ASSEMBLÉE NATIONALE

XV^e LÉGISLATURE

Compte rendu

Office parlementaire d'évaluation des choix scientifiques et technologiques

Jeudi 21 octobre 2021
Séance de 9 heures 30

Compte rendu n° 119

SESSION ORDINAIRE DE **2021-2022**

Présidence de M. Cédric Villani, *président*

ASSEMBLÉE NATIONALE

Office parlementaire d'évaluation des choix scientifiques et technologiques

Jeudi 21 octobre 2021

– Présidence de M. Cédric Villani, député, président de l'Office –

La réunion est ouverte à 9 h 35.

Audition publique sur la stratégie quantique de la France

M. Cédric VILLANI, député, président de l'Office. - Chers collègues, chers invités, je vous souhaite la bienvenue. Nous sommes réunis ce matin pour une audition publique sur la mise en place et l'avancement de la Stratégie quantique de la France. De la même façon que l'intelligence artificielle, le quantique fait partie des évolutions technologiques dont nous entendons régulièrement parler dans l'actualité et il était naturel que l'OPECST s'y intéresse. Entre les mois de mars et juillet 2019, l'Office a publié quatre courtes notes sur les technologies quantiques après avoir auditionné de nombreux acteurs, de la recherche fondamentale aux grands groupes industriels en passant par des *start-up*, le tout formant l'écosystème quantique français en liaison avec l'écosystème quantique international : *Les technologies quantiques : introduction et enjeux ; L'ordinateur quantique ; La programmation quantique ; Cryptographie quantique et post-quantique.*

En janvier 2020, la députée des Français d'Amérique latine et des Caraïbes, Mme Paula Forteza, a remis au gouvernement le rapport *Quantique, le virage technologique que la France ne ratera pas*, qui dessine les contours d'une stratégie quantique ambitieuse avec l'objectif des trois « 3 » : 3 axes de R&D : calcul, communication (dont la cryptographie) et capteurs quantiques ; 3 fois plus de budget pour la recherche, soit au moins 1 milliard d'euros sur 5 ans ; création de 3 hubs quantiques à Paris, Saclay et Grenoble, accompagnée d'une restructuration de l'écosystème de recherche attaché.

C'est une course mondiale aux technologies quantiques qui est en cours, avec des répercussions aussi bien scientifiques que stratégiques, voire géopolitiques. La France a tardé, mais y est désormais engagée via sa Stratégie nationale sur les technologies quantiques qui prévoit un plan d'investissement de 1,8 milliard d'euros, dont 1 milliard d'euros de l'État sur les 5 prochaines années. Cette stratégie reprend une large partie des recommandations du rapport de Paula Forteza et s'appuie sur les contributions et les conseils d'un grand nombre de scientifiques, d'industriels et d'institutions. Alain Aspect, membre du conseil scientifique de l'Office, y a été très impliqué.

Nous entendrons tout d'abord une présentation de la Stratégie quantique française, qui sera suivie de deux tables rondes, la première consacrée à l'ordinateur et aux capteurs quantiques, la seconde aux communications quantiques et à la cryptographie post-quantique.

Cette audition est publique. Elle est diffusée en direct puis en différé sur le site du Sénat. Dans la salle et en visioconférence sont présents des parlementaires, députés et sénateurs. Les internautes ont la possibilité de poser des questions en se connectant à la plateforme dont les coordonnées figurent sur les pages internet de l'Office. Nous nous ferons l'écho d'un certain nombre de ces questions auprès des intervenants. L'Office est un organe

bicaméral, ce qui lui confère une grande légitimité, une grande stabilité et une grande indépendance.

Il est intéressant pour le Parlement d'entendre une présentation de la Stratégie nationale quantique française et d'en discuter, mais il est aussi intéressant pour le responsable de cette stratégie de se confronter aux avis et questions de la représentation nationale et aux remarques et commentaires des experts.

M. Neil ABROUG, coordinateur national de la stratégie quantique française. - Merci de m'avoir invité à faire cette présentation. Je souhaitais commencer par rappeler la façon dont nous avons œuvré au cours des deux dernières années à l'élaboration et à la mise en œuvre de la Stratégie quantique française, mais la présentation que vient d'en faire le président se suffit à elle-même. Je propose donc d'aborder directement les enjeux et la répartition budgétaire. Je vous présenterai ensuite un point d'avancement de la mise en œuvre de cette stratégie, depuis l'annonce présidentielle faite au mois de janvier 2021.

La Stratégie quantique a été annoncée par le Président de la République ; elle part du constat que les technologies quantiques ont un potentiel de disruption très important dans plusieurs secteurs économiques sur lesquels un certain nombre d'entreprises sont déjà positionnées. Au regard des auditions qui ont eu lieu dans le cadre de la mission Forteza et des consultations que l'État a continué à mener pour mettre en œuvre les recommandations de cette mission, la France a les moyens de figurer dans le premier cercle des pays en capacité d'utiliser et de développer les outils quantiques.

Le premier enjeu est de conquérir des parts de marché mondiales dans le calcul, les capteurs, la cryptographie et les technologies capacitantes. La France accueille des acteurs industriels importants dans le calcul intensif tels que Atos, ainsi que dans le monde des capteurs avec les sociétés iXblue, Thalès et Airbus et un certain nombre de *start-up* qui collaborent avec ces grands groupes ou y sont intégrées depuis quelques mois. Nous avons également la capacité de conquérir des parts de marché dans les technologies capacitantes. Il s'agit des technologies qui ne sont pas quantiques, mais qui sont indispensables à la maîtrise et au développement des technologiques quantiques.

Le deuxième enjeu est sociétal, avec 1,8 milliard d'euros d'argent public investis sur les cinq prochaines années. Cette somme conséquente est comparable à ce qui se fait au niveau international. Vis-à-vis de nos concitoyens, il est nécessaire d'avoir un message de pédagogie, de créer une adhésion aux raisons qui ont amené l'État à investir dans ce domaine qui a des enjeux à long terme, tant sur la santé que la cybersécurité et la transition écologique.

Enfin, le dernier enjeu est scientifique et technologique ; il s'appuie sur un socle d'excellence scientifique. Les expériences d'Alain Aspect sont à la base des technologies quantiques telles qu'on les comprend aujourd'hui. Quelques pépites issues de la recherche académique française, rayonnent d'ores et déjà au niveau mondial et sont en compétition avec des industriels nord-américains tels qu'Amazon, Google ou Intel. Tout ceci n'aurait pas été possible sans l'excellence de notre recherche scientifique. L'enjeu est donc d'asseoir le rayonnement de la recherche française et d'en faire le bras armé de la compétitivité des entreprises françaises.

M. le président a évoqué la somme de 1,8 milliard d'euros pour les cinq prochaines années. Je propose de préciser comment ce montant s'articule. Nous avons fait le constat, dans le cadre de la mission Forteza, d'un investissement existant, non négligeable, qui place

déjà la France au 6ème rang des investisseurs mondiaux dans le domaine du quantique, avant même l'existence d'une stratégie nationale. Les organismes de recherche, les établissements d'enseignement supérieur et l'Agence nationale de la recherche (ANR) investissaient déjà avant la mise en place d'une stratégie quantique, jusqu'à 60 millions d'euros par an. Partant de ce constat, nous avons mis en place une stratégie d'accélération, dans l'idée d'investir là où la France possède déjà un avantage compétitif. Les domaines concernés sont :

- le calcul quantique avec deux composantes : les ordinateurs et les calculateurs « bruités » de taille intermédiaire, dits « NISQ », qui commencent à apparaître et qu'il convient de maîtriser et d'apprendre à utiliser ;

- le développement de l'ordinateur quantique capable de « passer à l'échelle », dit « LSQ », qui ouvrira la porte à des applications jusqu'à présent inatteignables (médecine, repliement de protéines, cryptographie et autres usages essentiels à l'exercice de la souveraineté) ; ce développement devrait pouvoir être financé par la recherche publique et les industriels français ;

- les capteurs quantiques, où la recherche publique et le ministère des Armées investissent déjà ;

- la cryptographie post-quantique, qui doit être mise à profit par l'industrie très développée de la cybersécurité ;

- les communications quantiques, avec de nombreuses « premières » mondiales issues de la recherche française ;

- les technologies habilitantes telles que la cryogénie, les lasers, l'électronique bas bruit qui servent au développement de l'ordinateur quantique. La logique scientifique est ici la même que la logique économique qui voit des PME et des industries de pointe contribuer à des programmes d'armement ou au projet ITER, dont l'issue n'est pas connue aujourd'hui. Cependant, ceci crée dès maintenant une émulation et l'on pense que l'un des impacts économiques les plus immédiats de la stratégie française viendra de ce que l'on consacre des moyens spécifiques à ces technologies habilitantes et capacitantes.

Le financement du Plan quantique français repose sur des sources diverses :

- 15 % proviennent de subventions pour charge de service public, qui vont aux organismes et établissements sous tutelle de l'État ; ces crédits budgétaires représentent l'effort actuel de l'État ;

- 35 % sont issus du Programme d'Investissements d'avenir (PIA) afin de renforcer l'effort de l'État ;

- 5 % sont issus des programmes de l'ANR et de la Direction générale de l'armement (DGA) ;

- 30 % sont issus d'investissements privés, grâce à un engagement ferme des industriels ;

- 15 % sont issus des cofinancements européens espérés.

C’est ainsi que se répartit le montant annoncé de 1,8 milliard d'euros, qui reflète donc une véritable co-construction entre l’État, ses opérateurs, les industriels et les programmes européens.

Depuis l’annonce du Président de la République au mois de janvier 2021, plusieurs actions ont été lancées :

- le Programme et équipements prioritaires de recherche (PEPR) à hauteur de 150 millions d'euros, qui vise quatre axes de recherche : les qubits à l’état solide avec une espérance de passage à l’échelle ; les qubits d’atomes froids, sur lesquels la France possède une avance concurrentielle par rapport à ses partenaires ; le logiciel, dont il faut absolument se saisir car cette dimension fera la cohérence des actions entreprises du côté du matériel ; et un dernier axe ouvert à toute innovation ou rupture, par définition non prévisible. Lorsque la conception de la stratégie a commencé, en 2019, il n’y avait pas les *start-up* « Alice & Bob » ou « C12 Quantum Electronics », qui sont maintenant des acteurs incontournables ;

- le programme Grand Défi dont l’objectif est de mettre en place en France une plateforme nationale de calcul quantique hybride, pour habituer les utilisateurs aux différentes technologies quantiques basées sur les atomes froids, les supraconducteurs, etc. en articulation avec le calcul classique. Le calcul quantique ne sera pas accessible depuis des ordinateurs de bureau domestiques, mais offre une modalité d’accélération de certains calculs non traitables aujourd'hui. L’articulation avec le calcul intensif classique est donc essentielle et c’est l’une des spécificités du plan français ;

- un appel à projets sur la cryptographie post-quantique qui sera ouvert à des partenariats entre des *start-up* et des grands groupes et des acteurs académiques ;

- un appel à manifestation d’intérêt (AMI) « Métiers d’avenir », relatif aux actions spécifiques à la formation des futurs talents qui alimenteront l’écosystème quantique français. Il est ouvert à l’ensemble des acteurs de la formation, publics ou privés ;

- un appel à manifestation d’intérêt (AMI) « Maturation » qui vise les organismes de transfert de technologie afin qu’ils puissent accompagner les recherches fondamentales et les innovations issues de cette recherche, dans le cadre du PEPR, ou les innovations déjà existantes dans les laboratoires pour les amener à un niveau de maturité qui puisse intéresser les industriels dans des phases de prématuration et de maturation.

Dans les trois prochains mois, deux programmes sur lesquels les consultations ont commencé seront lancés : le programme Grand Défi sur le passage à l’échelle du calcul quantique ; le programme Actions de soutien aux filières industrielles des technologies capacitantes : cryogénie, lasers, isotopes stables et autres technologies gravitant autour du quantique.

M. Cédric VILLANI, député, président de l’Office. - Les tables rondes donneront l’occasion d’aller plus avant dans l’état des lieux technologique actuel. Je vous poserai donc deux questions très ciblées. Tout d’abord, l’échelon européen n’a pas été évoqué dans cette déclinaison de la stratégie nationale. Comment celle-ci s’articule-t-elle avec l’« Initiative-phare » *(Flagship)* européenne qui comportait des moyens significatifs – et qui est peut-être déjà arrivée à son terme ? Deuxièmement, le programme que vous avez présenté fait état de

lignes et de budgets engagés et il est organisé en Actions de soutien, en Grand Défi, etc. Tout ceci est assez abstrait. Pouvez-vous mentionner des réalisations ou des évènements emblématiques, des étapes technologiques particulières – également en termes d'organisation humaine – qui devraient jalonner cette stratégie ?

