais qui ont l'avantage de pouvoir être simulés sur des machines classiques. A moyen terme, on cherche des algorithmes apportant une vraie accélération qui vont demander plus de 100 qubits logiques, c'est-à-dire non bruités. A long terme, l'objectif est de traiter des cas industriels en opération.

ERE	Type d'algorithme	Algorithme	Finalité
QA	QUBO	Quantum Annealing de modèle d'Ising (associé au QUBO)	Optimisation binaire quadratique sans contraintes
NISQ	Algorithme variationnel, formalisation Hamiltonien	VQE algorithmes hybrides	Simulation de chimie quantique, jusqu'ici fait avec des molécules de 2 à 3 atomes
		QAOA	Trouver des solutions approchées à des problèmes d'optimisation combinatoire (inclut la factorisation d'entiers)
		VQLS	Solveur linéaire quantique variationnel utilisé dans l'apprentissage automatique et pour résoudre des équations aux dérivées partielles
		QML	L'apprentissage automatique des circuits quantiques variationnels (machines à vecteurs de support quantiques, réseaux de neurones quantiques)
FTQC			
		<b>QFT</b> Utilisé dans un très grand nombre d'algorithmes à plus bas niveau	Estimation de phase quantique utilisées dans les simulations chimiques, HHL pour l'algèbre linéaire, apprentissage automatique quantique, équations aux dérivées partielles
		<b>QPE</b> Quantum phase estimation, <b>QAE</b> Quantum Amplitude Estimation	Utilise la QFT, mais demande un long temps de cohérence
		<b>HHL</b>	Résolution de systèmes linéaires
		<b>Algorithmes de Recherche</b>	Basés sur des oracles comme Grover, marches quantiques, TSP, ...
		<b>Factorisation</b>	Factorisation d'entiers courts (Shor) et algorithmes dlog, chiffrement
		<b>Algèbre de Lie</b>	Réseaux de neurones équivariants (Quantum Group Convolution)

Tableau 2 : Algorithmes

Comme il n'existe pas de preuve d'algorithme totalement résistant au bruit, il est nécessaire, pour que les machines *hardware* NISQ puissent produire des résultats d'intérêt, de développer les recherches dans la QEM (Quantum Error Mitigation<sup>14</sup> ou atténuation des erreurs, technique qui utilise le post traitement des résultats). La QEM est primordiale pour exploiter rapidement le potentiel de l'informatique quantique, en attendant la disponibilité de la QEC (Quantum Error Correction) pour les FTQC / LSQC.

<sup>14</sup> Mise en œuvre par IBM.

Le produit Qaptiva (évolution de la QLM) d'Eviden, permet aujourd'hui de simuler à l'aide d'un ordinateur classique 41 Qubit intriqués, avec simulation de bruit et donc de tester la résistance au bruit d'un algorithme, mais permet aussi de faire de la QEM.

Des recherches algorithmiques sont réalisées au sein des start-ups produisant les machines, cependant, les solutions qui en sortiront seront encapsulées en boîte noire dans des bibliothèques propriétaires et ne seront pas directement accessibles, ceci pour des raisons de compétition entre les différents acteurs. L'argument commercial sous forme d'un package *hardware/software* rend difficile pour une entreprise de se différencier de ses concurrents. Il ne faut pas oublier l'apport possible de la « déquantification » à savoir qu'étudier un problème avec une vision nouvelle (quantique) peut conduire à produire un nouvel algorithme classique bien plus performant que les algorithmes déjà existants, un précédent existe dans le cadre des algorithmes de recommandations (Prix Netflix). Ce gain « Quantum-Inspired » est en partie lié au fait que certains problèmes ont été initialement mal formalisés, et qu'une formalisation variationnelle avec Hamiltonien permet de faire émerger des schémas (classiques) plus efficaces.

### 3.2.3 Les QPUs

On regroupe dans le tableau suivant les principales technologies de QPU, les technologies en gras correspondant à des start-ups françaises. Ce tableau illustre la grande diversité des technologies et montre que la France est bien positionnée, car couvrant la plupart des technologies. Elle souffre en revanche d'un déficit de financement comparé aux entreprises équivalentes aux US. Le fait qu'il existe un grand nombre de technologies supportées ne doit pas être vu comme un point négatif (dispersion des financements), mais simplement pragmatique, en raison du fait qu'aujourd'hui il n'est pas possible de statuer sur la technologie qui dominera le marché par la suite. Il est envisageable que plusieurs technologies trouveront leur place, tel type de technologie étant plus adaptée à tel type d'algorithme, et donc à un type d'application. En France, le focus à court terme se porte sur les start-ups Pasqal et Quandela, qui sont les seules en mesure d'ouvrir un accès à des machines en mode Cloud à l'heure actuelle (début 2024), et qui seront accessibles au travers du programme HQI du Plan Quantique National. Les start-ups Quobly (ex Siquance), C12 et CrystalQC sont des start-ups plus récentes, il faudra donc encore attendre un peu pour avoir accès à leur *hardware*. La société Alice&Bob se positionne sur l'ère post NISQ (LSQC), avec l'utilisation de qubits de chat (code bosonique) associés à la technologie de feedback quantique développé par QUANTIC (Mines Paris, ENS, INRIA).

Technologie	Sociétés Française	Sociétés Européen	Sociétés hors UE
Ions Piégés	<b>CrystalQC</b>	AQT (Autriche), Quantinuum (UK)...	IONQ (US)
Atomes froids piégés	<b>PASQAL</b>		QuEra, ColdQuanta (US), Atom Computing
Supraconducteur		IQM (Finlande, Allemagne et France)	Google (US), IBM (US), Rigetti (US),
Supra à code Bosonic	<b>ALICE&amp;BOB</b>		AMAZON (US)
Spin Qubit sur Silicium et nanotubes	<b>Quobly</b> (ex Siquance), <b>C12</b>	Equal1 (Irlande)	Intel, DiraQ (Australie)
Photonique	<b>Quandela</b>	QuiXb (NL)	PsiQuantum (US), Xanadu (Canada),
Autres technologies			Qubits topologiques (Microsoft), lacunes de spin (Turing, ...), centres NV

			diamant (Quantum Brilliance, Australie)
Recuit quantique			D-Wave (Canada), Fujitsu, NEC

Tableau 3 : Technologies hardware

A noter que la société Atom Computing a annoncé fin octobre 2023 une machine à 1180 qubits. En 2021 cette société affichait une machine à 100 qubits, ce qui illustre la rapide évolution du hardware et qui montre que les technologies quantiques peuvent arriver plus tôt que prévu à maturité. A noter toutefois que cette annonce doit être mise en regard du fait que le nombre de qubits ne constitue pas en tant que tel un indicateur pertinent de la puissance de calcul d'une machine quantique, comme discuté dans la section suivante. Notons que certains développeurs de machines quantiques à base d'atomes neutres (QuEra, Atom Computing...), initialement tournés vers le NISQ, sont en train d'évoluer vers des architectures à bases de portes quantiques pour le calcul universel.

### 3.2.4 Benchmarking

La majorité des acteurs français du domaine sont en contact avec le projet BACQ (Benchmarks Applicatifs des Calculateurs Quantiques) que THALES pilote dans le cadre du programme MetriQs du LNE et qui propose une approche multi-critères :

- <https://www.lne.fr/fr/communiqués-de-presse/bacq-delivering-application-oriented-benchmark-suite-objective-multi-criteria>
- [https://teratec.eu/library/seminaires/2023/TQCI/2305/3\\_BACQ.pdf](https://teratec.eu/library/seminaires/2023/TQCI/2305/3_BACQ.pdf)
- [https://teratec.eu/Seminaires/TQCI/2023/Seminaire\\_TQCI-230511.html](https://teratec.eu/Seminaires/TQCI/2023/Seminaire_TQCI-230511.html)

Le benchmark des calculateurs quantiques est important pour suivre l'évolution des performances des QPUs. Il faut noter que le nombre de qubits n'est pas le seul critère dans l'évaluation d'une machine, il convient de prendre en compte d'autres critères dont chacun a des niveaux de maturité (TRL) différents très dépendant des technologies. Il faut aussi ne pas confondre les qubits physique et logique (qubit constitué d'un ensemble de qubits physiques permettant de corriger les erreurs liées au bruit). On propose dans ce qui suit une liste des principaux critères à prendre en compte pour l'évaluation de ces machines :

- Les temps de relaxation et de décohérence, qui doivent être mis en regard des temps de couplage entre les états (qui peuvent également varier d'une technologie à l'autre)
- La fiabilité des opérations de base de type « portes logiques »
- La fiabilité de lecture (60 à 99%)
- La facilité ou la possibilité de connecter les qubits entre eux de façon non contrainte
- Le nombre de qubits, à condition que ces qubits puissent être intriqués de façon fiable. Une métrique plus pertinente est la profondeur d'intrication atteinte par la machine, qui donne un meilleur aperçu de l'avantage quantique atteignable que le nombre de qubits seul. A noter que cette donnée n'est pas facilement disponible de la part des constructeurs.
- Le passage à l'échelle (comment on arrive à augmenter le nombre de qubits sans perte de fiabilité et de flexibilité),
- La contrainte d'exploitation (température système cryogénique, coût de fonctionnement)
- Le problème de défauts dans la production des qubits (sauf s'ils sont naturellement identiques comme pour les photons et les atomes)

- La prise en compte de la correction des erreurs (Riken système à 3 qubits sur silicium),
- La possibilité d'interconnecter plusieurs machines (voir les travaux de Welink à ce sujet)
- Le prix : le sujet coût est très peu évoqué, mais rappelons que la machine D-Wave 2000Q en 2021 était affichée à 15 M\$ prix catalogue. De ce fait, il est difficile pour un industriel de s'équiper en propre et les données disponibles sur le coût d'une heure de calcul donnent une fourchette entre 1000 et 5000 euros (sachant que faire tourner un calcul demande de nombreuses répétitions de la même séquence ce qui peut être consommateur de temps)
- La vitesse d'exécution des portes.

### 3.2.5 Environnement

Il existe, depuis plusieurs années, un ensemble de bibliothèques/simulateurs qui permet de se préparer dès aujourd'hui à la programmation de machines quantiques (Qiskit d'IBM, Cirq de GOOGLE, Q# de MICROSOFT, ...). Certains sont orientés programmation digitale ou analogique, d'autres plus spécialisés sur le recuit quantique. En pratique, on peut être amené à utiliser plusieurs environnements de développement en fonction des contraintes de performances : disponibilité d'une version GPU (exemple *Quilacs*) ou de certaines fonctionnalités (différentiation automatique *Penny Lane*). L'émulateur Qap-tiva/QLM d'Eviden/Atos a plusieurs atouts: la possibilité de traiter l'approche analogique et digitale, la possibilité de tester ses algorithmes au bruit, et donc la montée en échelle. Dans une phase de compréhension de l'algorithmie quantique et de tests, le passage d'un outil à l'autre n'est pas un problème bloquant, mais ceci le deviendra lorsqu'il s'agira de développements conséquents devant s'exécuter sur un ensemble de plateformes. La vision agnostique d'un produit est un plus pour la pérennité des développements. Les « constructeurs » (par exemple Quandela, Pasqal) disposent d'environnements propriétaires (Perceval, Pulsar) permettant de simuler leurs machines ou de les programmer. La majorité de ces outils sont dans le domaine public.

La partie programmation n'est que le premier maillon visible, mais c'est un ensemble de nombreux points qui doivent être pris en compte pour produire un environnement mature, ce que l'on appelle une « full quantum stack » qui englobe : les applications, la génération de circuits et la vérification de ces circuits, le multiplexage des signaux, les codes de correction d'erreur, l'électronique cryogénique pour le contrôle et la lecture des qubits, la compilation, les algorithmes hybrides, l'atténuation des erreurs, la modélisation du système quantique dans sa globalité. C'est l'ensemble de la chaîne qui doit être mature pour que le calcul quantique percole dans l'industrie.

Il faut un effort de mutualisation mais il ne doit pas se transformer en monopole. Parmi les émulateurs déjà utilisés aujourd'hui par la communauté (Qiskit, PennyLane, MyQLM, ...) on note que chacun est construit avec un certain paradigme, avec ses avantages et inconvénients. Se restreindre à l'utilisation d'émulateurs américains peut poser à terme un risque de perte d'accès à ces dispositifs.

Le calcul quantique et sa prise en main est complexe. Passer par une plateforme qui est en lien avec les constructeurs et fournisseurs de QPU simplifie les démarches à l'heure où on ne peut pas se contenter d'un seul type de QPU (ex. la topologie des QPU d'un constructeur n'est pas forcément adaptée à tous les problèmes). De ce fait son introduction dans l'industrie implique qu'il soit le plus accessible possible, et d'une mise en œuvre des plus simple, par conséquent le développement de plateformes agiles facilitant la portabilité sur des technologies hardware différentes (y compris en dehors de l'Europe) doit être encouragé .

Pour un objectif d'acculturation ces plateformes doivent proposer des spécificités liées aux métiers et à l'usage des utilisateurs et proposer un niveau d'abstraction évitant une programmation de bas niveau

mais il faut aussi un accès plus direct aux QPU pour les utilisateurs expérimentés qui pourront les exploiter au mieux.

Les QPUs étant pour l'instant limités en ressources (qubits, portes quantiques, ...), il est important de disposer de compilateurs de confiance permettant de synthétiser un circuit quantique sous contraintes de ressources de façon agnostique du hardware. Une seconde couche de compilateur propriétaire des QPUs servira à compiler les circuits quantiques sur les qubits et portes quantiques physiques.

### 3.2.6 Une Roadmap ?

En raison du grand nombre de points à prendre en compte tant algorithmique/*software* que *hardware*, il est difficile de se prononcer sur une roadmap généraliste réaliste. A noter que certaines roadmaps ont déjà été publiées (voir liste de rapports en annexe). Au niveau des annonces des constructeurs, on note deux stratégies d'affichage, ceux qui présentent une augmentation du nombre de qubits physiques pour créer un certain nombre de qubits logiques et ceux qui affichent une augmentation de la qualité de leurs qubits visant à réduire le nombre de qubits physiques (Alice&BoB, C12, ...). L'écosystème étant très dynamique et la qualité technologique des startups étant avérée, on peut espérer des progrès technologiques rapides mais la question de l'avantage quantique à court ou moyen terme reste ouverte.

Au financement des différents états s'ajoute l'apport des grandes entreprises qui investissent largement dans le quantique (Google, AWS...) et l'apport important des fonds privés, ce qui est un signe de pérennité du domaine à court terme. Cependant, il faut se méfier d'une survente du calcul quantique, qui pourrait conduire à une situation identique à ce que l'on a connu pour l'IA (les 2 hivers sur l'IA). Les actions de Benchmarks des calculateurs quantiques (BACQ en France, QED-C aux US, ...) devraient rassurer les investisseurs et éviter l'advenue d'un hiver quantique, en permettant de suivre régulièrement les progrès et de façon indépendante. Un risque de désengagement des capitaux privés à moyen terme n'est toutefois pas à exclure. Les technologies développées pour la mise en œuvre des ordinateurs quantiques profiteront aux autres domaines comme les communications et les capteurs au travers des avancées dans les technologies habilitantes. D'après certains fabricants de machines quantiques, on peut espérer une démonstration d'un avantage sur machine analogique et NISQ à partir de 2025, et un avantage FTQC après 2030. L'accès aux premières opérations entre qubits logiques en 2024 devrait marquer une étape importante vers le FTQC.

Devant les incertitudes, un certain nombre de jalons peuvent être mis en place pour suivre et faire évoluer la roadmap du calcul quantique, selon la liste suivante :

- La disponibilité du 1<sup>er</sup> qubit logique, suivi par la disponibilité de 50 qubits logiques (égale à la puissance d'un super ordinateur dans le top 500). La disponibilité de 60 qubits est un saut de puissance de calcul d'un facteur 1000 par rapport à 50 qubits.
- La mise à disposition d'un QC permettant la démonstration d'une suprématie quantique : résoudre un problème simple et utile que l'on sait aujourd'hui hors d'atteinte par le calcul classique. Les technologies étant différentes, il faut bien séparer l'approche analogique de l'approche digitale (*gate-based*), la première étant celle qui doit permettre plus rapidement un avantage quantique, mais qui reste moins universelle.
- La mise à disposition d'un QC permettant la démonstration d'une suprématie énergétique à puissance égale avec un ordinateur classique.
- Le développement commercial d'un QC *gate-based* "utile": capable de résoudre des problèmes d'intérêt pratique sur un nombre très restreint d'applications.
- Le développement d'un QC affichant 100 qubits logiques et de plus haute-fidélité (50 qubits logiques étant considéré comme la puissance actuelle d'un grand système HPC)

- Le développement d'un QC affichant plus de 1000 qubits logiques
- Le développement d'un QC tolérant aux fautes couplant plusieurs QC

Un des enjeux importants est la mise en place d'une boucle vertueuse (loi de Moore pour le quantique, appelée loi de Rose, qui prédit le doublement du nombre de qubits tous les ans, évolution des machines D-WAVE passées de 128 qubits à 2011 à plus de 5000 qubits en 2021 avec la machine Advantage) qui passe par des succès intermédiaires pour aller de l'ère NISQ à l'ère FTQC.

Citons aussi la roadmap d'IBM qui annonce en 2029 un premier système à 100 millions de portes avec 200 qubits utilisant la correction d'erreurs et en 2033 le système Bluejay avec 1 milliards de portes et 200 qubits.

Les défis à relever sont importants :

- Augmenter la fidélité des qubits,
- La correction d'erreur, et le quantum feedback
- L'interconnexion entre QPU (notamment pour les architectures où le nombre de qubits par QPU est limité)
- Les technologies habilitantes (câblage, cryogénie, ultravide, ...)
- La consommation énergétique
- Les entrées/sorties car la bande passante des machines quantiques, exprimée en GigaOctets par seconde, est très faible
- Les mémoires quantiques (pour le couplage entre accélérateurs quantiques)
- La diffusion du calcul quantique qui permettra de réduire le prix de vente des machines
- Le manque d'algorithmes sur les sujets d'intérêt industriels
- La disponibilité de *full-stack* (compilation, bibliothèque, langage, ...),
- L'intégration d'ordinateurs quantiques dans l'écosystème classique (HPC, Cloud), avec une interconnexion directe entre différentes technologies de qubits et une interconnexion réseau protégée entre les utilisateurs et les sites de production
- L'intégration dans le monde HPC. Le calcul quantique a besoin de HPC (validation des algorithmes jusqu'à 40 qubits, *debug*, optimisation des circuits, préparation des données d'entrée, traitement des données de sortie, correction d'erreur).

### 3.3 Les actions à poursuivre et/ou intensifier

En fonction du contexte présenté précédemment, il semble utile de mettre en évidence un certain nombre de points d'attention.