M. Neil ABROUG. - La stratégie française s'inscrit entièrement dans l'effort européen. L'outil *Flagship* date de la programmation Horizon 2020. Aujourd'hui, le programme Horizon Europe a repris le nom de « *Flagship* » pour évoquer le domaine des outils quantiques, sans en reprendre les outils. Les modalités d'intervention sont différentes. Les outils européens FPA et SGA permettent d'identifier des *consortia* porteurs de certaines thématiques, dans une perspective de cofinancement et de collaborations avec les partenaires européens. La France a ainsi un accord de collaboration fort avec les Pays-Bas, qui identifie des complémentarités. La France a également identifié des complémentarités particulières avec l'Allemagne, l'Italie et l'Autriche sur certaines technologies clés. Aujourd'hui, les programmes européens sont conçus comme étant le liant de mise en cohérence des différents plans nationaux.

Au-delà du *Flagship*, d'autres programmes européens concernent le quantique, comme l'entreprise commune Euro HPC, qui investit dans des moyens de calcul et des supercalculateurs et qui a lancé depuis 2020 un certain nombre d'appels à projets et d'appels d'offres pour acquérir des machines quantiques complétant les supercalculateurs. La France et l'Allemagne se sont positionnées et sont colauréats d'un projet HPC-QS relatif à la mise en place d'un supercalculateur articulé avec un simulateur quantique basé sur la technologie française Pasqal, qui s'inscrit pleinement dans la plateforme évoquée précédemment. Un financement français complétera l'action européenne : les entreprises communes européennes ne sont financées qu'à 50 % par l'Union européenne et à 50 % par l'État membre. Cela crée une forte incitation à la complémentarité et à la cohérence globale.

Il existe également une initiative européenne sur les communications quantiques, dans laquelle le plan français co-investira à 50 % avec l'Union européenne.

La France s'inscrit donc pleinement dans la dynamique européenne et les espérances de cofinancements européens que j'ai évoquées précédemment concernent ces différentes échéances.

M. Cédric VILLANI, député, président de l'Office. - Pouvez-vous nous dire quelques mots sur cet appel à projets gagné conjointement par la France et l'Allemagne ?

M. Neil ABROUG. - Ce projet vise à acquérir un simulateur quantique. Il ne s'agit donc pas d'un ordinateur quantique à portes mais d'un ordinateur quantique analogique, adapté à la simulation de la chimie ou à l'optimisation combinatoire. C'est donc un premier pas. La *start-up* Pasqal a été sélectionnée pour être le fournisseur de cette machine. Le consortium inclut le Grand équipement national de calcul intensif (Genci) français, le centre de calcul Jülich allemand et des partenaires des autres pays membres. Le lancement officiel du projet est prévu le 1er décembre 2021 et la phase actuelle est celle de la vérification des différents contrats, conventions et notifications qu'il faut adresser aux bénéficiaires.

Concernant votre question relative aux évènements et jalons, une nouveauté du 4ème PIA est de mettre en place une évaluation au fil de l'eau de l'exécution de chaque programme par des revues de programme. L'action la plus avancée aujourd'hui est le PEPR, qui doit durer 6 ans. Deux jalons décisionnels sont programmés dans 2 et 4 ans ; d'autres

jalons sont également prévus, soit techniques (nombre de qubits, niveau de puissance de froid…), soit relatifs à l'écosystème construit autour du projet (nombre de publications, nombre de personnes recrutées, nombre de brevets déposés). Les talents sont l'un des principaux enjeux de la compétition internationale sur le quantique. C'est pourquoi l'un des objectifs donnés aux porteurs de projets est de faire croître en compétence les talents internes ou de mettre en place les conditions d'attractivité pour que les talents internationaux identifient la France comme une destination clé pour la recherche et l'entrepreneuriat dans le quantique.

M. Cédric VILLANI, député, président de l'Office. - Je vous remercie. En l'absence de questions supplémentaires sur cette stratégie, nous allons aborder les tables rondes, qui sont entremêlées à la stratégie.

*
* *

Première table ronde : l'ordinateur et les capteurs quantiques

M. Cédric VILLANI, député, président de l'Office. - Pour la première table ronde, dans laquelle nous allons évoquer les progrès vers l'ordinateur quantique ainsi que les améliorations de précision et l'extension des usages dans le domaine des capteurs quantiques, nous accueillons :

- Philippe CHOMAZ, directeur scientifique du CEA, qui développe dans son pôle grenoblois une technologie de qubits semi-conducteurs à base de silicium et participe à d'autres projets quantiques sur le plateau de Saclay ;

- Pascale SENELLART, directrice de recherche au CNRS au centre de nanosciences et de nanotechnologies, cofondatrice de la société Quandela, qui travaille sur une technologie photonique ;

- Georges-Olivier REYMOND, PDG de Pasqal, société qui développe des qubits d'atomes froids ;

- Philippe DULUC, Chief Technology Officer Big Data and Security chez Atos, qui utilise les qubits développés par Pasqal et les met à disposition pour favoriser le développement d'un langage informatique quantique ;

- Thierry DEBUISSCHERT, chef de la section Physique quantique appliquée chez Thales Research & Technology, qui travaille sur les capteurs quantiques à base de diamants ultrasensibles ;

- Jean LAUTIER-GAUD, directeur commercial chez IXblue Quantum Sensors, qui développe des capteurs quantiques aux applications diverses, notamment un accéléromètre à atomes froids.

Je souligne la grande qualité des intervenants et je retrouve avec grand plaisir certaines personnalités scientifiques que j'ai pu côtoyer à différentes époques de ma vie.

M. Philippe CHOMAZ, directeur scientifique du CEA. - En introduction, je voudrais souligner que nous devons savoir de quelles « ruptures » nous parlons et quelles sont les promesses du quantique, et maîtriser le verrou de la décohérence.

Cette rupture du quantique « 2.0 » provient du fait que des avancées scientifiques et technologiques permettent de maîtriser les objets quantiques individuellement et de travailler dans l'espace gigantesque des états quantiques, d'atteindre des propriétés et d'obtenir des capacités nouvelles et ultimes. Les promesses sont extraordinaires, avec une sensibilité extrême des capteurs, des communications inviolables et des calculs massivement parallèles. Il est en effet possible de calculer dans l'espace des états quantiques en atteignant des dimensions de calcul gigantesques et de résoudre des problèmes insolubles autrement. J'insiste sur un verrou en particulier, celui de la décohérence, c'est-à-dire la perte de notre maîtrise des objets quantiques, de notre capacité à rester dans l'espace des états quantiques, ce qui obligerait à revenir dans une physique classique et à un ordinateur classique. Maîtriser ce verrou de la décohérence conditionne la capacité à rester dans l'espace des états quantiques.

Le CEA aborde cette question avec un biais : il est l'un des acteurs français et européens de la microélectronique et possède des capacités importantes en matière de puces électroniques ; il oriente donc ses recherches sur les systèmes à l'état solide et travaille sur des puces quantiques. Lorsque j'évoquerai les projets d'équipement de nos centres de calcul avec nos partenaires (universités, CEA, Inria, Genci), il sera question de l'ordinateur Pasqal. Nous faisons du développement *hardware* et nous avons conscience, dans les applications et les centres de calcul, que d'autres sont plus avancés et nous souhaitons les soutenir et faciliter ce déploiement. Le CEA limite donc ses travaux aux systèmes à l'état solide.

Pour aborder le verrou de la maîtrise de la décohérence, deux voies sont aujourd'hui identifiées à l'international. La première voie s'appuie sur la théorie de la correction des erreurs. Si on laisse un système quantique à deux états (qubit) évoluer seul, il perdra rapidement sa capacité à exister simultanément dans ces deux états, c'est-à-dire qu'il sortira de l'espace des états et ne sera plus quantique. Pour maîtriser la décohérence de cet unique qubit, il est nécessaire de corriger les erreurs. Or, pour faire un calcul quantique, il faut combiner plusieurs systèmes à deux niveaux pour obtenir des états quantiques à 2^n valeurs, n étant le nombre de qubits créés. Pour maîtriser la décohérence du système global, il faut donc coupler un très grand nombre de qubits (on appelle ceci un code de surface, qui est une sorte de calcul de correction des erreurs quantiques) : il faut en fait des milliers de qubits physiques pour obtenir un qubit logique. Il est nécessaire de passer à l'échelle et nous estimons que la technologie du silicium – pour laquelle le record de nombre de transistors sur une puce avoisine 50 milliards – permet d'aller vers un très grand nombre de transistors quantiques de qubits, et qu'elle est donc un pari intéressant pour obtenir des puces dotées d'un très grand nombre de qubits couplés pour faire de la correction d'erreur et maîtriser la décohérence. Le CEA travaille avec le CNRS, les universités et l'Inria sur cette première voie.

La deuxième voie est alternative en ce qu'elle cherche à s'appuyer sur de nouveaux concepts de qubits robustes et intrinsèquement protégés d'un certain nombre de sources de décohérence. Ces dernières années, la *start-up* Alice et Bob s'est par exemple appuyée sur des avancées académiques portant sur des « qubits de chat ». D'autres qubits sont protégés par des propriétés topologiques du système ou par des symétries. Des systèmes hybrides permettent de coupler des qubits issus du spin du noyau, très protégés, avec des qubits qui feront les calculs – à cet égard, un article récent de *Physical Review Letters* évoque le calcul dans la mémoire quantique.

Le CEA explore donc deux voies : les recherches sur le silicium pour aller vers un très grand nombre de qubits et corriger les erreurs, et les voies alternatives relevant de la physique de l'état solide qui ouvrent vers de nouveaux concepts et paradigmes, en travaillant au plus près des fondements physiques de la cohérence quantique.

Cette stratégie fait écho au PEPR quantique qui, pour sa partie calcul, distingue deux grands projets : un projet dénommé Presquile adossé à tous les développements sur le silicium, domaine qui s'appuie également sur un financement du Conseil européen de la recherche par le mécanisme « ERC Synergy Grants », obtenu par les centres CEA et CNRS de Grenoble, et sur un projet *Flagship* ; un projet PEPR dénommé RobustSuperQ sur les puces supraconductrices, avec la volonté d'équiper Grenoble et Saclay en capacité de fabrication et de travailler avec l'ensemble des acteurs de ces voies alternatives (Alice & Bob et d'autres encore).

En dernier lieu, dans le cadre du consortium européen HPC-QS et du programme « Grand Défi NISQ » sur le calcul, nous commençons à préparer la communauté du calcul haute performance (HPC) – qui possède des centres de calcul structurés aux niveaux français et européen – à l'équipement de ses centres avec des ressources de calcul quantique. Les premiers concernés sont les centres français de Bruyères-le-Châtel et allemand de Jülich, avec une machine Pasqal qui fonctionnera en analogique et peut-être ensuite, nous l'espérons, avec un système de portes. Cette première ressource quantique sera mise à disposition de nos communautés avec deux objectifs : être en capacité de maîtriser toute la chaîne jusqu'à l'utilisateur ; être en capacité d'attirer de nouveaux utilisateurs, notamment le CERN, qui a lancé un programme d'utilisation de ressources quantiques, et les théoriciens français qui travaillent autour du problème à N-corps quantique non seulement en chimie mais aussi en physique nucléaire. On voit en effet à l'étranger que les chercheurs qui font des développements de calcul de chimie quantique utilisent des approches *ab initio* de résolution du problème à N-corps issu de la physique nucléaire qui ont été développées dans les toutes dernières années.

M. Cédric VILLANI, député, président de l'Office. - Je vous remercie. Les questions seront posées à la suite de l'ensemble des présentations, et je vous propose d'entendre à présent l'exposé de Pascale Senellart.