#### Algorithmie

- Le plan quantique a principalement orienté les financements vers le développement de startups produisant des QPU. Cependant, il n'y aura pas d'avantage quantique sans algorithme quantique. Il est donc important d'encourager et de soutenir le développement de l'algorithmie quantique. Le nombre d'algorithmes quantiques reste très limité, de ce fait, il est difficile de revendiquer un gain concurrentiel en restant un simple utilisateur de solutions proposées par le constructeur de QPU, un investissement algorithmique est donc nécessaire au niveau de l'industrie

- Il faut en parallèle soutenir les laboratoires français travaillant sur les sciences fondamentales liées aux algorithmes, afin de s'assurer que la France reste à la pointe dans ces domaines

## **QPU et benchmark**

- Il faut continuer à soutenir les start-ups produisant des ordinateurs, des interconnexions de calculateurs quantiques multi-modalités (ex : utilisation techno Welink), et les technologies habilitantes, et tout ce qui est lien (*hardware* et *software*) avec les codes de correction d'erreurs : code surfacique, codes LDPC, codes bosoniques (Cat Qubit, GKP Qubit, ...) avec feedback quantiques.

- Concernant les actions de Benchmarks pour les calculateurs quantiques, il existe des actions à l'étranger sur le sujet (QED-C, DARPA/Raytheon, ...), le projet BACQ répond à ce besoin pour la France. Il semble pertinent d'étendre cette action de Benchmark au niveau européen (avec TU Delft/TNO aux Pays-bas, Fraunhofer Institute IKS en Allemagne, ...) pour promouvoir un benchmark européen de référence.

- Le projet BACQ vise à fournir un benchmark au LNE. Il y a un intérêt à étendre BACQ pour un benchmark orienté vers les verticaux applicatifs (exemple : calcul optimisé de forme d'avion, vol en essaim, ...) en lien avec les besoins du GIFAS en coordination avec le LNE et THALES

- Il existe un ensemble d'outils/environnements pour la programmation (Microsoft #Q, Rigetti Forest, IBM QX (OpenQASM), QISKIT, SiQ, CIRQ, Quipper, QFC, QPL, Atos QLM), un effort pour éviter de se disperser en factorisant les développements autour d'outils de confiance communs serait profitable (cf. ce qui a été fait pour l'IA avec Scikit Learn).

## **International**

- Actions de normalisation et de standardisation sur le calcul quantique : il existe des initiatives à l'étranger (CEN/CENELEC, ISO, IEEE Quantum Computing Benchmark, ...). Le projet BACQ répond aujourd'hui à ce besoin

- Mettre en place une veille technologique sur les sources de compétition internationale en lien avec les industriels concurrents du GIFAS dans le monde: Europe (SAAB, LEONARDO, HENSOLDT,...), US (Raytheon, Lockheed, Honeywell, Northrop,...), Israël (Elta, Rafael, ...), Japon (NEC, Fujitsu,...), Chine, Russie, groupe de travaux OTAN

- Besoin d'une conférence internationale (type IEEE Quantum Week) orientée ingénierie via la SEE pour afficher la position de la France dans le domaine et disposer d'une place d'échanges techniques entre académiques et industriels. Les événements type Q2B sont parfois jugés trop 'commerciaux' en raison du manque de présentations académiques.

## **Environnement**

- Il est nécessaire de disposer de compilateurs performants, le développement de compilateurs HW-Agnostique (et HW-Dependent) existe en dehors de la France (exemple : Classiq en Israël [www.classiq.io](http://www.classiq.io))

- Le besoin existe de développement et de maintien de bibliothèques 'haut niveau' de confiance avec les laboratoires académiques et les start-ups françaises : librairie concurrente de Qiskit d'IBM, CIRQ de GOOGLE, ... Généralement, il n'existe pas de source de financement pour faire vivre les outils issus du monde de la recherche (citons un contre-exemple de 'success story' dans le domaine du machine Learning, la 'fondation Inria' permet de faire vivre des outils en dehors de la recherche, c'est le cas pour *scikit-learn* qui aura une suite avec le développement de l'infrastructure P16 de la SNRIA pour l'extension de cet outil).

- Il faut favoriser le développement de *stack* logiciel de confiance. Par exemple, la Chine travaille en ce sens (annonce en février 2021 de la Chine par Origin Quantum Computing Technology (Origin Tech



(<http://www.origingc.com.cn/>) du premier système d'exploitation (OS) chinois pour les ordinateurs quantiques baptisé Origin Pilot, qui doit permettre l'exécution en parallèle de plusieurs tâches de calcul quantique, l'étalonnage automatique des qubits et la gestion unifiée des ressources de calcul quantique. L'utilisation avec Origin Quantum Cloud doit permettre de contrôler des ordinateurs quantiques multi-cœurs. Il existe aussi un besoin d'outils de *profiling* et d'optimisation des circuits à portes qui devra être pris en compte. On peut citer aussi la société Riverline qui travaille sur le développement d'une stack logicielle prenant en compte la correction d'erreur.

### Accès aux machines

- Support des start-ups françaises pour faciliter l'accès souverain des membres du GIFAS aux machines françaises (voire européennes) (financements aux USA x10 à 100 pour leurs QPU providers)
- Besoin d'industrialiser les solutions *cloud* et d'optimiser les simulateurs (temps de simulation encore trop long) chez les providers de qubits français.
- Les solutions *clouds* actuelles d'accès aux calculateurs quantiques ne sont pas compatibles des contraintes de sécurité des industriels du GIFAS. Il faut développer un cloud cybersécurisé permettant l'accès aux machines avec des niveaux de sensibilités élevés. La mutualisation d'un ensemble de machines dans un centre dédié est à étudier en fonction de modèles économiques (temps d'amortissement des machines, dans le HPC le temps moyen de la maintenance est de 5 ans, dans le cas du quantique les progrès du hardware étant rapide, une machine sera très vite dépassée). Le coût d'une heure de calcul en mode QCaaS (Quantum Computing as a Service) serait entre 1k\$ et 5k\$. En raison du prix des machines et de leurs évolutions rapides, très peu d'utilisateurs opteront pour une solution locale et la demande se portera sur des solutions externalisées et mutualisées. A terme ce qui sera recherché, pour les applications sensibles, c'est une solution quantique globale qui implique de disposer d'un réseau protégé de bout en bout entre les utilisateurs et les machines de production. Le financement d'un réseau national relevé d'un modèle économique différent de celui du financement des start up *provider* d'accélérateur quantique, et doit être pris en compte dès à présent en raison des coûts et du temps de déploiement.

## 3.4 Conclusions et recommandations

Il convient tout d'abord de rappeler que le Quantum Computing n'est pas destiné à remplacer tout le HPC, l'avantage quantique sera réservé à certaines applications. Il convient également de rappeler que l'avantage quantique sur des problèmes d'intérêts pratiques n'est pas encore acquis et dépendra des progrès techniques et scientifiques qui pourront être réalisés dans les prochaines années.

La fin de la loi de Moore sur le HPC impose pour monter en puissance de calcul, de passer à de nouvelles technologies, il faut encourager les entreprises à se lancer dans le quantique car la prise de risque n'est pas si importante et reste faible par rapport au risque de rater un virage technologique disruptif.

Si la réalisation de calculs quantiques à applications industrielles ne semble pas pour tout de suite, la route est cependant pavée de jalons (machine NISQ, FTQC, LSQ). La prise en main du calcul quantique peut se faire dès à présent par l'accès à des simulateurs/émulateurs et en 2024 à de vraies machines. Même si l'ère NISQ ne permet pas d'atteindre des objectifs de calcul opérationnel, elle ouvre la voie à une réflexion qui peut être profitable au calcul classique (déquantification). L'enjeu pour challenger le HPC classique est de réussir à créer un qubit logique avec le moins de qubits physiques, ce qui ouvrira la voie au LSQ. L'introduction du calcul quantique dans le monde industriel implique un éco système

cohérent et mature. Aujourd'hui, le Plan Quantique National répond à un grand nombre de besoins, cependant, un certain nombre d'actions devraient être pérennisées, amplifiées ou lancées.

- ✓ Etendre les activités du projet BACQ. La thématique *benchmarking* est orientée problème générique (simulation physique, optimisation, résolution de systèmes linéaires et factorisation), un benchmark plus orienté verticales industrielles serait profitable. Benchmark portant sur l'environnement et sur des cas d'utilisation. Il permettrait d'établir et de suivre au mieux une roadmap qui aujourd'hui est sujette à trop d'incertitudes en fonction des cas d'application, de la technologie des qubits, et de la disponibilité des algorithmes. Cette action devra être coordonnée avec le LNE et THALES pour étendre les activités de BACQ pour les besoins du GIFAS. Les benchmarks des quatre problèmes génériques pourraient être élargis pour des cas d'usage du GIFAS :
  - ✓ Simulation physique :
    - a. Étude matériaux pour la furtivité (radome, UCAV, ...)
    - b. Etude de poudres propulsives et explosives (munitions, booster à poudre de fusée, ...)
    - c. Étude oxydation
  - ✓ Optimisation
    - a. Optimisation du design des équipements embarqués et de leur emport (antennes Radar/GE/COM embarquées aéroporté ou satellites)
    - b. Aide au déploiement et à la préparation de mission
    - c. Reconfiguration des systèmes complexes en cas de pannes ou de changement de mission
    - d. Optimisation de la trajectoire de drones ou de remote-carrier en essaim
  - ✓ Résolution de systèmes linéaires
    - a. Simulation électromagnétique
    - b. Simulation en mécanique des structures
    - c. Simulation en mécanique des fluides
  - ✓ Factorisation
    - a. Cyber sécurité des plateformes
    - b. Durcissement de codes post-quantiques

Afficher un effort concerté sur le développement de stack logicielles de confiance (maintenues). C'est un sujet global qui regroupe un très grand nombre de points techniques (compilateur, langage, OS, intégration dans les centres de calcul, accès Cloud, ...). Toutefois, les technologies hardware du quantique sont très différentes (ex : atomiques vs photoniques), évoluent rapidement et sont propriétaires, de ce fait développer une stack logiciel universelle dans un environnement qui n'est pas encore mature reste une gageure (et pourrait présenter le risque d'induire une rigidification du hardware). Une stack logiciel développée pour un accélérateur NISQ devra être réécrite pour la prise en compte du traitement des corrections d'erreurs.

- ✓ Favoriser le développement de l'algorithmie quantique orientée vers les besoins industriels et l'étude de nouveaux algorithmes en ruptures pour reprendre le leadership sur les USA.
- ✓ Favoriser l'introduction du calcul quantique dans les entreprises (accélérer la formation continue)
- ✓ En complément des stratégies orientées constructeurs (plan quantique France), il est également crucial d'assurer aux utilisateurs un accès continu aux différentes technologies d'ordinateur quantique déjà disponibles, en France en dehors, à la fois pour des raisons de formation continue, qui se fait actuellement largement de manière autodidacte en expérimentant les différentes technologies, et pour des raisons de benchmarking, il est essentiel pour un industriel de la Défense d'estimer quelle est la technologie la plus adaptée à son usage et comment se comparent ses solutions quantiques à celles de ses concurrents hors Europe. Cette facilitation à l'accès aux heures de calcul

des machines quantiques pour les membres du GIFAS, doit se faire avec des niveaux de sensibilités adaptés pouvant être élevés.

- ✓ Développer une solution d'accès sécurisé aux machines quantiques, soit via des protocoles de calcul encapsulés pour la protection (mais risque d'overheads trop importants en qubits) soit via des protocoles sans overhead mais nécessitant un lien de communication quantique

### 3.5 Synthèse des recommandations

- Encourager le développement de la recherche sur les algorithmes quantiques et les cas d'usage ASD associés (par exemple en soutenant des projets impliquant des industriels du GIFAS et des acteurs académiques du domaine). Cette action pourra s'appuyer sur le projet BACQ existant.
- Faciliter l'accès pour les industriels du GIFAS aux machines quantiques déjà disponibles avec le bon niveau de sécurité : à court terme par la subvention d'heures de calcul pour pouvoir tester des algorithmes élémentaires (ne pas forcément se limiter aux machines françaises dans un premier temps pour ne pas prendre du retard)
- A long terme par le soutien à la maturation technologique d'un réseau quantique pour permettre de faire tourner des algorithmes sensibles ou confidentiels de façon sécurisée via le cloud (et aussi pour interconnecter les calculateurs quantiques)
- Encourager les industriels du GIFAS à adopter et à faire évoluer les benchmarks proposés par le projet BACQ et à en publier les valeurs mesurées afin de partager un outil d'évaluation commun pour suivre quantitativement les progrès des machines quantiques disponibles.
- Encourager le développement de piles logicielles de confiance (compilateur, bibliothèque, outils de programmation/ingénierie logicielle) (pour aller du langage de haut niveau jusqu'au niveau circuit quantique)
- Promouvoir les liens entre HPC classique et calcul quantique, car il est clair que ce dernier ne trouvera d'applications qu'en complément des moyens de calcul classique existants
- Consolider / veiller à être en mesure de garantir une filière industrielle européenne pour garantir à terme l'accès aux machines et un modèle économique viable pour les constructeurs de machines français (subventions à l'achat...)

(page laissée intentionnellement blanche)

# 4. Technologies habilitantes

## 4.1 Résumé aux décideurs

Les technologies quantiques s'appuient sur la maîtrise de plusieurs domaines techniques. On peut en particulier citer : la cryogénie, l'électronique, les lasers, les sources et les détecteurs de photons, les techniques de fabrication de semi-conducteurs, la production de matériaux spécifiques, les technologies du vide...

Ces secteurs sont stratégiques pour mettre en place les futurs systèmes quantiques, mais il faut néanmoins noter qu'ils ne sont pas exclusifs à ceux-ci et peuvent être utilisés pour d'autres applications ce qui éloigne le risque de désintérêt industriel qui serait lié au manque de volume d'équipements à produire.

Il est par ailleurs important de souligner que bien que ces technologies partagent des principes communs, elles ont aussi leurs spécificités et sont à des stades différents de développement et de commercialisation.

La feuille de route technologique fait ainsi apparaître un enchaînement naturel des « produits » quantiques utilisables qui s'organiserait aujourd'hui comme suit : industrialisation des capteurs (en particulier la compacité de ceux-ci), puis les communications quantiques et enfin le calcul. Cette frise chronologique favorisera la maturation des technologies habilitantes décrites dans les sections ci-après de ce chapitre.

Le suivi de cette route permet de souligner l'importance de la bascule vers l'industrialisation des capteurs pour leurs utilisations dans les secteurs aéronautique et spatial. Citons par exemple les gravimètres atomique embarquables, qui sont déjà opérationnels et utilisés pour l'établissement de cartes de gravité.

Pour les communications quantiques, l'objectif est d'établir un (des) réseau(x) puisque l'intention est de distribuer et de manipuler l'information quantique sur de grandes distances, avec un grand nombre d'utilisateurs. Les technologies habilitantes sont celles nécessaires pour construire des infrastructures, organisée, de façon raisonnée, pour constituer une chaîne de la valeur des communications quantiques. On peut donc ainsi souligner que pour ce qui est des sources et systèmes de réception/consommation de la ressource, le niveau de TRL est à 4 chez Thales, et souligner l'importance de la démonstration des démonstrations de 2028 à savoir : établissement d'un segment réseau sol/orbite (satellite QINSAT) avec la démonstration de la distribution d'intrication.

Pour le calcul quantique, le champ des possibles est aujourd'hui important et plusieurs technologies restent en lice : semi-conducteurs ; supraconducteurs ; ions piégés ; à atomes froids ; photoniques. Il semble essentiel à ce stade de ne négliger aucune de ces filières, en soutenant leur développement dans les années qui viennent au cours desquelles des investissements seront encore nécessaires avant de pouvoir bénéficier des premières applications.

## 4.2 Liste des technologies habilitantes

### Cryocoolers pour solutions quantiques embarquées (capteurs ou communication quantique)

- **Fonction** : solution de refroidissement actif de composants quantiques permettant d'atteindre quelques Kelvins, à intégrer dans des solutions autonomes et embarquées : sources et détecteurs de photons uniques, ions terre rare dans les cristaux pour l'analyse RF, certaines formes de mémoire quantique.
- **TRL actuel** : Des systèmes commerciaux à TRL9 existent mais sont fabriqués en nombre, notamment aux Etats-Unis et au Japon, mais leurs facteurs de forme/autonomie/opérabilité ne sont pas compatibles avec des déploiements sur les terrains opérationnels (locaux réseau, capteurs, embarquement à bord d'un avion ou d'un satellite...). A noter que le développement de machines à froid compactes et européennes, mises en série pour ce domaine de température (2-4 K), aura un impact favorable également sur la disponibilité d'une cryogénie ultracompacte dans la une gamme étendue de température (typiquement 20-80K) où pourront être utilisés les cryostats issus de la détection IR.
- **Principe de fonctionnement** : Le domaine des 4K est relativement « chaud » selon les normes cryogéniques et peut être atteint par une boucle de réfrigération en cycle fermé en utilisant hélium comme fluide caloripporteur.
- **Verrous à traiter** :
  - De nombreux éléments de base doivent fonctionner sur une période de temps prolongée avec des opérations de maintenance aussi rares que possible et prenant un temps de court.
  - L'adoption généralisée de la technologie de communication quantique nécessite que les composants fonctionnent sans un support de maintenance technique spécialisé.
  - De nombreuses applications nécessitent des composants ne provenant pas de l'UE27.
- **Action proposée** : Développer une solution EU27 portable et nécessitant peu de maintenance – les acteurs comme AirLiquide, Absolute Systems ou Thales Cryogenics pourraient être impliqués. La cryogénie autour de 4K compacte, compatible de porteurs embarqués et optimisée en consommation est une technologie habilitante clé à développer en Europe pour servir les besoins liés aux développement des capteurs et communications quantiques.

### Matières premières

Les matériaux utilisés pour les technologies quantiques sont variés et dépendent du type de technologie quantique choisie. On peut citer en particulier les supraconducteurs, les aimants (ferroaimants, antiferroaimants, etc.), le silicium, le diamant.

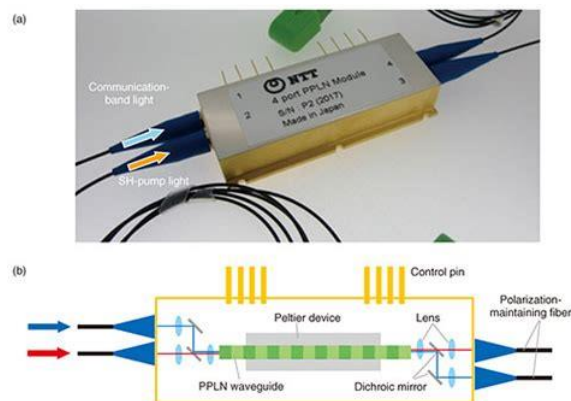
Des capteurs quantiques s'appuient sur des cellules en verre sous vide intégrant l'atome (usuellement Césium ou Rubidium) ou des cellules en verre intégrant l'atome et un mélange de gaz pour fonctionner. Si deux acteurs industriels français travaillent sur des solutions de cellules intégrant du Césium (Thales pour les cellules de taille centimétrique et Tronics pour les micro-cellules), aucune perspective industrielle française rubidium ne semble avoir été financée. Les développements français capteurs quantiques Rubidium s'appuient donc généralement sur des solutions US. Si le soutien des acteurs actuels est indispensable pour conserver la maîtrise de la technologie Césium, leur diversification et/ou la création d'un nouvel acteur industriel pour les cellules rubidium seraient un atout pour les technologies dépendant de cet atome. Cette diversification pourrait être dans un second temps étendue au Strontium.