Mme Pascale SENELLART, directrice de recherche au CNRS, professeure chargée de cours à l'École polytechnique et cofondatrice et conseillère scientifique de Quandela. - Mesdames et Messieurs les députés et sénateurs, je vous remercie de m'avoir invitée à cette audition. Je suis directrice de recherche au CNRS, professeure chargée de cours à l'École polytechnique, cofondatrice et conseillère scientifique de Quandela. J'ai coordonné le centre quantique de Paris Saclay de 2018 à 2021 et j'ai, à ce titre, représenté les universités dans la *task force* qui a contribué à la mise en place du Plan Quantique. Je vais m'exprimer avec les deux points de vue, académique et applicatif.

La *start-up* Quandela développe un ordinateur quantique optique. Celui-ci utilise les particules élémentaires de lumière, les photons, pour encoder l'information et faire des calculs. Il s'agit d'une des deux seules plateformes au niveau international à avoir pu démontrer un avantage quantique en termes de calcul avec des portes logiques. Ce système présente des spécificités très importantes, car le photon est une particule sans masse ni charge et n'interagit pas avec l'environnement. Il s'agit d'un atout majeur pour ne pas être soumis à la décohérence. Cependant, l'ordinateur quantique optique est pensé et conçu différemment des autres plateformes car le photon ne se prête pas au cadre des portes logiques. D'autres

développements, dans le cadre d'autres feuilles de route, sont lancés pour développer un calcul quantique universel à base de photons.

Ceci motive la création d'entreprises depuis un certain nombre d'années avec des acteurs majeurs en Amérique du Nord (PsiQuantum et Xanadu), mais également en Europe (Quandela en France, QUIX aux Pays-Bas, ORCA et Duality au Royaume-Uni).

L'ordinateur quantique optique est par essence modulaire. La source part de générateur de qubits (les photons) qui se propagent à la vitesse de la lumière et arrivent dans une puce dotée de circuits dans lesquels les photons sont guidés, interagissent les uns avec les autres et réalisent des opérations captées en sortie par des détecteurs.

Quandela a été créée en 2017 sur la base d'une rupture technologique réalisée au Centre de Nanosciences et de Nanotechnologies (C2N) sur la partie « génération de bits quantiques photon-uniques », une unité mixte CNRS/Université Paris Saclay. Cette technologie de rupture nous a conduits à créer une société qui commercialise et livre à l'international des générateurs de qubits photoniques aux équipes qui développent l'ordinateur quantique optique. En parallèle, nous avons décidé de nous lancer dans la création d'une petite plateforme de calcul, qui relève de la catégorie du *Noisy intermediate-scale quantum (NISQ) computer*, donc un calculateur de première génération. L'équipe de Quandela comptait en septembre une trentaine d'employés.

Les *start-up* du quantique ont bénéficié d'un fort soutien depuis le lancement de la réflexion nationale. En avance de phase du Plan Quantique, les outils étatiques de soutien des *start-up* ont bien joué le jeu : Quandela a obtenu le Grand Prix iLab en 2018 puis un certain nombre de financements par le PIA3 (iLab et i Nov) puis Innov'up, avec un co-investissement de la BPI. Elle a enfin obtenu depuis 2021 un certain nombre de soutiens via le Plan de Relance. Valerian Giesz, CEO de Quandela, a dit que « *grâce au plan Deeptech, Quandela a pu lancer des projets ambitieux et nous espérons que ces projets seront soutenus par le plan quantique quand celui-ci sera opérationnel* ».

Concernant la recherche sur le calcul quantique optique, toutes les *start-up* et tous les développements technologiques quantiques reposent fortement sur un lien avec les équipes académiques. Quandela s'intéresse donc également aux développements réalisés en recherche fondamentale sur le calcul quantique optique. Je salue les importants investissements annoncés sur la recherche publique, notamment via l'outil PEPR. Celui-ci se décline en deux parties : des « projets dirigés », pour lesquels les équipes identifiées ont déjà été financées, et des « appels à manifestation d'intérêt ». Quandela regrette que le calcul quantique optique n'ait été identifié que dans la seconde partie, qui n'a pas encore donné lieu à financements alors que le contexte international est très concurrentiel.

M. Cédric VILLANI, député, président de l'Office. - S'agit-il d'un frein administratif ?

Mme Pascale SENELLART. - Je ne peux pas vous apporter de réponse, n'ayant pas participé aux discussions. Il s'agit d'une constatation…

M. Cédric VILLANI, député, président de l'Office. - À raison !

Mme Pascale SENELLART. - Le potentiel à exploiter est très important, notamment sur les plateformes de développement technologique au LETI du CEA sur la partie calculateur quantique optique. Dans le schéma que j'ai présenté précédemment, il s'agit de la brique « intermédiaire », pour laquelle Quandela ne dispose pas de la technologie et s'appuie sur des fonderies au niveau international. Une belle fonderie française a commencé ce travail et le potentiel à exploiter est important. Certains outils mentionnés par Neil Abroug pourraient être dédiés à ces développements technologiques de haut niveau et j'attire votre attention sur les moyens importants qu'ils requièrent.

Je vais à présent exprimer mon point de vue d'enseignante-chercheuse et de coordinatrice du centre Quantum de l'Université Paris-Saclay. Un enjeu essentiel du plan quantique est la formation des cerveaux : la création de valeur, l'innovation et la création d'ordinateurs et de capteurs reposent sur la matière grise formée dans les universités et les équipes de recherche. Actuellement, nous constatons un équilibre remarquable sur la création de valeur observée et la mise en route de l'écosystème, avec une accélération rapide au niveau industriel et des *start-up*. Par ailleurs, la France est devenue une terre d'accueil pour les *start-up* étrangères. Cette situation est très positive, mais elle n'est pas exempte de points de vigilance au regard de la formation. En effet, la taille du vivier d'embauches a déjà atteint ses limites, notamment sur la partie *hardware*, alors que la croissance toujours plus rapide du nombre des *start-up* oblige à former de plus en plus de cerveaux. Le Plan Quantique s'est saisi de ce problème dès cette année, mais je considère qu'il est nécessaire d'élargir fortement l'effort de formation par la recherche. Un plus grand nombre d'équipes doit contribuer à la formation des cerveaux, même si elles interviennent dans le quantique sans être spécialistes des technologies quantiques.

L'autre danger est la difficulté de maintenir la recherche fondamentale dans un contexte où les entreprises privées seront de plus en plus attractives. Voici 3 ans, mon équipe recevait 20 CV et j'en adressais quelques-uns à Quandela. Aujourd'hui, c'est l'inverse : Quandela reçoit une vingtaine de CV et j'en reçois 1 ou 2. Mon équipe reste scientifiquement attractive, mais souffre de cet effet d'aspiration des cerveaux par les *start-up*.

Pour former et attirer un grand nombre de cerveaux, une piste clairement identifiée est celle de l'attractivité et de la visibilité des grands centres de recherche français. Avant même le travail réalisé par les pouvoirs publics, les chercheurs du quantique ont créé des centres quantiques, notamment à Grenoble, Saclay et Paris et plus récemment en Occitanie, à Strasbourg et à Bordeaux. Ils se sont structurés et se sont réjouis de la recommandation du rapport Forteza de soutenir ces initiatives, qui sont la clé pour attirer les cerveaux, augmenter l'effort de formation par la recherche et favoriser l'interdisciplinarité. Force est de constater que cette recommandation n'a pas été reprise pour le moment par le Plan Quantique français. Le centre quantique comme entité régionale, avec une politique scientifique locale d'innovation, d'interdisciplinarité et de lien avec la formation est pourtant un modèle européen standard, mais la France ne s'en est pas encore emparée.

M. Cédric VILLANI, député, président de l'Office. - M. Abroug, souhaitez-vous commenter la dernière interpellation de Mme Senellart ?

M. Neil ABROUG. - La stratégie déployée n'a pas prévu à ce stade d'action pour les écosystèmes locaux tels que conçus jusqu'à maintenant. Néanmoins, nous partageons le constat fait à l'instant et nous avons engagé des discussions avec les écosystèmes locaux. Nous incitons ces centres à mobiliser les deux AMI qui vont arriver concernant les volets formation et maturation pour adopter une logique d'écosystème. Nous serons vigilants sur la

complémentarité entre les deux AMI afin que des moyens soient accordés aux écosystèmes. D'une manière générale, la majorité des équipes est mixte et elles recevront à ce titre des financements dans le cadre du PEPR. Enfin, nous veillerons à ce que des écosystèmes locaux se positionnent sur le 4ème axe « interdisciplinarité » du PEPR.

Mme Pascale SENELLART. - Les parties formation et maturation permettront de financer le fonctionnement des centres. Pour l'instant, ce sont des appels à projets nationaux pilotés via l'ANR. Déléguer une partie des financements au niveau local permet d'avoir une réactivité, une connaissance du terrain et une adaptation aux enjeux et aux défis du moment que des appels à projets nationaux ne permettent pas d'avoir. Mes collègues – Eleni Diamanti du Hub de Paris et Alexia Auffèves du Hub de Grenoble – et moi-même avons défendu la nécessité qu'une partie du financement soit locale pour gérer ces enjeux et nourrir les équipes contribuant à l'effort de formation par la recherche.

M. Cédric VILLANI, député, président de l'Office. - Je vous remercie. J'invite maintenant Georges-Olivier Reymond à intervenir et à répondre en premier lieu à une question d'ordre général, à savoir qu'est-ce que physiquement un qubit ? M. Chomaz a distingué les qubits physiques des qubits logiques, Mme Senellart a évoqué les qubits photoniques et M. Reymond parlera des qubits d'atomes froids. Pouvez-vous nous donner un panorama général des différentes sortes de qubits existant actuellement ?

M. Georges-Olivier REYMOND, président-directeur général de Pasqal. - Merci de votre invitation. Je vais essayer d'être concret. Je suis cofondateur de la société Pasqal qui fabrique des processeurs quantiques. J'ai réalisé une thèse en physique voici 20 ans sur la technologie qui est aujourd'hui au cœur du savoir-faire de Pasqal. J'ai ensuite rejoint le monde de l'industrie dans des grands groupes et des *start-up*. Voici deux ans, j'ai créé Pasqal, fort de toute cette expérience. Mon parcours illustre le cercle vertueux de la recherche fondamentale : je n'aurais jamais pensé voici 20 ans qu'une *start-up* pourrait être créée sur le sujet de mes travaux d'alors. Aujourd'hui, le marché existe, nous livrons les machines à des clients comme le centre CEA de Bruyères-le-Châtel ou le centre de calcul de Jülich, et elles résolvent des problèmes. Nous travaillons avec EDF, le Crédit agricole. Deux machines sont en cours de construction et assureront notre service Cloud afin de rendre le calcul disponible en ligne aux utilisateurs. Deux autres machines sont prévues pour les centres de calcul.

Les smartphones actuels, qui tiennent dans une poche, sont un million de fois plus puissants que les ordinateurs qui ont amené l'homme sur la Lune. Or, un million de ces smartphones mis côte à côte à travailler ensemble ne suffiraient pas à résoudre les problèmes calculatoires qui se posent à nous. Ils ne permettraient pas de trouver de nouvelles molécules pour créer des médicaments, de simuler la matière pour inventer de nouveaux matériaux, de nouvelles batteries, des panneaux photovoltaïques et participer à la résolution du problème du changement climatique.

La solution est quantique. Une première révolution quantique a eu lieu au XXe siècle et a permis l'invention du transistor, du laser, de l'IRM… Aujourd'hui, nous assistons à une deuxième révolution quantique en utilisant les qubits et en les superposant dans leurs états intriqués, afin de réaliser des calculs massivement parallèles. Il ne s'agit pas d'une amélioration continue, mais d'une révolution du calcul, équivalente au passage du travail manuel à la machine à vapeur.

Une étude du Boston Consulting Group a évalué la valeur créée par le calcul quantique à 800 milliards de dollars en 2030. Pour une société comme Pasqal, le chiffre d'affaires annuel à cet horizon peut être estimé à 10 ou 20 milliards.

M. Cédric VILLANI, député, président de l'Office. - Entendez-vous par « valeur créée » la résolution de nouveaux problèmes ou des paris sur les réalisations à venir ?

M. Georges-Olivier REYMOND. - J'entends par valeur créée ce qui est apporté à l'économie, sur toute la chaîne de valeur, depuis les utilisateurs jusqu'aux sous-traitants. Une partie de ces revenus concerne les fabricants et les fournisseurs de solutions comme Pasqal.

M. Cédric VILLANI, député, président de l'Office. - Pouvez-vous nous donner un exemple : sur ces 800 milliards de dollars, combien seront obtenus grâce à la résolution de quoi ?