## Technologies du vide

Le vide et sa qualité sont des prérequis à la manipulation ou interrogation d'atomes, ions etc. Des filières industrielles françaises existent et commercialisent des solutions s'appuyant sur les technologies du vide et de l'ultravide.

### Cristaux non-linéaires haute brillance

- **Fonction** : les cristaux dits « non-linéaires » sont des cristaux dans lesquels on peut activer des processus d'optique non-linéaire, c'est-à-dire des processus durant lesquels la longueur d'onde de la lumière transmise est modifiée par rapport à la longueur d'onde de la lumière avec laquelle on les éclaire. Ces processus ont la faculté de générer des photons appariés dans un état intriqué sur l'observable temps-énergie. Ils sont à la base de la génération de la ressource d'intrication des RIQ.
- **Principe de fonctionnement** : Un laser dit 'de pompe' éclaire le cristal. Avec une faible probabilité, le cristal peut absorber un photon de la pompe et réémettre son énergie partagée entre deux photons partenaires qui sont émis simultanément, dans un état intriqué. On appelle *conversion descendante spontanée paramétrique* ce phénomène et on appelle la 'brillance' de ce cristal la grandeur qui caractérise l'efficacité de ce processus de génération de photons intriqués. Elle s'exprime en nombre de photons émis par unité de puissance et par unité de fréquence de la largeur de bande du laser de pompe.
- **TRL actuel** : il existe des cristaux non linéaires disponibles dans le commerce à des prix relativement élevés, mais leurs conditions de fonctionnement en environnement spatial ne sont pas encore bien connues. De plus les fournisseurs de ces cristaux sont essentiellement asiatiques, ce qui pose un problème d'autonomie stratégique.
- **Verrous à traiter** : outre les deux aspects autonomie stratégique et spatialisation, il convient de travailler sur la brillance de ces cristaux, afin d'améliorer, si possible de l'améliorer de plusieurs ordres de grandeur.
- **Actions proposées** : soutenir les acteurs de la filière optique notamment Exail afin de leur permettre d'identifier des matériaux ayant une potentialité de brillance supérieure au Niobate de Lithium actuellement utilisé, ainsi que les dispositifs de montage ou d'environnement permettant de maximiser cette potentialité.



Cristal non-linéaire monté dans un contrôleur de température de la société NTT (Japon)

A noter qu'à plus long terme, la disponibilité d'éléments non-linéaires réalisés directement en technologie « photonique intégrée » (niobate sur Si ou sur SOI) sera également très intéressante pour l'ensemble des capteurs (sources lasers accordables pour le contrôle des atomes froids, des atomes de Rydberg, pour les horloges atomiques, les ions terres rare...)

## Circuits photoniques intégrés (PIC)

- **Fonction** : Ces plateformes permettent une intégration optimale et une réduction ultime de la taille des dispositifs photoniques nécessaires au fonctionnement des systèmes quantiques, à la fois pour les capteurs, la communication et l'informatique quantique. Les circuits photoniques intégrés (PICs) peuvent inclure toutes des fonctions passives (guides, lignes à retard, coupleurs directionnels, filtres spectraux, contrôle de la polarisation) et actives (modulateurs, commutateurs, convertisseurs de fréquence non-linéaires, sources lasers, amplificateurs...). Toutes ces briques peuvent être intégrées sur le même dispositif en hybridant différentes plateformes (Si, SiN, LiNbO<sub>3</sub>, InP,...).
- **TRL actuel** : La technologie PIC est largement déployée dans les applications de télécommunications terrestres (TRL 9). Pour les communications quantiques, les principales fonctions requises pour la génération, la transmission, la manipulation et la détection de qubits ont été implémentées dans la technologie PIC jusqu'à un TRL 4. Des développements sont également en cours, notamment à Thales R&T, pour implémenter sur PIC des fonctions nécessaires à la manipulation d'atomes par laser.
- **Principe de fonctionnement** : Des motifs tels que des guides d'ondes et des composants sont formés sur des tranches de matériau par photolithographie. Cela permet une intégration bien plus grande, de la même manière que les circuits intégrés électroniques.
- **Verrous à traiter** :
  - Exécution des fonctions critiques avec la technologie PIC avec une performance qui respectant les spécifications.
  - Coût d'entrée important qui ne devient rentable que pour les grandes séries de production.
  - Besoin des développements compatible avec des exigences de l'espace (fiabilité).
- **Action proposée** : Stimuler le transfert de technologie des laboratoires via la montée en puissance des start-ups.

## Lasers pour les technologies quantiques

Ils sont utilisés notamment avec les **atomes froids**, des **ions piégés** et les **qubits de photons**, ainsi qu'avec des équipements quantiques. Le domaine des lasers est très diversifié avec des produits couvrant différentes gammes de longueurs d'onde, puissance, lasers continus vs pulsés, etc. On peut par exemple citer la nécessité de lasers bleus continus à la fois puissants (1W) et fins spectralement (<100kHz) pour les capteurs Rydberg ou les ions piégés. Bien que le développement d'une filière nationale ou au moins européenne soit absolument indispensable pour l'ensemble des capteurs, communications et calcul quantiques, la diversité de ce domaine « lasers pour les QTs » rend une action concertée nationale relativement difficile à mettre en place. Un premier pas a été fait avec la mise en place, dans le cadre du plan quantique national du projet AtomQTRL, mais celui-ci reste bien modeste et trop focalisé sur les seuls besoins « calcul/simulation » alors que les capteurs et les communications quantiques devraient être la priorité à court et moyen terme. Le besoin de lasers dans les domaines de longueur d'ondes du visible et du très proche infra-rouge ne sera pas comblé par le développement de sources pour les télécoms : des développements spécifiques pour une émission directe ou pour conversion non-linéaire de longueur d'onde sont absolument nécessaires à l'avènement d'un réel écosystème national quantique.

## Détecteurs de photons haute efficacité / faible bruit

- **Fonction** : Les détecteurs de photons participent à la réalisation de plusieurs fonctions. En aval d'un dispositif analyseur d'état, ils permettent de finaliser la mesure de l'observable d'encodage et de ce fait de récupérer une partie de l'information quantique portée par le photon. Dans un dispositif de mesure de Bell, ils participent à la commutation de l'intrication entre plusieurs paires de photons intriqués.



- **Principe de fonctionnement** : il existe plusieurs types de détecteurs de photons. Les détecteurs de la famille des photomultiplicateurs (y c. les photodiodes à avalanche) absorbent le photon par effet photoélectrique, et ensuite accélèrent le photoélectron qui en résulte pour lui faire déclencher une cascade de d'électrons secondaires qui mènent à un courant macroscopique. Les détecteurs supraconducteurs utilisent le fait que le passage d'un photon dans un milieu supraconducteur va briser localement la supraconductivité, et générer une résistance non-nulle, donc une tension mesurable aux bornes du matériau.
- **TRL actuel** : il existe des produits commerciaux de TRL9, mais qui ne combinent pas facteur de forme et performance nécessaires à nos systèmes.
- **Verrous à traiter** : Les supraconducteurs sont très efficaces (un photon qui le traverse a une très grande probabilité d'être détecté) et peu bruités : le nombre de fausses détections est de l'ordre de la centaine par seconde. Mais ils requièrent un cryocooler dont les modèles actuels sont peu compatibles avec la fiabilité en opération ou la transportabilité : ce sont les verrous de cette catégorie (cf. les recommandations sur le développement d'une cryogénie souveraine embarquable à 2-4K). Les photomultiplicateurs à l'inverse, sont miniaturisés, mais la probabilité de détection d'un photon est nettement plus basse, de plus, ils présentent des taux de fausses détection (courant d'obscurité) d'un ordre de grandeur supérieur : ce sont les verrous de cette catégorie.
- **Actions proposées** : pour les supraconducteurs, rechercher des designs qui continuent à approcher leur efficacité de 100%, et soutenir la miniaturisation des cryocoolers ou utiliser des supraconducteurs à plus haute température ; pour les photomultiplicateurs, avancer vers des combinaisons matériaux/design qui améliorent efficacité et courant d'obscurité – en s'appuyant sur le savoir-faire des laboratoires et industriels qui maîtrisent ces objets.



*Détecteur supraconducteur de photons et cryocooler de la société IDQuantique (Suisse)*

### **Sources de photons uniques, si possibles non-cryogéniques**

- **Fonction** : Des sources de photons uniques (par opposition aux sources cohérentes très atténuées) sont requises pour les applications qui utilisent des qubits photoniques (par ex. ordinateurs quantiques photoniques). Ils seront généralement utilisés dans les dispositifs quantiques communicants et ne font pas partie intégrante du réseau d'information quantique lui-même, qui repose plutôt sur la distribution par intrication. Une source de photon unique peut être exploitée pour la cryptographie quantique, mais n'est pas obligatoire puisque le protocole BB84-decoy permet l'utilisation des sources cohérentes atténuées
- **TRL actuel** : 3
- **Principe de fonctionnement** : On peut exciter un système à deux niveaux afin d'émettre un photon unique. Des systèmes adaptés sont

- Une atome neutre unique
- Un ion unique
- Une molécule unique
- Un centre de couleur dans le diamant
- Une boîte quantique
- Une source à conversion paramétrique descendante spontanée (SPDC) en exploitant émission annoncée
- **Verrous à traiter** : Brilliance/bande passante, facteur de forme, Poids, Pas de cryogénie ou cryogénie simplifiée
- **Action proposée** : Stimulation de l'écosystème français (e.g. Quandela), en synergie avec les recommandations plus générales sur les lasers et sur les PICs.