M. Georges-Olivier REYMOND. - Le premier secteur qui bénéficiera de ces technologies est celui de l'énergie. Pasqal travaille avec EDF sur un cas d'usage visant à faciliter la mobilité urbaine. Les automobilistes commencent à basculer vers les véhicules électriques et sont confrontés à la problématique de recharge. Le fait que des milliers de véhicules doivent se recharger en même temps pose d'énormes contraintes sur la grille électrique, car la demande est brutalement très forte sur un nombre limité de stations. Un ordinateur classique ne sait pas résoudre un problème aussi complexe. L'ordinateur quantique permettra de lever ce verrou de calcul. Il intervient dans la mobilité urbaine, l'invention de nouveaux matériaux, l'amélioration de la distribution d'énergie, etc.

Une course est lancée pour fournir les premières machines à usage industriel. Des preuves de concept ont été démontrées. Pasqal et sa technologie sont en tête de course, car elles proposent un nombre de qubits (200) supérieur à celui proposé par exemple par Google (50) – ces nombres sont publiés dans des revues scientifiques à comité de lecture. Les qubits sont des atomes qui encodent l'information et interagissent pour faire les calculs. Le passage de 50 à 200 qubits n'induit pas une évolution proportionnelle de la puissance de calcul : celle-ci est multipliée par deux à chaque qubit ajouté, selon une loi exponentielle. Le passage de 50 à 200 qubits permet de passer de démonstrations de principe au traitement de cas d'usage.

La deuxième course est celle de l'armement. Des levées de fonds et des investissements privés sont très importants notamment aux USA sur des technologies pourtant moins avancées. IonQ, une société similaire à Pasqal avec un ou deux ans d'avance, mais avec une moins bonne technologie est récemment entrée en bourse et vaut déjà deux milliards de dollars. D'autres levées de fonds mobilisent plusieurs centaines de millions de dollars. Certains des concurrents de Pasqal aux USA disposent de 600 millions d'euros pour mener leur stratégie à bien.

Pasqal est une société issue de l'Institut d'Optique, sur le plateau de Saclay, bâtie sur des fondements académiques et sur des années de recherche réalisées au CNRS. Deux de nos cofondateurs sont Alain Aspect, médaille d'or du CNRS, et Antoine Browaeys, médaille d'argent du CNRS. Pasqal bénéficie donc d'une forte expertise technologique. Elle est la 3ème plateforme qui a démontré l'avantage quantique – la publication correspondante a été faite dans *Nature* –, sur un cas d'usage, en résolvant avec 200 qubits un problème de physique fondamentale, la construction du magnétisme quantique dans les matériaux, avec des applications dans les sciences des matériaux et la physique théorique.

Notre avantage est le nombre de qubits. C'est lorsque les technologies sont encore au stade de développement que les avantages qu'elles procurent ont les effets les plus importants et permettent de faire la différence : ils nous permettent aujourd'hui de faire la course avec Google.

Pasqal a été créée en mars 2019 et compte aujourd'hui 40 employés de 9 nationalités. Elle attire des talents de l'étranger. Mme Senellart a dit que les *start-up* prendraient des ressources à la recherche ; je dirais plutôt qu'elles offrent des débouchés aux brillants étudiants qui ont des difficultés à trouver des postes et mettent en valeur l'environnement. Elles prennent certes de la place, mais font aussi grossir le marché global et les parts de chacun. Pasqal a bénéficié d'un financement de 25 millions d'euros en avril 2021 venant de divers investisseurs internationaux. Enfin, des machines sont en construction et seront installées dans des centres de calcul en Allemagne et en France (CEA, GENCI et Atos). Dans cette première structure de calcul hybride, le calcul quantique sera intégré au calcul classique.

L'action publique est très importante dans l'écosystème : le Plan Quantique, le Plan France 2030, le *Flagship* européen PASQuanS, les systèmes de subvention européens EIC qui soutiennent les *start-up*. Un autre levier est la commande publique : le projet HPC-QF en est une belle illustration. Dire à des investisseurs que Pasqal a vendu deux machines a fortement pesé dans la balance de la levée de fonds. Pour la prochaine levée de fonds, si nous pouvons dire que Pasqal a vendu à la France des machines de 1 000 qubits (celles que nous développons actuellement) positionnées dans des centres de calcul, cela aura un énorme impact auprès des investisseurs.

La première révolution quantique a été développée par des physiciens européens, mais le marché est essentiellement positionné aux Etats-Unis. Pour la deuxième révolution, essayons d'en conserver un plus gros morceau !

M. Philippe DULUC, Chief Technology Officer Big Data and Security chez Atos. - Mesdames et Messieurs les députés et sénateurs, je vous remercie d'avoir invité Atos à témoigner de l'avancement du Plan Quantique et de sa propre stratégie de développement autour du quantique. J'évoquerai notre stratégie Atos Quantum et ferai un focus sur les partenariats et les financements.

Atos est un grand groupe international dédié à la transformation digitale avec plus de 100 000 employés et 11 milliards d'euros de chiffre d'affaires. 235 millions d'euros ont été dépensés en 2020 sur la R&D. Il est aujourd'hui impossible de survivre dans la compétition internationale sans investissement important sur l'innovation et la R&D, car la seule manière de se différencier est d'avancer et de conserver sa place face aux géants américains (GAFA) et aux acteurs chinois en plein développement.

Le programme Atos Quantum a démarré en 2016 et est parti du constat suivant : Atos est leader dans le marché des supercalculateurs et seul constructeur européen – je souligne l'usage de souveraineté des supercalculateurs en sécurité et simulation nucléaire – et constate que le quantique disrupte le domaine du HPC, car il permet d'accélérer les calculs, alors que ceux des supercalculateurs deviennent difficiles à accélérer à cause de la difficulté croissante à avoir des puces performantes.

La deuxième raison pour laquelle Atos investit dans le quantique est la cybersécurité, dans laquelle Atos est leader européen. Les technologies quantiques disruptent également ce domaine, face aux risques de décryptements quantiques et d'algorithmes cryptographiques qui

pourraient mettre en danger la sécurité d'internet. Atos a été dans l'obligation de définir un plan pour se développer dans le domaine du quantique. Ce plan a été lancé par Thierry Breton, qui était PDG d'Atos en 2016, en s'appuyant sur un conseil scientifique indépendant dont Cédric Villani a fait partie.

Ce conseil a mis en place un plan d'action résumé ainsi :

- développer une plateforme de programmation et d'apprentissage du quantique ;
- accélérer les calculs des supercalculateurs grâce au quantique ;
- créer une activité de conseil en calcul quantique ;
- rendre les produits de cybersécurité Atos résistants aux attaques quantiques.

Dès 2017, Atos a commercialisé l'Atos QLM (*Quantum Learning Machine*), un serveur permettant aux utilisateurs de programmer des algorithmes quantiques, de les optimiser et de simuler leur exécution comme s'ils tournaient sur un ordinateur quantique. Cette machine est vendue dans le monde entier, par exemple à des laboratoires fédéraux américains.

Les recherches sur le HPC hybride se sont poursuivies, en examinant comment incorporer l'accélération quantique dans nos supercalculateurs. En 2023, nous serons en capacité de fournir un supercalculateur accéléré par du quantique. La stratégie d'Atos est de ne pas investir sur les processeurs quantiques, mais sur la partie logicielle, intégration et calculs et de s'appuyer sur des partenariats en identifiant des fabricants de processeurs (Pasqal, Quandela, le CEA et d'autres *start-up* françaises et européennes). Nous estimons qu'au moins une technologie émergera en 2023 et pourra accélérer les capacités de nos supercalculateurs.

Nous avons mis en place une activité de conseil en 2020, qui a déjà plusieurs clients. Elle est basée à Grenoble.

Enfin, sur les produits de cybersécurité, notre choix a été d'aller vers la cryptographie post-quantique, dans l'objectif de rendre tous nos équipements de cybersécurité résistants aux attaques quantiques, en implémentant des standards en cours de validation (développés par NIST) dont la publication est attendue entre 2022 et 2024.

Le financement de la R&D est essentiel pour ne pas se faire distancer par les concurrents internationaux. Atos consacre chaque année un flux constant de financement sur fonds propres à ses activités quantiques et de cybersécurité. De 2015 à 2017, 100% de cet effort a été fourni sur les fonds propres du groupe. Atos a mis en place une équipe d'une vingtaine de personnes (laboratoire Atos Quantum) composée de physiciens, mathématiciens et spécialistes de l'informatique, qui dépose des brevets et publie des articles. Atos est le premier déposeur européen de brevets sur le calcul quantique.

À partir de 2018, Atos a commencé à bénéficier de compléments de financement issus de l'ANR, du PIA, et de la région Ile-de-France. À partir de 2019, Atos a bénéficié de compléments de financements européens notamment via le Quantum *Flagship*, dans lequel Atos est présent avec quatre projets (AQTION, PASQuanS, NEASQC et QLSI). L'impact de ces compléments de financement n'est pas négligeable. Par exemple, le QLM est capable de

simuler l'exécution mathématique d'un programme, ainsi que les caractéristiques physiques du qubit ; l'obtention d'un financement de type AQTION a permis d'ajouter dans le QLM la simulation des ions piégés ; avec PASQuanS, nous avons pu y ajouter la simulation des atomes froids pour faire de la simulation hamiltonienne. Les compléments de financement permettent d'accélérer la feuille de route et d'ajouter des fonctionnalités.

Le projet européen HPC-QS, sous l'égide du *European High-Perfomance Computing Joint Undertaking* (EuroHPC JU), a vocation à équiper les États membres en supercalculateurs avec un financement de 50% de l'Union et de 50 % des États. EuroHPC est orienté sur les supercalculateurs et a pris en compte avec HPC-QS la dimension quantique. Atos a obtenu conjointement avec Pasqal un financement de HPC-QS pour mettre en place une capacité d'accélération dans un supercalculateur.

À partir 2021, les compléments de financement proviennent également de la Stratégie nationale des technologies quantiques.

Atos continue à répondre aux différents volets (NISQ, LSQ, formation et cryptographie post-quantique). Atos participera au programme Grand Défi sur la plateforme nationale de calcul quantique hybride, répondra à l'AMI « métiers d'avenir » et à l'appel à projets « cryptographie post-quantique » et sera également présent sur le Grand Défi de passage à l'échelle du calcul quantique. Tout ceci nous aidera à accélérer et à améliorer nos projets, sur le plan tant des performances que des fonctionnalités. Trois *start-up* américaines sont aujourd'hui valorisées à plus de 1 milliard de dollars (IonQ, PsiQuantum et Rigetti Computing). Elles ont été créées en 2016 et deux d'entre elles entreront bientôt en bourse.

Le domaine des technologies quantiques est très complexe et rien ne peut se faire sans partenariats larges avec des institutions académiques, des *start-up*, des fournisseurs de technologies habilitantes. Les partenariats les plus emblématiques d'Atos sont les suivants :

- la chaire industrielle NASNIQ pour co-financer avec le CEA-Saclay la recherche fondamentale sur des qubits hyperstables ;

- les bourses CIFRE qui ont permis de financer 5 doctorants dans le laboratoire Atos Quantum avec l'Ecole polytechnique, l'Inria, le CNRS, l'université Paris-7 et l'université de Grenoble ;

- les nombreux projets de recherche collaboratifs aux niveaux régional, national et européen avec des acteurs académiques français et européens ;

- le pôle de compétitivité Systematic Paris-Région : Atos anime l'écosystème quantique d'Ile-de-France ;

- des *start-up* françaises et européennes, car Atos n'investit pas sur les processeurs quantiques et s'appuie sur des partenaires R&D et des projets collaboratifs (C12 electronics, Pasqal, Alice&Bob, Quandela…). Avec ces *start-up*, Atos veut apporter les parties relatives à la connexion aux supercalculateurs, au logiciel et au pilotage, en se reposant sur les technologies matérielles de ces *start-up*.

M. Cédric VILLANI, député, président de l'Office. - Vous travaillez sur l'accélération du HPC avec différentes technologies quantiques. Quels types de calcul peuvent être accélérés ? Quels cas d'usage pourraient illustrer la différence entre le HPC classique et le HPC avec accélération quantique ?

M. Philippe DULUC. - Le premier cas d'usage que l'on voit apparaître est l'optimisation combinatoire. La simulation d'une molécule de 10 ou 15 atomes est facile avec un HPC. Plus la molécule est grosse, plus la complexité est forte. La simulation d'une molécule de 100 atomes est ainsi inaccessible à un HPC. Seule la voie du calcul quantique permet d'envisager de continuer à faire de la simulation, d'analyser les réactions chimiques, etc. Total Énergie travaille par exemple sur la séquestration du carbone avec des molécules de plus de 50 atomes et doit utiliser le calcul quantique. On en est encore au stade de la recherche. D'autres exemples d'optimisation combinatoire existent dans le domaine de l'énergie.

M. Philippe CHOMAZ. - Lorsque nous équipons nos centres HPC avec les accélérateurs, nous sommes bien dans une phase de démonstration et de préparation de la phase suivante. C'est le bon moment pour réaliser ces investissements, avec un avantage concurrentiel direct aujourd'hui. Il est important de les intégrer à cette communauté HPC et de travailler avec les acteurs du domaine pour coupler les accélérateurs aux calculateurs. La génération de supercalculateurs Exascale qui arrive n'aura pas d'accélérateur opérationnel. On peut avoir une ambition et tracer une route, mais il ne faut pas confondre le monde d'aujourd'hui et le monde qui vient.

M. Cédric VILLANI, député, président de l'Office. - M. Chomaz, vous avez évoqué l'exemple du silicium et vous avez insisté sur la différence entre les qubits physiques et les qubits logiques et sur l'existence de verrous techniques. Nous avons ensuite entendu parler de qubits photoniques, de qubits à atomes froids, etc. Pouvons-nous avoir un panorama d'ensemble et comprendre comment replacer la performance à 200 qubits dans cette compétition générale ?

M. Philippe CHOMAZ. - C'est très ouvert. Dès que l'on maîtrise un quantum, c'est-à-dire un objet quantique que l'on peut contrôler – qu'il s'agisse d'un spin d'électron, d'un photon, d'un quantum de courant dans un circuit supraconducteur –, on peut commencer à imaginer des qubits et à les coupler. Le nombre de voies possibles est considérable, car tout degré de liberté quantique peut à terme être une source de calcul quantique. Les 200 atomes piégés dans des systèmes optiques de Pasqal ont une certaine avance à l'international, car les avancées académiques sont importantes et que la société Pasqal les maîtrise. Ce système reste toutefois un démonstrateur : ce n'est pas encore aujourd'hui que l'on utilisera uniquement un calculateur quantique versus un calculateur classique. Je suis plus prudent que mes collègues.

M. Cédric VILLANI, député, président de l'Office. - Les 200 qubits annoncés par Pasqal sont-ils de vrais qubits logiques ? Certaines technologies distinguent le qubit logique du qubit physique, car on est certain de ce qui va se passer pour l'un, mais pas pour l'autre.

M. Georges-Olivier REYMOND. - Le qubit logique n'existe pas pour le moment, seuls les qubits physiques existent. Des équipes – dont celle de Pasqal – travaillent à créer le premier. Ces développements sont encore très fondamentaux et prendront du temps.

Il faut remettre en perspective ce que nous vivons aujourd'hui : nous sommes au début de l'histoire du calcul quantique. Nous n'imaginons pas encore ce que nous allons faire avec les machines que nous créons. Les premiers processeurs inventés étaient spécifiques à une activité, la comptabilité. La situation sera identique pour le calcul quantique. Les différents qubits existant aujourd'hui présentent des avantages et des inconvénients. Telle technologie permettra de bien résoudre tel problème, telle autre permettra d'en accélérer une autre.

M. Cédric VILLANI, député, président de l'Office. - Entre les années 1950 où les premiers ordinateurs ont été développés et le moment où les bénéfices de l'informatique ont été considérables pour la société, il s'est écoulé un certain temps. Vous avez cité une étude évaluant à 800 milliards de dollars la valeur ajoutée pour l'économie liée à ces technologies : d'ici à 2030, quels cas d'usage pratiques pourront dégager de telles sommes bénéficiant à la société ?

M. Georges-Olivier REYMOND. - Le cas d'usage avec EDF que j'ai évoqué est un problème d'optimisation combinatoire. Il s'agit d'optimiser un planning pour que le temps global de charge de la flotte de véhicules soit minimal. Notre démonstrateur est dans la gamme de 100 à 200 qubits : nous savons qu'elle n'est pas suffisante pour EDF, qui a intérêt à continuer à travailler sur ses calculateurs classiques. Le traitement d'un cas d'usage sur une machine quantique avec de vraies données du terrain est une première mondiale. Un article a été publié récemment montrant l'avantage que pourrait avoir EDF à basculer sur la technologie quantique autour des 1 000 qubits. Pour Pasqal, cette échéance est prévue en 2023. Le problème d'optimisation d'EDF est donc un cas industriel spécifique dont le traitement quantique pourrait commencer à créer de la valeur à partir de 2023 ; les autres cas d'usage restent à identifier.

Autre exemple : nos atomes permettent de simuler le comportement d'un champ d'éoliennes et d'estimer les effets d'éventage – lorsqu'une éolienne est sous le vent d'une autre, son rendement diminue. Pour qu'un champ d'éoliennes soit rentable, il suffit d'apporter quelques pourcentages d'optimisation à l'installation du champ. L'effet de seuil est très fort.

M. Philippe DULUC. - Il est difficile de comparer les technologies : Atos est orienté vers les usages et les applications et a développé une métrique Q-Score basée sur les applications. Elle compare les technologies et les processeurs quantiques sur leur capacité à résoudre un problème d'optimisation combinatoire (Max-Cut).

M. Cédric VILLANI, député, président de l'Office. - Il s'agit d'une sorte de *benchmark*…

M. Philippe DULUC. - Oui. Ce souci de *benchmark* est également présent dans la Stratégie nationale.

M. Cédric VILLANI, député, président de l'Office. - Je vous remercie. Je donne la parole à Thierry Debuisschert.

M. Thierry DEBUISSCHERT, Chef de la section physique quantique appliquée chez Thales Research & Technology. - Je vous remercie de me permettre de présenter les travaux de Thales sur les capteurs quantiques, notamment sur les capteurs quantiques à base de centres NV du diamant.

Je suis chercheur chez Thales Research & Technology à Palaiseau. J'ai réalisé ma thèse sur la réduction des fluctuations quantiques de la lumière, puis j'ai travaillé sur les communications quantiques et je m'occupe actuellement des capteurs quantiques dans la même entreprise.

La première révolution quantique a montré que l'énergie était quantifiée et qu'elle se décrivait par des états discrets (état 0 ou état 1 par exemple). La microélectronique est basée sur cette avancée scientifique. Depuis une dizaine d'années, nous sommes capables de fabriquer des objets quantiques uniques ; par exemple, une source de photons uniques a été développée au Centre de Nanosciences et de Nanotechnologies (C2N), et un qubit supraconducteur a été développé au CEA. Ces objets mésoscopiques ont des propriétés quantiques au même titre qu'un atome. Une fois maîtrisé ce niveau de conception et de fabrication, nous sommes en capacité d'exploiter pleinement une propriété spécifiquement quantique, à savoir la superposition d'états : le système peut être simultanément dans l'état 0 et dans l'état 1. C'est cette propriété qui est exploitée par les capteurs quantiques, dans des systèmes à 1 qubit. Ces systèmes sont placés dans une superposition des états 0 et 1 puis, une fois couplés à un système extérieur qui matérialise la grandeur à mesurer, on regarde comment celui-ci les modifie. La modification de la superposition permet de remonter à la grandeur physique mesurée.

Les capteurs quantiques sont nombreux et il existe différentes plateformes. Thales développe par exemple :

- des horloges atomiques compactes qui peuvent être embarquées sur une plateforme mobile ;

- des systèmes à base d'atomes froids sur puce : les atomes sont refroidis à quelques millikelvins et manipulés sur une puce microélectronique avec des champs électriques et magnétiques pour les faire passer à volonté de l'état 0 à l'état 1 ;

- des matériaux supraconducteurs à haute température de Curie, comme les cuprates YBaCuO et les supraconducteurs dits « haut-Tc », pour réaliser des antennes de très petite taille pour mesurer le champ électromagnétique ;

- des cristaux dopés à base de terres rares pour réaliser des capteurs et analyseurs de champs électromagnétiques, ou encore des mémoires quantiques ;

- des centres NV du diamant, sur lesquels mon exposé va principalement porter.

Un cristal de diamant est naturellement plein d'impuretés, qui lui donnent sa couleur. Une impureté commune est l'inclusion d'azote dans l'arrangement d'atomes de carbone qui constitue le cristal de diamant. Un atome d'azote (N) remplace un atome de carbone (C) et crée aussi une lacune (V) dans le cristal. Ce centre NV (azote couplé à la lacune) se comporte comme un atome artificiel et est la base du « capteur du centre NV du diamant ». Il se comporte comme un aimant de la taille d'un atome que l'on peut insérer dans un diamant de synthèse – on sait aujourd'hui fabriquer des diamants de synthèse de très grande pureté et de très grande qualité cristalline, qui permettent d'explorer les propriétés des impuretés, voire d'une impureté unique, et c'est ce qui nous donne accès à cette physique. Les centres NV ont des propriétés remarquables : de taille atomique, ils permettent d'obtenir des capteurs ayant une résolution spatiale nanométrique, essentielle pour la nanoélectronique ou le nanomagnétisme par exemple ; ils sont à l'état solide, ce qui facilite leur manipulation et leur

mise en œuvre ; ils fonctionnent à température ambiante, ce qui est très important pour les applications pratiques telles que celles que recherche Thales ; ils peuvent être manipulés optiquement, par exemple ils peuvent être pompés par un laser vert et on mesurera la luminescence induite qui sera faite de lumière rouge.

De nombreuses applications sont envisagées pour ces capteurs de centre NV :

- pour les véhicules autonomes : gyromètres miniatures permettant de mesurer la position des véhicules de manière indépendante, notamment des signaux GPS ;

- dans le domaine de la communication : mesure et analyse spectrale des champs électromagnétiques pour caractériser le rayonnement électromagnétique ambiant ;

- pour des applications médicales : capteurs de champ magnétique très sensibles permettant de faire à terme de la magnétoencéphalographie, c'est-à-dire la mesure des champs magnétiques produits par les courants circulants dans les neurones.

Ces applications sont en cours de développement et ont de bonnes perspectives. Ces technologies sont développées dans un contexte fortement collaboratif. Je suis le coordinateur du projet européen Asteriqs du *Flagship*, qui réunit 23 partenaires européens, avec une forte participation française, allemande et suisse. Toutes les applications possibles des centres NV du diamant sont incluses dans ce projet. Thales est aussi impliqué dans d'autres projets européens qui développent d'autres technologies de capteurs.

La France possède des acteurs majeurs dans le domaine, qui permettent de couvrir toute la chaîne de valeur de ces capteurs : des laboratoires universitaires comme le Laboratoire des sciences des procédés et des matériaux (LSPM) et l'Institut de Recherche de Chimie Paris (IRCP) qui sont spécialistes de la croissance du diamant synthétique et peuvent faire des diamants de très haute qualité ; les laboratoires du CNRS et de l'ENS Paris Saclay qui développent des applications innovantes des centres NV, par exemple leur inclusion dans les enclumes en diamant qui sont utilisées pour les recherches sur des matériaux soumis à de hautes pressions pour lesquelles il n'existe pas d'autres moyens de mesure ; Thales, qui développe des dispositifs tels que des analyseurs de spectre utilisant les centres NV du diamant.

Le marché des capteurs quantiques sera en progression régulière au fil des ans et couvre tous les domaines d'activité : médical, communication, navigation, etc. Cette progression sera de l'ordre de 1 milliard de dollars sur les 10 prochaines années. Ce montant ne concerne pas uniquement les capteurs mais aussi tout l'équipement environnant ; par exemple, si des capteurs de champ magnétique miniature sont mis au point, cela s'accompagnera d'une diminution de la taille des équipements médicaux. L'essor des capteurs quantiques aura donc un impact considérable sur de nombreux domaines d'activité. Il est essentiel de développer ces capteurs extrêmement performants et miniaturisés.