## Technologies pour les ordinateurs quantiques à l'état solide

Les **câbles supraconducteurs** et les filtres jouent un autre rôle clé, en particulier pour les qubits à supraconducteurs. La réduction des coûts de ces éléments passe par la possibilité de multiplexage des signaux ce qui réduira le nombre de câbles nécessaires et les coûts associés. Une brique technologique importante associée concerne les systèmes de génération de micro-ondes et de lecture de micro-ondes. L'enjeu est d'arriver à les miniaturiser, d'en réduire leur consommation d'énergie et de les placer au plus près des qubits à températures cryogéniques.

Des progrès sont également nécessaires dans le domaine de la **cryo-CMOS<sup>15</sup>** et **l'électronique supraconductrice**. On peut aussi citer la nécessité d'amélioration des **circulateurs** (pour isoler les bits quantiques des bruits indésirables qui pourraient perturber leur état) et des **amplificateurs paramétriques** (pour la détection précise de l'état des qubits lors de l'exécution des algorithmes).

**La fabrication de composants électroniques** est un sujet stratégique s'appuyant sur des techniques de fabrication génériques ou spécifiques aux technologies quantiques comme avec la fabrication de **qubits supraconducteurs** et de points quantiques.

On peut citer également la technologie *FD-SOI (Fully Depleted Silicon On Insulator)* développée par Quobly (ex Siquance), très prometteuse pour réaliser un grand nombre de qubits sur une surface réduite, avec l'électronique de contrôle sur le même substrat. Cette technologie doit être soutenue dans les années qui viennent pour permettre à la France de conserver son avance acquise dans ce domaine grâce aux travaux pionniers du CEA LETI.

## Briques de bases spécifiques aux communications quantiques

### Technologie : Source de photons intriqués spatialisée

- **Fonction** : création de la couche physique d'un réseau d'information quantique – comme les ondes radio en téléphonie mobile.
- **TRL actuel** : il existe sur le marché des sources sol à TRL 8, mais pour le spatial l'état actuel est TRL 4 (démonstration sur table). TRL8-9 sera nécessaire à la mise en œuvre du démonstrateur QINSAT.
- **Principe de fonctionnement** : le principe est de générer des photons par paires dans un même processus physique, de façon à ce qu'ils soient liés, par exemple via une quantité conservée (énergie, etc.). Il existe plusieurs moyens de réaliser une telle source – en général, on éclaire avec un laser un cristal ou une cavité non linéaire qui absorbe les photons reçus et les réémet par paire de photons

---

<sup>15</sup> La cryo-CMOS est une technologie qui permet l'intégration d'un circuit d'électronique classique avec un système quantique. Elle est utilisée pour mesurer le courant à travers des boîtes quantiques par des composants électroniques CMOS sur une seule puce refroidie à 10 mK.

de d'énergie moitié. D'autres moyens plus complexes pour l'instant, peuvent aussi être utilisés (boîtes quantiques, etc.). Une fois les paires de photons produites, l'intrication peut être portée par différentes observables (temps/énergie, polarisation, moment cinétique, etc.).

- **Verrous à traiter** : ils sont de plusieurs nature.
  - Fonctionnellement, une annonce de la création de paires est souhaitable, mais encore non réalisée à des débits raisonnables, ce qui nécessite d'autres mesures pour contrôler le processus.
  - Du point de vue des performances, une augmentation du débit par rapport aux valeurs actuelles est souhaitable (dépasser le milliard de paires par seconde).
  - Du point de la robustesse à l'environnement spatial, tout reste à faire pour des sources qui puissent opérer en orbite (mécanique, thermique, radiations).
- **Action proposée** : développer une telle source dans le cadre du programme national QINSAT avec une contribution du plan quantique (cf recommandations « Lasers pour QTs », « PICs » et « Sources de photons uniques, si possibles non-cryogéniques ». Tous ces développements doivent s'inscrire dans une feuille de route globale, nationale ou plus probablement européenne).



*Source de photons intriqués de la société OZ optics (Canada)*

### Technologie : Routeurs d'intrication

- **Fonction** : commuter la ressource d'intrication de lien en lien de façon à propager ces corrélations quantiques vers les utilisateurs qui la consommeront. Ces terminaux participent à l'interface entre les réseaux spatiaux et terrestres.
- **TRL actuel** : état actuel est TRL 2 (design et validation de composants). TRL8-9 sera nécessaire pour la deuxième phase du démonstrateur QINSAT.
- **Principe de fonctionnement** : un routeur est à l'interface entre plusieurs liens créés par autant de sources d'intrication (en orbite ou au sol). Le routeur reçoit des instructions pour connecter deux liens suite à la demande d'un utilisateur et de l'identification du chemin optimal les connectant. Il va connecter ces deux liens en réalisant une mesure de Bell sur une paire de photons dont chacun arrive d'un lien différent. L'effet de cette mesure est de propager l'intrication en intriquant les deux autres photons émis par ces deux sources.
- **Verrous à traiter** : ils sont de plusieurs nature.
  - Il convient de pouvoir réaliser un jeu de mesures de Bell aussi complet que possible, et donc de disposer d'un analyseur d'états complet.
  - Pour fluidifier les opérations, il est nécessaire de pouvoir stocker les photons reçus quelques temps dans une mémoire quantique (voir fiche correspondante)
  - La synchronisation précise des mesures de Bell afin de pouvoir identifier l'autre photon vers qui l'intrication a été propagée.
- **Action proposée** : développer une telle interface spatiale en lien avec les acteurs terrestres pour préparer la phase 2 de la démonstration QINSAT, qui enchaînera plusieurs liens d'information quantiques.



*Routeur d'intrication terrestre de la société Qunnect (USA)*

Ce besoin s'inscrit également dans le cadre de celui fait pour les PICs

### Technologie : Terminaux récepteurs d'intrication

- **Fonction** : recevoir les photons intriqués à chaque extrémité d'un lien, créé par une ou plusieurs sources, pour les consommer. Ces terminaux participent à l'interface entre les réseaux spatiaux et terrestres.
- **TRL actuel** : état actuel est TRL 4 (démonstration sur table). TRL8-9 sera nécessaire à la mise en œuvre du démonstrateur QINSAT.
- **Principe de fonctionnement** : un tel récepteur est placé dans une station sol en sortie du télescope qui collecte les photons qui arrivent de la source en orbite. Il est constitué d'un analyseur d'état qui fixe un contexte de mesure en séparant les photons selon les différentes modalités de l'observable qui encode l'intrication (filtres polarisant, interféromètres de Michelson etc. en fonction de l'observable choisie), puis détecte les photons sur des compteurs de photons, et enfin reconstitue la date d'émission du photon reçu de façon retrouver son partenaire dans l'autre station sol.
- **Verrous à traiter** : ils sont de plusieurs nature.
  - La performance de détection, qui s'appuie sur des détecteurs à la fois efficaces et peu bruités – donc le plus souvent cryogéniques.
  - La datation précise de la détection, afin de pouvoir retrouver sans erreur le photon partenaire s'il est arrivé à l'autre station sol.
- **Action proposée** : développer une telle source dans le cadre du programme national QINSAT avec une contribution du plan quantique.

### Technologie : Terminaux de clés quantiques

- **Fonction** : Leur fonction est de générer une clé aléatoire partagée entre deux nœuds, Alice et Bob, tout en garantissant que toute information mutuelle supplémentaire pouvant être obtenue par un attaquant, Eve, est garantie inférieure à une valeur spécifiée,  $\epsilon$ . La clé partagée peut être utilisée pour des applications cryptographiques. Cette méthode se distingue des méthodes cryptographiques actuelles puisqu'elle ne repose pas sur des hypothèses de complexité informatique et est donc à l'abri des développements en cryptanalyse, y compris ceux basés sur l'informatique quantique.
- **TRL actuel** : 8 (il manque l'homologation de sécurité par une agence habilitée)
- **Principe de fonctionnement** : Les protocoles dits 'Prépare et Mesure' (PM) exploitent des informations encodées par Alice sur des modalités de contextes incompatibles de photons individuels ('variables discrètes') ou d'impulsions cohérentes faibles ('variables continues'). Bob effectue une série

de mesures sur ces mêmes signaux optiques, en utilisant des contextes de mesure choisis aléatoirement pour ne pas être tout le temps compatibles avec le contexte d'encodage. En échangeant des informations sur un canal public authentifié, Alice et Bob sont alors en mesure de générer une suite de données possédant de 'l'information mutuelle' supérieure à celle entre Alice et un éventuel espion. Le canal classique peut être authentifié par une clé pré-partagée, auquel cas la procédure est *sûre inconditionnellement* ('Information Theoretically Secure' – ITS). Alternativement, il peut être authentifié au moyen d'une procédure de clé publique (y compris la cryptographie post-quantique), auquel cas la procédure est dotée de *sécurité persistante* ('Everlasting Security').

- **Verrous à traiter** : Les terminaux QKD sont actuellement commercialisés. Toutefois, une adoption généralisée en Europe est entravée par les facteurs suivants
  - Débit plus élevé, surtout sur de longues distances
  - Des implémentations 'UE27' sont requises pour les applications CE
  - Les équipements doivent être développés dans un environnement sécurisé
  - Compatibilité avec les communications classiques mutualisées
  - Nécessité de critères communs pour l'acceptation de la sécurité acceptés par les agences de sécurité nationale
  - Standardisation de toutes les interfaces (y compris le canal quantique, la procédure d'authentification et les couches réseau)
  - Moyens d'homologation des équipements sur la base des critères communs
  - Développements des terminaux pour des applications spatiales
- **Action proposée** : Participation des acteurs principaux aux groupes de normalisation. Groupes de travail sur la sécurité et présentations aux groupes de travail. Soutenir l'industrialisation des prototypes de Thales et Exail par des PME.