Parmi les perspectives spécifiques aux capteurs à centre NV, je vais d'abord mentionner l'intégration : ce dispositif tient dans quelques millimètres cubes et tous les éléments nécessaires à son contrôle pourraient être positionnés sur le même substrat électronique. Il y aussi la technique PDMR (*Photoelectric Detection of Magnetic Resonance*) : plutôt que d'utiliser un signal optique pour détecter l'état de spin électronique du centre NV, on pourra utiliser un signal électrique, ce qui permettra d'aller plus loin dans la miniaturisation des dispositifs. Enfin, les centres NV peuvent aussi être utilisés dans le

domaine des communications et des calculs quantiques, car ils peuvent être une source de photons uniques, on peut les intriquer à distance, et on peut aussi les coupler à des mémoires quantiques constituées du spin nucléaire du carbone 13 dans la maille du diamant.

M. Cédric VILLANI, député, président de l'Office. - Je vous remercie. Je propose d'entendre le dernier exposé de cette première table ronde en donnant la parole à Jean Lautier-Gaud.

M. Jean LAUTIER-GAUD, Directeur commercial chez iXblue Quantum Sensors. - Mesdames et Messieurs les parlementaires, je vous remercie de votre invitation. J'apporterai trois éclairages : celui d'iXblue, qui est une entreprise de taille intermédiaire (ETI), celui de Muquans, une PME qui intervient dans les technologies quantiques et qui vient d'être acquise par iXblue, et enfin ma vision d'ancien chercheur passé dans le privé. Le distillat de ces trois éclairages proposera des pistes pour l'implémentation de la stratégie quantique.

iXblue est un groupe français de haute technologie implanté sur plusieurs sites, notamment à Besançon, Lannion et Bordeaux. Il est spécialisé en photonique et opère dans trois grands secteurs d'activité : la navigation inertielle, les activités marines, et les activités photoniques, notamment pour le spatial et le quantique.

iXblue a récemment acquis la société Muquans, une PME implantée à Bordeaux depuis 10 ans et active dans le secteur des capteurs quantiques. Cette acquisition a donné lieu à la création au sein du groupe de la division iXblue Quantum Sensors. Celle-ci va fournir des capteurs quantiques et des technologies habilitantes qui pourront servir à tous les piliers des technologies quantiques.

Pour mesurer le saut parcouru dans le domaine des capteurs quantiques et de la filière à atomes froids, j'illustrerai ma présentation avec la photo d'une expérience usuelle d'atomes froids en laboratoire et avec celle d'un capteur quantique commercial. Un effort colossal a été fourni pour réduire la compacité et la complexité de la machine. Il est à noter que le physicien présent sur la première photo a disparu de la seconde : le rêve consistant à transmettre la technologie quantique à un non-spécialiste pour ses propres applications est en cours de réalisation. Le gravimètre est désormais déployé sur le terrain. Un gravimètre positionné sur le mont Etna mesure les flux et mouvements de magma dans le sous-sol.

M. Cédric VILLANI, député, président de l'Office. - En quoi ce gravimètre est-il quantique ?

M. Jean LAUTIER-GAUD. - Il est quantique, car il exploite la superposition d'états des particules quantiques dans des atomes neutres, en exploitant plus particulièrement le principe d'interférométrie atomique permettant des mesures de grande précision, par exemple les mesures inertielles d'accélération.

Cette réalisation est remarquable, nécessaire, mais pas suffisante. Ces technologies peuvent être prises en main par des non-spécialistes mais restent une première génération de capteurs. Il est nécessaire d'aller plus loin, notamment de renforcer la fiabilité de long terme, de diminuer le facteur d'échelle et de fiabiliser ces capteurs pour des utilisations plus opérationnelles et industrielles.

Ce résultat est celui de toute la filière atomes froids en France. Je salue notamment les laboratoires LNE-SYRTE de l'Observatoire de Paris et LP2N de l'Institut d'Optique, les établissements publics qui travaillent sur le sujet et nos fournisseurs. Je souligne l'excellence de la filière française des atomes froids, ce qui augure bien de la suite de la stratégie quantique.

L'activité d'iXblue Quantum Sensors est très vaste et repose sur la fourniture de capteurs aux non-spécialistes : gravimètres servant à suivre les flux de masse dans le sous-sol pour obtenir une meilleure exploitation en géothermie, pour mieux suivre le stockage de CO_2 dans le sous-sol et pour améliorer la gestion des aquifères ; horloges atomiques – iXblue propose actuellement la meilleure horloge atomique commerciale du monde ; sous-systèmes dans le périmètre des technologies habilitantes qui offrent des solutions de photonique, d'optomécanique et d'électronique pertinentes pour toute la filière quantique française et européenne.

M. Cédric VILLANI, député, président de l'Office. - L'horloge atomique offre une précision relative de 10^{-15} sur la fréquence. Les précisions indiquées sont-elles, chacune dans leur domaine, parmi les meilleures imaginables aujourd'hui ?

M. Jean LAUTIER-GAUD. - Exactement, au niveau industriel. Cette horloge n'est pas la meilleure du monde, car les horloges optiques permettent de gagner un facteur 1000 sur les performances, mais elles sont toujours au stade du laboratoire. Nous parlons ici d'une horloge clé en main, livrable partout dans le monde et installée par n'importe quel technicien.

Le groupe iXblue, avec la reprise des activités de Muquans, incarne une excellence industrielle française pour tout ce qui concerne la manipulation des atomes neutres. Dès qu'il s'agira de manipuler des atomes neutres pour mettre en œuvre différentes technologies quantiques, les technologies habilitantes photoniques développées notamment par iXblue seront de bons candidats. Dans le portefeuille d'activités d'iXblue au sens large, les solutions photoniques seront très pertinentes pour la manipulation des photons et pour des mesures dans les centres NV.

Le travail réalisé pour rendre les capteurs quantiques industriels et fiables permet de les utiliser pour mettre en œuvre d'autres technologies quantiques, en vue de faire des preuves de concept, de développer des produits et de les commercialiser à terme.

IXblue est une entreprise rentable qui finance sur fonds propres une bonne partie de sa R&D. Cela n'est toutefois pas suffisant pour atteindre cette deuxième génération de capteurs et de technologies habilitantes pour les fiabilités à long terme.

Je souhaite évoquer les choses qui fonctionnent bien, notamment par le biais des « équipements d'excellence » (Equipex) et des partenariats public-privé de manière générale. Il est très sain que les *start-up* et les PME puissent être associées à des projets de recherche et de développement. Je rends hommage aux premiers succès du Plan Quantique, en mentionnant l'action du CNES dans le cadre du Plan de Relance qui nous permet de développer un système laser vers une version spatialisable et un contrat avec la Délégation générale pour l'armement (DGA) dans le cadre du programme CHOF (capacité hydrographique et océanographique future) de la Marine nationale, qui permettra de développer et fournir quatre gravimètres marins destinés au Service hydrographique et océanographique de la Marine (SHOM). La première génération d'instruments est donc validée par les clients et distribuée dans le monde entier.

Cela n'est toutefois pas suffisant et nous souhaitons vous suggérer quelques pistes d'amélioration. La première est le renforcement de l'écosystème des technologies habilitantes, notamment pour l'excellence de la filière française des atomes froids. La deuxième, dans le cadre de la stratégie quantique nationale, serait l'affichage direct des industriels dans les appels à projets PEPR, ce qui n'est pas le cas actuellement. La troisième serait d'utiliser les budgets pour rendre ces technologies plus fiables pour atteindre les applications cibles et satisfaire les besoins des clients, seul moyen de rendre ces activités économiquement viables et pérennes après la clôture du *Flagship* et du Plan Quantique.

M. Cédric VILLANI, député, président de l'Office. - À quelle date est prévue la clôture du *Flagship* et des autres grands financements en cours ?

M. Jean LAUTIER-GAUD. - Dans sept ans.

M. Cédric VILLANI, député, président de l'Office. - Dans une de vos présentations, l'agriculture est citée comme étant une des applications possibles de ces technologies quantiques. Je serais curieux d'en savoir plus !

M. Thierry DEBUISSCHERT. - Il peut s'agir d'obtenir des capteurs plus performants pour faire par exemple de la détection et du contrôle d'émissions de gaz dans les silos à grains. Il n'est pas forcément nécessaire d'avoir des capteurs de haute précision pour cela mais on a besoin de capteurs petits et intégrés.

M. Jean LAUTIER-GAUD. - Pour l'agriculture, le gravimètre permet de suivre les mouvements d'eau dans le sous-sol. Le capteur est au cœur d'une meilleure gestion des ressources en eau, eau potable pour les villes ou eau pour l'irrigation des sols agricoles. Il sera nécessaire d'avoir un capteur encore plus précis et sensible pour mieux suivre en temps réel la charge et la décharge des aquifères suite à une exploitation par l'homme.

M. Cédric VILLANI, député, président de l'Office. - Il est donc nécessaire de suivre les variations infimes du champ gravitationnel liées aux mouvements aquatiques.

Dans l'exemple mentionné par Thierry Debuisschert du capteur NV intégré dans le diamant, comment vient l'idée d'utiliser ce genre de dispositif ? Sur quels travaux et modélisations s'appuie-t-elle ? Quel dispositif réalise la mesure et ramène l'information ?

M. Thierry DEBUISSCHERT. - Le centre NV du diamant est un défaut naturel du diamant, connu bien avant la découverte des propriétés quantiques. Il s'agit de l'impureté la plus commune des diamants naturels, qui leur donne une couleur rosée. Il existe une centaine de défauts connus dans le diamant. Le centre NV a d'abord été identifié pour ses propriétés d'émetteur de photons uniques. Le centre NV peut être isolé. En le pompant avec un laser impulsionnel suffisamment intense, on peut lui faire émettre un photon à la fois. Il s'agit d'une des premières sources de photons uniques jamais développées et il a l'avantage d'avoir une très grande photostabilité : il peut être éclairé de manière intense sans être détruit et il est stable dans le temps. L'information est captée en mesurant la quantité de lumière rouge émise par le centre NV. Lorsqu'il interagit avec une grandeur extérieure, cette quantité de lumière va diminuer avec un phénomène de résonance. Lorsque la radiofréquence qui va exciter le centre NV coïncide avec la transition (les deux niveaux que j'ai évoqués), la luminescence diminue. En mesurant cette diminution de luminescence, on peut caractériser et mesurer la grandeur à déterminer.

M. Cédric VILLANI, député, président de l'Office. - J'invite les parlementaires qui sont en ligne à intervenir s'ils le souhaitent.

M. André GUIOL, sénateur. - Ces présentations étaient passionnantes. J'ai connu les premiers pas de l'informatique et vos descriptions donnent le vertige pour l'avenir. J'ai relevé que 5 % du financement du Plan quantique étaient issus du budget de la défense nationale : est-ce suffisant compte tenu des enjeux stratégiques auxquels nous serons confrontés dans les années à venir ?

M. Georges-Olivier REYMOND. - Je précise que le fonds d'investissement de la Défense (Def'Innov) a investi dans Pasqal. De nombreux cas d'usage sont à développer dans le domaine. Un axe de la commande pourrait être de développer ces applications pour la défense. Les technologies commencent à être prêtes.

M. André GUIOL, sénateur. - Quand on sait quelle était la compétence technologique dont disposait la France en matière de microprocesseurs et qu'elle l'a perdue, et quand on connaît les difficultés que rencontre par exemple l'industrie automobile aujourd'hui, il faudra veiller à ne pas se laisser distancer dans ces nouvelles technologies quantiques, notamment en matière de matériel.

M. Neil ABROUG. - La DGA est pleinement associée à la gouvernance multipartite du Plan Quantique assurée par les ministères de l'Économie, de la Recherche et des Armées. La DGA est soumise à une loi de programmation militaire (LPM) qui fige ses investissements sur le long terme. La contribution de la DGA dans le cadre du Plan Quantique s'inscrit dans la LPM, dans laquelle elle a pris le maximum des libertés qu'elle pouvait prendre. La DGA était bien consciente des enjeux du quantique, avant même la mise en place du Plan Quantique, notamment en matière de capteurs et de cryptographie post-quantique. Il est probable que les prochains exercices de la LPM renforceront ce volet. Aujourd'hui, elle correspond à ces 5 %. Dans le cadre de la stratégie nationale, il nous revient donc de veiller à la cohérence et la coordination entre les actions portées par la DGA et la liberté d'action que nous avons dans le cadre du PIA.

L'appel à manifestation d'intérêt « maturation » qui ciblera spécifiquement les capteurs et qui sera rendu public dans les trois prochaines semaines, mentionne explicitement le fait que les porteurs des actions de maturation doivent mettre en place une coordination avec la DGA, afin que les travaux issus des structures de transfert de technologies puissent à la fois alimenter les programmes de la DGA pour les applications de défense et alimenter les programmes soutenus par le PIA pour les applications civiles des capteurs.

L'un des principaux enjeux de la stratégie est également la viabilité économique à long terme des capteurs. Il est important d'avoir de la commande publique par la DGA et des programmes de défense sur les capteurs, mais il est peut-être encore plus important que les capteurs quantiques trouvent des débouchés civils. Nous avons la responsabilité dans le cadre du PIA d'inciter à développer les marchés civils de ces capteurs. Leur sophistication et leur précision font qu'ils ciblent aujourd'hui des applications de niches. Il est nécessaire de leur trouver une viabilité économique en dehors du marché de la défense.

M. Jean LAUTIER-GAUD. - Une des clés consistera à pouvoir appliquer ces capteurs au domaine civil. Je rends en cela hommage aux travaux du service des biens à double usage du ministère de l'Économie, car cet objectif devra être conservé tout au long des

développements et des premières applications militaires pour pouvoir les appliquer un jour au domaine civil.

M. André GUIOL, sénateur. - Il s'agit de favoriser d'une manière générale la technologie duale.

M. Jean LAUTIER-GAUD. - Tout à fait.

M. Philippe CHOMAZ. - Le *hardware* est effectivement clé, d'autant que l'on pourrait nous en limiter l'accès. Sans accès au *hardware*, pas de *software* en France et en Europe. Il est important de veiller à conserver des développements de *hardware* en Europe et en France. Il ne faut pas se tromper de bataille. Par ailleurs, les capteurs quantiques sont très mûrs et sont déjà très avancés, les communications sont également bien avancées et l'ordinateur quantique est dans une phase semblable à celle des années 50, avant que la NASA remplace ses calculateurs manuels par des ordinateurs. Les enjeux d'applications pour la défense sont importants et il est nécessaire d'investir sur ces sujets, car nous faisons face à une forte concurrence. Dans les communications, il faut considérer le quantique comme une ressource et un élément de sécurité supplémentaires : nous n'allons pas basculer dans un monde « tout quantique ». La transformation aura lieu au niveau du système, avec le déploiement de ressources classiques et de quelques ressources quantiques.

M. André GUIOL, sénateur. - Vous avez évoqué nos partenaires européens et les Etats-Unis, mais sait-on où en est la Chine dans ce domaine ?

M. Philippe CHOMAZ. - La Chine investit massivement et possède depuis longtemps un Plan quantique très développé, sur différents systèmes. Elle a réalisé des premières démonstrations avec les communications par satellite. Dans sa stratégie de « saute-mouton », la Chine parie sur la génération qui vient. Il s'agit d'un concurrent fort sur la scène internationale.

Mme Pascale SENELLART. - Nous avons bien identifié la force de frappe des chercheurs chinois. On entend peu parler de *start-up* chinoises, mais des groupes académiques sont massivement financés. L'avantage quantique calculatoire réalisé avec des photons a été démontré par un groupe chinois très connu, qui a bénéficié de moyens financiers hallucinants. Par exemple, l'équipe chinoise s'est attaquée à des problèmes calculatoires de complexité informatique très connus (calcul des permanents) et a comparé la vitesse des meilleurs supercalculateurs existants avec leur machine quantique. Les pairs scientifiques consultés pour la publication des travaux ont constaté que l'équipe montrait un avantage vis-à-vis d'un supercalculateur, mais ont noté que le calcul n'avait pas été réalisé avec beaucoup de qubits. Pour répondre à cet argument, l'équipe a dépensé près de 200 000 dollars supplémentaires. Cela ne se voit pas ailleurs.

M. Cédric VILLANI, député, président de l'Office. - Sur ce calcul des permanents, leur ordinateur quantique a donc été plus efficace que l'ordinateur classique.

Mme Pascale SENELLART. - Selon mes collègues théoriciens, le calcul des permanents est un des rares problèmes pour lequel l'avantage quantique est démontré théoriquement.

M. Sébastien TANZILLI, directeur de recherche à l'Institut de physique de Nice. - Au-delà des financements, la Chine a la particularité de beaucoup anticiper. Philippe Chomaz a mentionné le programme de communication quantique par voie spatiale. Les premiers résultats ont abouti en 2016 et le programme spatial chinois de satellites de communication quantique a commencé dès les années 2007 et 2008, avec des financements monumentaux.

M. Philippe DULUC. - Concernant la cryptographie post-quantique, il existe un programme chinois concurrent direct du programme de standardisation américain que j'ai évoqué.

M. Thierry DEBUISSCHERT. - Les Chinois possèdent 5 satellites en réserve pour étendre un réseau. L'Agence spatiale européenne (ESA) a été sollicitée depuis une quinzaine d'années pour lancer des satellites quantiques, et ce sont les Chinois qui l'ont finalement fait. J'ai assisté à des réunions à l'ESA dans lesquelles les chercheurs européens et notamment l'équipe d'Anton Zeilinger de Vienne insistait pour que l'ESA lance ces satellites quantiques, car toute la technologie et le savoir-faire étaient disponibles. Cela n'a jamais pu être fait et la Chine a devancé l'Europe et les États-Unis avec un changement d'échelle.

Les Chinois ont la volonté d'apparaître comme des leaders, quitte à lancer des opérations de communication à la limite de la désinformation, comme l'illustre l'affaire des « radars quantiques » grâce auxquels les Chinois prétendaient être capables de détecter des avions à des centaines de kilomètres. Cette annonce a suscité une effervescence dans tous les ministères de la défense européens et américains : il s'agit probablement d'une désinformation qui amène les autres pays à mobiliser, voire détourner les énergies des vrais objectifs.

M. Cédric VILLANI, député, président de l'Office. - Je reviens sur les cas d'usage. La programmation quantique a pris un virage quand Peter Shor a montré qu'un algorithme quantique pouvait factoriser les très grands nombres premiers. La question des problèmes que l'on pouvait mieux résoudre de manière quantique que de manière classique s'est alors posée. L'apprentissage automatique quantique par les machines est resté longtemps un problème ouvert, puis des voies de résolution sont arrivées. Le calcul des permanents évoqué par Pascale Senellart est un des rares problèmes pour lequel une suprématie théorique du quantique a été démontrée. Quel est aujourd'hui l'état de l'art sur les cas d'usage et les problèmes dont on sait qu'ils pourront être traités plus efficacement d'une manière quantique que d'une autre ?

Mme Pascale SENELLART. - Le calcul quantique des permanents est désormais une réalité. Les cas d'usage se développent au fur et à mesure des progrès techniques. Nous voyons se développer des algorithmes très spécifiques, comme la résolution d'équations différentielles appliquées à la chimie qui peut se transposer à d'autres systèmes. Il serait hasardeux de rechercher dès à présent des cas d'usage bien identifiés, car la communauté se construit progressivement, comme toutes les communautés de rupture. Il est difficile de ce fait de vous apporter des exemples plus concrets que ceux évoqués au cours de cette table ronde. Les nouveaux cas d'usage émergeront lorsque de grands acteurs industriels comme EDF, Orange, Total rechercheront des optimisations.

M. Philippe CHOMAZ. - Le problème à N-Corps en chimie sera probablement un des premiers résolus par le quantique et la résolution des problèmes pourra aller jusqu'à l'équation de Navier-Stokes.

M. Cédric VILLANI, député, président de l'Office. - Deepmind annonçait il y a peu de temps pouvoir prédire la structure de protéines grâce au logiciel d'intelligence artificielle (IA) Alphafold, donc sans ordinateur quantique mais avec un algorithme « réseau de neurones ». Est-il possible de rétorquer que ces problèmes pourront être résolus par d'autres manières, moins exhaustives et plus approchées, mais qui seront suffisantes pour les cas d'usage ?

M. Philippe DULUC. - Il existe des cas d'usage en d'apprentissage machine. Les sujets d'optimisation combinatoire permettent de traiter des algorithmes d'apprentissage comme le *clustering*, qui vise à classer des populations selon des critères complexes et fondés sur la détection automatique de similarités. Nous savons le faire via le calcul quantique. Plusieurs cas d'usage ont été cités ce matin. Concernant l'optimisation combinatoire, un domaine intéressant pour certains utilisateurs est le problème « des voyageurs du commerce » qui permet de réaliser de l'optimisation de ressources (*ressources scheduling*), car celle-ci devient complexe dès lors que les ressources sont nombreuses. Le calcul quantique s'applique très bien dans ce domaine.

M. Georges-Olivier REYMOND. - Nos premiers concurrents sont les technologies classiques, qui réalisent également d'importants progrès. Le calcul quantique apporte un avantage important en termes d'énergie consommée : un processeur quantique consomme moins d'électricité que cinq sèche-cheveux. Pasqal a développé un algorithme d'apprentissage machine quantique, qui pour le moment n'est pas aussi performant que les solutions d'apprentissage profond, mais consomme 5 kilowatts, ce qu'il faut comparer aux « tonnes » d'électricité nécessaires pour faire tourner un centre HPC construit à base de processeurs graphiques. L'avantage réside certes dans la performance, mais également dans le coût économique et énergétique sous-jacent.

M. Cédric VILLANI, député, président de l'Office. - Cette remarque est très intéressante. Pour aller au bout de la logique, il serait nécessaire de comparer également les coûts de production, mais ces technologies en sont à des stades de maturation différents et sont donc difficilement comparables en l'état.

Mme Pascale SENELLART. - L'estimation de l'avantage énergétique apporté par les technologies quantiques est engagée. La question, compliquée, est liée à la qualité et la fiabilité du calcul quantique. On ne sait pas encore si un ordinateur avec correction d'erreur serait plus économe en énergie qu'un ordinateur classique. Il semblerait que les ordinateurs de petite taille avec des qubits imparfaits présentent un avantage énergétique mais on ne sait pas si cela reste vrai en passant à l'échelle ; il serait nécessaire de lancer une étude sur le sujet.

M. Philippe CHOMAZ. - Je confirme que les technologies classiques avancent : en termes énergétiques, la spintronique, les nouveaux moyens de calcul électroniques, la vallée-tronique bénéficient de nombreuses innovations. Il s'agit d'une course. L'élément le plus marquant à mon sens est la taille de l'espace de Hilbert, c'est-à-dire la taille de la mémoire nécessaire pour stocker les calculs. Certains calculs réalisés sur un ordinateur quantique ne rentrent dans aucune mémoire d'ordinateur classique. Il faut avoir en tête ces ruptures relatives à la mémoire.

M. Cédric VILLANI, député, président de l'Office. - Je vous remercie de tous ces éléments. Nous aborderons la deuxième table ronde après une courte pause.

*
* *

Seconde table ronde : communications quantiques et cryptographie post-quantique

M. Cédric VILLANI, député, président de l'Office. - Cette seconde table ronde sera plus courte que la première, avec quatre intervenants. On peut regretter l'absence de parité. Les sujets technologiques manquent hélas de femmes et notre société doit se donner l'objectif d'y remédier. Nous accueillons :

- Sébastien TANZILLI, directeur de recherche à l'institut de physique de Nice, pilote de l'équipe Quantum@UCA, projet-pilote de communication quantique en région PACA en partenariat avec Orange ;

- Cédric OUDIETTE, directeur de la stratégie des programmes futurs pour les communications sécurisées chez Airbus, impliqué dans le consortium européen EuroQCIE, pour les premiers éléments du futur internet quantique européen ;

- Henri GILBERT, responsable des laboratoires de cryptographie de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), qui exposera la vision de l'ANSSI du monde post-quantique et ses recommandations en matière de cryptographie ;

- Damien STEHLÉ, professeur à l'ENS Lyon, qui présentera les dernières avancées des méthodes de cryptographie post-quantique.

Je vous propose comme précédemment d'enchaîner les exposés avant de procéder aux questions/réponses.