*Terminal de clés quantiques Toshiba (Japon)*

#### Technologie : Générateurs quantique de nombres aléatoires

- **Fonction** : Générer des séquences de nombres aléatoires qui dont l'aléa est garanti par les lois de la physique quantique, et ne repose pas sur des hypothèses computationnelles ou sur l'ignorance du fonctionnement détaillé d'un dispositif.
- **TRL actuel** : état actuel est TRL 8 au sol, TRL 4 pour le spatial en Europe mais rien en France. TRL8-9 sera nécessaire pour la mise en œuvre de la composante spatiale de réseaux sécurisés par voie quantique (SAGA, IRIS<sup>2</sup>).
- **Principe de fonctionnement** : il existe différentes mises en œuvre, mais le principe de fonctionnement est toujours le même. On prépare un système quantique dans un contexte initial (p.ex. état

d'énergie d'un atome isolé, photon polarisé verticalement etc), puis on l'observe dans un contexte de mesure différent (P.ex. introduction d'une interaction électromagnétique avec l'atome, filtre polarisant oblique, etc), ce qui force les résultats de mesure à être aléatoires.

- **Verrous à traiter** : ils sont de plusieurs nature.
  - Ces dispositifs ne doivent pas être biaisés par des problèmes de réglage (angle du polarimètre) ou d'influence extérieure.
  - Il convient de réaliser des équipements qui génèrent des giga-octets de nombres aléatoires par seconde, ce qui suppose des détecteurs rapides et non bruités, et une électronique de contrôle rapide.
  - Il convient enfin d'optimiser les algorithmes qui transformeront la séquence brute en séquence garantie.
- **Action proposée** : développer un tel générateur en national ou dans le cadre de la contribution française au programme SAGA de l'ESA.



*Générateur quantique de nombres aléatoires de la société QuSide (Espagne)*

### Technologie : Systèmes de gestion de clés

- **Fonction** : Le mécanisme QKD génère une clé partagée entre deux nœuds au niveau du lien. Un système de gestion des clés est nécessaire pour
  - Générer des clés pour l'utilisateur final en exploitant des clés au niveau du lien
  - Effectuer la gestion du cycle de vie des clésCes fonctions doivent être exécutées en garantissant que le haut niveau de sécurité atteint par le protocole QKD ne soit pas dilué.
- **TRL actuel** : Les KMS classiques sont répandus avec un TRL 9. Ceux développés pour la QKD sont commercialisés (par exemple par Toshiba et IDQuantique) avec un TRL9. Des travaux de normalisation sont toujours en cours. Dans EuroQCI THALES prototype un KMS compatible avec ses produits de chiffrement et le contrôleur de réseau AIRBUS.
- **Principe de fonctionnement** : Le matériel de clé au niveau du lien est généré par QKD. En fonction des instructions de la couche de contrôle, le KMS exploite les clés intermédiaires pour générer de la clé au niveau du réseau.
- **Verrous à traiter** : Standardisation, Interopérabilité, analyse de sécurité
- **Action proposée** : Participation dans des groupes de standardisation par des acteurs principaux. Groupes de travail ciblés sur la sécurité et présentations aux agences nationaux de sécurité.



*Système de gestion de clés de la société Huawei (R.P. Chine)*

### Technologie : Lasers télécom bande étroite, spatialisés

- **Fonction** : on utilise essentiellement les lasers pour pomper les cristaux non-linéaires et déclencher les processus de génération de photons intriqués. Ces lasers peuvent également servir au contrôle et à l'activation des dispositifs de mémoire quantique. En outre, ils sont également utilisés dans plusieurs types de capteurs quantiques.
- **Principe de fonctionnement** : leur principe de fonctionnement est similaire à celui des lasers habituels. Les paramètres importants sont d'une part la largeur de bande de la lumière émise par ces lasers, mais aussi la stabilité des longueurs d'ondes émises.
- **TRL actuel** : Il existe des lasers bande étroite produits en petite série dans le cadre des capteurs quantiques. Leur niveau de qualification permet de les évaluer à un TRL 8. Par contre leur fonctionnement en environnement spatial n'est pas connu. De plus, leur pilotage en puissance et en impulsion sera un élément clé de leur utilisabilité.
- **Verrous à traiter** : il convient de mettre sur le marché des lasers ayant des propriétés proches de celles des composants utilisés dans les capteurs quantiques, et aptes à fonctionner en environnement spatial.
- **Actions proposées** : financer la spatialisation d'un produit laser télécom existant sur le marché des capteurs quantiques comme ceux d'Exail ou de Lumibird.

(cf.recommandations « lasers pour QTs », « PICs »,.... Cette recommandation s'inscrit dans un contexte plus large concernant « capteurs », « communications » et « calcul » quantiques).

### Technologie : Systèmes de synchronisation et de datation ultra précis

- **Fonction** : les photons que l'on utilise en communications quantiques sont des particules indiscernables. Une fois longueur d'onde et polarisation fixées, la seule 'étiquette' pour les identifier est leur date d'émission. Aussi, il est critique pour la mise en œuvre d'un, puis de plusieurs liens réseau, de disposer d'une telle étiquette de haute fiabilité.
- **Principe de fonctionnement** : plusieurs options sont possibles. On peut soit s'appuyer sur un système de distribution du temps indépendant, de type GNSS, et dans ce cas, il va être clé d'associer les détecteurs d'une part à une horloge physique stable et d'autre part à des algorithmes de synchronisation précis. On peut également distribuer un temps de référence via des signaux optiques co-transmis avec le signal quantique, ce qui suppose d'avoir les moyens d'éviter le brouillage du

second par le premier. Dans tous les cas la performance de datation doit être meilleure que la nanoseconde en temps réel. Elle va conditionner le débit.

- **TRL actuel** : il existe des équipements de laboratoire dont les performances approchent potentiellement le besoin. Mais il convient de développer des produits qui sont d'une part conçus pour fonctionner avec une partie en orbite, dans un réseau de communication quantique (en particulier avec les bonnes interfaces) et d'autre part produits en grand nombre, car chaque nœud réseau en comptera au moins un.
- **Verrous à traiter** : définition des interfaces, moyens de filtrage optique, algorithme de restitution instantanée
- **Actions proposées** : dans le cadre des études système des guichets nationaux, comparer GNSS et distribution optique de temps, fixer les interfaces afin de permettre le développement d'équipements utilisables, avec des acteurs comme SigmaWorks.

### Technologie : Mémoires quantiques longue cohérence, facilement adressables

- **Fonction** : Un réseau d'information quantique est d'abord un système qui produit de la ressource d'intrication sur des liens élémentaires, puis commute cette ressource de lien en lien pour générer de l'intrication à longue distance. Cette ressource se présente sous la forme de systèmes quantiques dans un état corrélé et délocalisé – c'est-à-dire intriqué. Une particularité des communications quantiques est qu'en principe, une fois cette ressource établie, on n'est pas obligé de la consommer immédiatement en exécutant des protocoles de téléportation, de synchronisation ou de clés. Pour pouvoir attendre, il faut pouvoir stocker cet état corrélé dans des dispositifs que la communauté appelle mémoires quantiques. A plus court terme, de telles mémoires soulageront les contraintes de synchronisation des opérations réseau.
- **Principe de fonctionnement** : plusieurs plateformes matérielles sont envisagées, avec leurs avantages et inconvénients. Les nuages d'atomes très froids (millikelvins), les noyaux d'isotopes fermioniques du carbone dans les diamants, certaines impuretés de terres rares dans des cristaux optiques peuvent jouer ce rôle. Le plus souvent, il s'agit d'activer une propriété stockante en activant une partie du système par excitation laser, qui permet d'écrire l'état dans la mémoire, puis de le lire à la demande.
- **TRL actuel** : des démonstrateurs de laboratoire atteignent un TRL de l'ordre de 4, avec des probabilités d'accès d'au mieux 90% et des temps de stockage en dizaines de microsecondes. Elles seront nécessaires dans la deuxième phase de TeQuant, après la première démonstration d'un lien bord-sol.
- **Verrous à traiter** : probabilité de succès d'écriture/lecture proche de 100%, temps de stockage maintenant la cohérence quantique au-delà de la seconde, fidélité de l'état restitué à l'état écrit proche de 100%, capacité à recevoir des signaux quantiques dans une bande large ou du moins à longueur d'onde modulable.
- **Actions proposées** : soutenir des actions d'exploration avancée des possibilités de plusieurs plateformes matérielles dans les entreprises comme WeLinq (atomes froids) ou Thales + académiques (ions terres rares).





*Mémoire quantique de la société Qunnect (USA)*

### Technologie : Optique adaptative légère et bas cout

- **Fonction** : Plusieurs applications nécessitent qu'un canal optique en espace libre soit injecté dans une fibre optique monomode. Un exemple de tel système est un système QKD basé sur satellite qui utilise des détecteurs de photons uniques à nanofils supraconducteurs. Ceci est réalisé en focalisant le faisceau pour produire une tache lumineuse aux dimensions qui lui permette d'entrer aussi entièrement que possible dans la fibre monomode (couplage des modes spatiaux espace libre et fibre). Cependant, en présence de turbulences atmosphériques, le front d'onde reçu du satellite subit des perturbations de phase, et la tache lumineuse résultant est déplacée, étalée et déformée, et ce qui rend difficile le couplage dans les fibres. Une optique adaptative est nécessaire pour redresser le front d'onde en corrigeant les erreurs de phase, et améliorer le couplage.
- **TRL actuel** : L'optique adaptative est très mature dans le domaine de l'astronomie (TRL 9) et a été déployée dans le domaine des communications optiques en espace libre (TRL9). Il est encore en développement pour les applications de communications quantiques
- **Principe de fonctionnement** : Une partie du faisceau entrant est dirigée vers un capteur de front d'onde (par exemple une matrice Shack Hartmann). En fonction des erreurs de front d'onde détectées, l'électronique de contrôle commande en temps réel un petit miroir déformable pour corriger les erreurs de phase. A noter que ce principe de compensation de défauts de phase peut également être mis en œuvre au moyens de circuits en photonique intégrée (cf. projet européen VERTIGO). Le TRL dans ce cas n'est pas au niveau de celui des miroirs déformables, mais la compacité et la simplicité de commande en font une technologie candidate extrêmement prometteuse, d'ores et déjà démontrée dans le domaine des communications optiques « classiques » et à valider dans celui des communications quantiques.
- **Verrous à traiter** : Les systèmes Space QKD nécessiteront un déploiement généralisé de modules d'optique adaptative. Cela nécessitera :
  - Solutions à faible coût
  - Solutions à faible maintenance
  - Solutions capables de fonctionner dans des environnements urbains très turbulents
- **Action proposée** : pour l'optique adaptative, s'appuyer sur les entreprises existantes (par exemple ALPAO, ImagineOptics) pour cibler cette gamme de produits, en s'appuyant sur la recherche publique déjà effectuée dans le domaine notamment à l'ONERA. Pour les PICs, s'appuyer sur les développements en cours, au niveau européen pour les communications classiques et en valider la transposition aux communications quantiques.

## Technologie : Systèmes de contrôle de la polarisation

- **Fonction** : Le degré de liberté photonique de polarisation est fréquemment utilisé pour les communications quantiques, en particulier les transmissions en espace libre. Cependant la polarisation demande d'être contrôlée avec soin. D'une part le satellite est en rotation par rapport au récepteur et les directions de polarisation changent avec cette rotation. D'autre part l'état de polarisation peut être dégradé par le canal de communication. Une partie de ces perturbations peut être corrigée en appliquant des transformations unitaires au signal reçu.
- **TRL actuel** : Pour les applications QKD TRL 9 pour les systèmes simples (rotation de phase uniquement) (IQOQI - Autriche).
- **Principe de fonctionnement** : Un système typique utilise une référence de polarisation co-localisée avec la source. Un module de détection au niveau du récepteur caractérise les perturbations de polarisation. Enfin, la polarisation est corrigée. Un moyen d'y parvenir consiste à utiliser une lame demi-onde motorisée (pour mettre en œuvre une rotation de polarisation) ou par une combinaison de deux plaques à quarts d'onde et une lame demi-onde pour mettre en œuvre toute transformation unitaire.
- **Verrous à traiter** : Coexistence avec canaux quantiques et canaux classiques. Simplicité. Vérification de compatibilité avec démonstrations de sécurité.
- **Action proposée** : Développements dans le cadre des projets tel TeQuants pour préparer le démonstrateur en orbite QINSAT.

## Technologie : Dispositifs de distillation d'intrication

- **Fonction** : la ressource des réseaux d'information quantique est l'intrication entre des photons générés simultanément puis distribués vers différents nœuds du réseau. Si les sources que nous envisageons produisent en théorie des paires de photons maximales intriquées (les amplitudes de probabilité des deux modalités de mesures sont de même module), la mise en œuvre concrète de la génération puis de la propagation et enfin de l'analyse peut dégrader cette symétrie et diminuer le taux d'intrication de la ressource, ce qui impacte la performance des transmissions. La fonction est de rétablir le niveau d'intrication aussi proche du maximum que possible.
- **Principe de fonctionnement** : le principe est simple : il s'agit de collecter un certain nombre de systèmes de photons de niveau d'intrication dégradé pour en produire un nombre plus petit mais de plus forte intrication – d'où la notion de distillation. La mise en œuvre concrète utilise d'une part des mémoires quantiques permettant d'accumuler les systèmes élémentaires, et de dispositifs de type mesure de Bell successives pour progressivement augmenter le niveau d'intrication en consommant une partie des systèmes élémentaires.
- **TRL actuel** : des concepts et de preuves de principe élémentaires existent à un TRL de l'ordre de 3. Il est tributaire du TRL des mémoires. Ces dispositifs seront nécessaires après la première démonstration d'un lien bord-sol.
- **Verrous à traiter** : mémoires et transfert fidèle des degrés de liberté photoniques sur des degrés de liberté matériels, mesures de Bell en cascade.
- **Actions proposées** : encourager cette piste dans les laboratoires d'optique quantique, et la soutenir dans les start-ups qui travaillent sur les mémoires quantiques

# 5. Formation

Le développement des technologies quantiques implique un besoin croissant en termes de formation d'ingénieurs et de techniciens. La formation est prise en compte dans le Plan Quantique National (projet QuantEDu). Elle est encore en évolution mais se structure, illustrons par deux exemples :

## UPSaclay :

M2 QLMN (Quantum Light Matter & Nanosciences), M1 QDCS (Quantum & Distributed Computer Science), ARTeQ, QUARMEN (Erasmus Mundus), parcours Quantum Engineering à Telecom Paris et à CentraleSupélec, complété par les formations Ingénieur à l'IPP (X, Ensta)

## Paris Centre :

- Sorbonne Université : Masters en Computer Science - Quantum Information Course (M1+M2), en Physics - Quantum Information Course (M2), et Light, Matter, Interactions – LUMI (M2), Université Paris Sciences et Lettres : Master Quantum Engineering (M1+M2)
- Master International Center for Fundamental Physics (ICFP) - Quantum Physics Course (M2), ENS-PSL, Sorbonne Université, Université Paris Cité
- Master in Physics and Applications, Quantum Devices track, Université Paris Cité
- Master in Physics and Applications - NanoQuad International Double Degree Course (M1+M2), Université Paris Cité, Politecnico de Turin

Les formations portent sur la science du quantique, les technologies, la cryptographie, mais il y a encore peu de formations dédiées au calcul quantique proprement dit. Même si le nombre de formations augmente, le nombre d'étudiants dans chaque formation étant limité, le nombre d'étudiants en sortie est restreint. Un certain nombre d'étudiants s'orientent vers des thèses en dehors de la France (laboratoire universitaire en Suisse en lien avec IBM, laboratoire de recherche à Delft...), et/ou sont ensuite recrutés par des start-ups ce qui pèse sur les laboratoires académiques (difficulté de recruter des postdocs notamment).

La formation continue va être une composante importante pour les industriels pour former leurs ingénieurs, car la formation initiale ne fournira pas le contingent de jeunes diplômés nécessaire pour remplir les besoins. Une difficulté peut apparaître liée aux fondements mathématiques de la théorie quantique, qui nécessiteront sans doute de mettre en place plusieurs niveaux dans l'offre de formation continue aux technologies quantiques.

Une bonne connaissance de l'algorithmie classique étant nécessaire pour appréhender les enjeux du calcul quantique, il serait également pertinent de développer de telles formations dans le cadre du plan quantique national.

## Quelques recommandations...

- Eviter ce qui s'est passé pour le HPC au niveau de la formation (notion de Computer Science sous-estimée en France) et de la difficulté de recrutement des talents, qui s'est amplifiée pour l'IA en raison de la forte attraction des GAFA.

- Importance pour l'industrie de la formation continue, soutenir des initiatives type EduQuantum, SAE-EUROSAT, ...

- Si dans la formation d'étudiants on est face à un public homogène, dans le cadre de la formation continue sur le calcul quantique, il faut prendre en compte le profil des utilisateurs, en raison de la disparité de niveau en mathématique/algorithmie. On doit s'orienter sur des formations a deux niveaux, visant ceux qui sont capables de développer des algorithmes et ceux qui vont les utiliser en boite noire. Nécessité de formations continues plus longues d'habituellement (par exemple 2 semaines).

# Glossaire

ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
ASD	Aéronautique - Spatial - Défense
ASIQ	Antenne Supraconductrice à Interférence Quantique
CSAC	Chip Scale Atomic Clock
CSWaP	Cost Size Weight and Power
FTQC	Fault Tolerant Quantum Computing
GNSS	Global Navigation Satellite System
HPC	Calcul Haute Performance
LSQ	Large Scale Quantum
NISQ	Noisy Intermediate Scale Quantum
NIST	National Institute of Standards and Technology (US)
NV	Nitrogen Vacancy
OCXO	Oven Controlled X-tal(Crystal) Oscillator
PIC	Photonic Integrated Circuit
QC	Quantum Computing
QCaaS	Quantum Computing as a Service
QFT	Quantum Fourier Transform
QIN	Quantum Information Network
QINSAT	Quantum Information Network Satellite
QKD	Quantum Key Distribution
QML	Quantum Machine Learning
QPIC	Quantum Photonic Integrated Circuit
QPU	Quantum Processing Unit
RIQ	Réseau d'Information Quantique
RMN	Résonance Magnétique Nucléaire
SHOM	Service Hydrographique et Océanographique de la Marine
SQUID	Superconducting Quantum Interference Device
SQUIF	Superconducting Quantum Interference Filter
SWaP-C	Size Weight and Power-Cost
TCXO	Temperature Compensated X (Crystal) Oscillator
TRL	Technology Readiness Level