M. Sébastien TANZILLI, directeur de recherche à l'institut de physique de Nice. - M. le président, Mesdames et Messieurs les députés et sénateurs, je vous remercie de votre invitation. Je suis directeur de recherche du CNRS à l'Institut de physique de Nice, laboratoire conjoint de l'Université Côté d'Azur (UCA) et du CNRS. Je me propose de vous présenter un point de situation sur la mise en place d'un *test bed* (banc d'essai) d'un réseau de communication quantique opérationnel à Nice Côte d'Azur nommé Quantum@UCA. J'ai sous-titré ma présentation en indiquant que nous allons de la production d'intrication photonique à l'établissement de clés secrètes de cryptographie. Comment établir des clés secrètes entre partenaires distants pouvant servir à des tâches de cryptographie avec de l'intrication photonique ? L'idée est d'établir un *benchmark* quantique grâce à des clés privées de cryptographie pour effectuer des tâches de communication que les moyens d'information classiques ne permettent pas de faire ou ne font pas de manière satisfaisante.

Une source génère une paire de photons intriqués, dont l'un est envoyé à Alice et l'autre à Bob. Dans la table ronde précédente, il a été question de superposition cohérente d'états d'un système quantique unique (état 0 et état 1). Ici, on a augmenté la dimension de l'espace de Hilbert des configurations quantiques, puisqu'on dispose d'une paire de qubits qui lorsqu'ils sont produits, sont tous les deux dans une superposition des états 0 et 1. Si ces deux photons sont distribués respectivement à Alice et à Bob, ces derniers peuvent demander à leur photon respectif quelle est sa valeur d'information. Grâce à l'intrication quantique, si Alice obtient la valeur logique 0 sur l'un des deux qubits intriqués, le photon de Bob aura automatiquement la même valeur. Les résultats des mesures chez Alice et Bob, lorsqu'on produit un état intriqué de cette manière, sont parfaitement corrélés.

Comment aller jusqu'à l'établissement de clés secrètes entre ces deux partenaires, éloignés de quelques kilomètres à plusieurs centaines de kilomètres ? Le protocole basé sur l'intrication induit que les résultats chez Alice et Bob sont non seulement parfaitement corrélés, mais aussi purement aléatoires. Le photon parti de la source jusqu'à chez Alice n'a jamais porté seulement l'état 0 puisqu'il était dans une superposition des états 0 et 1. C'est seulement lorsqu'Alice a procédé à sa mesure que ce photon a révélé son état logique. Automatiquement, la même valeur est apparue chez Bob. Des chaînes de bits établies de part et d'autre, chez Alice et Bob, sont donc à la fois parfaitement corrélées et parfaitement aléatoires. Elles peuvent être considérées comme parfaitement secrètes. La sécurité vis-à-vis de ces chaînes de bits établies aléatoirement et parfaitement corrélées est testée grâce à des témoins d'intrication. Plutôt que de faire des analyses dans la base 0 et 1, les analyseurs permettent de tester la qualité de l'intrication et de savoir, en cas d'attaque, si les clés sont bien secrètes.

Le projet Quantum@UCA vise la mise en place d'un réseau quantique opérationnel en champ réel, en partenariat entre l'UCA et Orange. Une convention de coopération a été signée en mai 2019 et a consisté à réserver une paire de fibres noires pouvant relier 3 campus de l'UCA. Il a été nécessaire de déterminer le routage spécifique de ces fibres pour relier ces 3 campus en évitant tous les systèmes classiques incompatibles avec la manipulation d'information quantique. Il a fallu également réaliser des travaux de génie civil pris en charge par Orange afin de concaténer ces fibres noires, d'éviter les répéteurs et d'avoir accès aux fibres optiques dans les bâtiments prévus. La convention crée aussi une collaboration entre les laboratoires d'Orange travaillant sur la cryptographie sécurisée par des moyens quantiques (*Quantum Safe Cryptography*) et notre équipe, afin de rendre ce réseau fonctionnel à court terme.

L'objectif est de créer un lien de communication quantique avec un *benchmark* de cryptographie quantique : le premier site (Bob) est dans la salle des machines d'Inria du campus SophiaTech, le deuxième (Alice) est basé à l'Institut de physique de Nice et le troisième (source des paires de photons intriqués) dans un bâtiment de la métropole Nice Côte d'Azur, dans le nouveau campus « Ecovallée de la Plaine du Var » de l'UCA. 15 kilomètres séparent la station centrale d'Alice et 35 kilomètres séparent la station centrale de Bob, soit 50 kilomètres au total. Lorsqu'une paire de photons est produite, l'un est véhiculé vers Alice et l'autre vers Bob. La mise de fonds de ce projet s'est faite via l'Idex UCA^{Jedi}, la métropole Nice Côte d'Azur, la société Orange et un projet Horizon 2020.

Les fibres opérationnelles ont été obtenues en janvier 2020, mais la crise sanitaire n'a pas permis de reprendre nos activités de recherche sur le terrain avant novembre 2020. Depuis juillet 2021, les caractéristiques opérationnelles de ce réseau sont les suivantes :

- le lien fonctionne en continu, ce qui est une première en Europe ;
- toutes les opérations effectuées (génération, mesure, distillation des clés…) sont faites à la volée, ce qui a permis de développer des algorithmes de correction d'erreurs, d'amplification de la confidentialité ;
- le système permet de générer et transmettre des clefs secrètes avec un débit de 10 kilobits par seconde soit 10 millions de bits secrets par heure ;

- la plupart des systèmes sont développés en interne, à l'Institut de physique de Nice : source d'intrication, analyseurs de qubits, synchronisation des nœuds, logiciels de traitement.

Le réseau Quantum@UCA se veut être un *test bed* ouvert offrant un environnement propice pour tester divers protocoles et divers états quantiques et diverses technologies de photonique quantique.

Les perspectives à court terme consistent à augmenter le débit : une démonstration de laboratoire a montré que via des stratégies de multiplexage fréquentiel et temporel compatibles avec les réseaux télécoms standards, on pourrait viser des débits de clefs secrètes proche du mégabits par seconde.

Les perspectives à court et moyen terme consistent à utiliser ce lien de cryptographie quantique et faire de la téléportation à base de photons uniques (fournis par Quandela) et d'intrication photonique. Nous développons un étage de conversion de fréquence en optique non linéaire intégrée : il s'agit de convertir la longueur d'onde des photons issus de la boîte quantique vers une longueur d'onde télécom, afin de rendre les sources de photons uniques compatibles avec les standards de télécommunication.

À plus long terme, nous avons obtenu, avec Thales Alenia Space et Sorbonne Université, un contrat avec le CNES pour définir des architectures de communication quantique via le segment spatial. Nous avons également obtenu un soutien de l'Agence de l'innovation de défense pour intégrer des sources de lumière quantique afin qu'elles répondent aux contraintes spatiales et être embarquées sur un satellite.

M. Cédric VILLANI, député, président de l'Office. - Je vous remercie. Il est intéressant de voir à quel point ce projet est leader dans son domaine. Je donne la parole à M. Oudiette.

M. Cédric OUDIETTE, directeur de la stratégie des programmes futurs pour les communications sécurisées chez Airbus. - Merci beaucoup M. le président, Mesdames et Messieurs les parlementaires. Je vous présenterai ce que fait Airbus dans le domaine des communications quantiques, notamment dans le cadre du programme européen Europlus Line.

Le cœur de métier de notre activité concerne les communications hautement sécurisées pour les gouvernements et les ministères de la défense. L'avènement des ordinateurs quantiques est riche de promesses, mais amène également de nouvelles menaces. Il met notamment en péril la sécurité des réseaux tels qu'on les connaît aujourd'hui et fragilise la robustesse de la cryptographie des échanges qui transitent dans un réseau.

L'objectif du programme européen est de développer la première brique d'un internet quantique à l'échelle européenne et d'assurer une transmission de clés sûre permettant de répondre à ce nouveau défi lié au progrès quantique. La transmission de la clé est totalement sécurisée, basée sur les propriétés physiques de la lumière, et il est impossible pour un *hacker* de lire cette information sans que ceci soit connu. Les communications quantiques sont à la fois l'épée et le bouclier, car elles créent de nouvelles menaces, mais permettent aussi de communiquer de manière totalement sécurisée.

La vision européenne est incrémentale : l'étape de l'année 2021 est celle des études de systèmes qui permettront de définir l'architecture des prochains réseaux. Airbus mène un des deux consortia aujourd'hui avec Orange et de nombreux partenaires européens. À l'issue de cette étude, la Commission européenne exploitera une architecture technique afin de déployer un premier système par étape : démonstrateurs en 2024, système pleinement opérationnel permettant l'échange de clés quantiques en 2028 afin d'aller vers l'internet quantique complet et totalement inviolable en 2035.

Ce programme intègre une dimension terrestre, portée par Orange, et une dimension spatiale. En effet, l'une des problématiques des communications quantiques est la préservation de la clé sur une distance de plus de quelques dizaines de kilomètres. Les solutions spatiales permettent d'avoir une plus grande élongation. La vision est celle d'un système : pour avoir un réseau résilient pour un usage gouvernemental, il est nécessaire de combiner à la fois une dimension terrestre, organisée autour d'un réseau de fibres noires avec des nœuds sécurisés sur le territoire national et des nœuds frontières entre les pays, et une dimension spatiale satellitaire, qui permet de transmettre des clés par envoi de photons et qui présente à la fois un avantage en termes de distance et des inconvénients liés à une moindre efficacité pendant la journée et à des moindres débits. Pour l'utilisateur final, le système fonctionne de manière transparente et permet de passer des communications sécurisées. Un orchestrateur allouera en permanence le trafic, priorisera et déterminera des règles d'acheminement et de transmission des clés.

Un des principaux défis de ce programme concerne l'interopérabilité. L'information doit passer des frontières et transiter dans un réseau avec des particularités régionales ou locales. L'objectif est de concevoir une architecture système pleinement interopérable et interconnectée. Orange nous apporte son savoir-faire dans ce domaine en s'appuyant sur l'infrastructure existante, en faisant mûrir des solutions et en les transposant à l'échelle industrielle.

Le rythme des prochaines étapes est rapide. Sur les systèmes, des appels d'offres européens sont attendus dès 2022 sur la partie terrestre et orchestration, avec un objectif de déploiement d'un premier prototype en 2024. Sur le segment spatial, la réponse de l'ESA est arrivée et des appels d'offres sont attendus début 2022. À un horizon de 3 ou 4 ans, nous aurons en orbite et au sol des éléments de systèmes permettant d'avoir une première expérience opérationnelle. L'objectif est ensuite de passer d'une étape d'innovation en laboratoire ou en *start-up* à une échelle opérationnelle, avec des éléments mesurables pour un utilisateur.

En connexion avec le Plan Quantique français, nous avons d'excellentes chances de positionner la France comme un acteur leader dans ce programme européen. Cela passe par une exploitation maximale et une optimisation des complémentarités entre financements européens et français et par la mise en place d'une équipe française unie et forte.

Toutes les technologies sont maîtrisées en laboratoire et dans des universités et il est désormais nécessaire de passer à une échelle industrielle, de bâtir des filières d'excellence et d'être capable de produire de manière récurrente un service reconnu comme fiable et résilient. D'un point de vue technique, les communications optiques sont la base des communications quantiques. Airbus est le chef de file dans le domaine spatial pour structurer la filière industrielle concernant les liaisons laser entre l'espace et le sol. Capitaliser sur les filières qui existent déjà en France permettra d'aboutir à une autonomie maximale en Europe avec un contenu français important.

Je souligne l'importance du Plan Quantique français qui permettra de passer à la vitesse supérieure en accélérant et démultipliant les actions en cours. Le fait que l'État se positionne en utilisateur de ce système est un fort élément de crédibilité apporté aux futurs utilisateurs.

M. Cédric VILLANI, député, président de l'Office. - Messieurs Tanzilli et Oudiette, à quel horizon peut-on attendre que ces usages soient bien implantés et deviennent courants ?

M. Sébastien TANZILLI. - En tant que pilote du projet, j'ai toujours souhaité inscrire ce *test bed* de communication quantique azuréen dans son territoire, ce qui explique la présence de la métropole Nice Côte d'Azur. Nous identifions actuellement un cas d'usage qui permettrait de sécuriser des échanges de données sensibles entre divers bâtiments de la métropole. La sécurisation des échanges de données soulève deux questions : pour un jeu de données, quel est le niveau de sécurisation nécessaire ? Quel est le degré de pérennité avec lequel on souhaite sécuriser cette information sensible ? Ce cas d'usage répondrait à cette question de haute sécurité et de pérennité.

M. Cédric OUDIETTE. - On peut distinguer deux étapes. La première consiste à échanger des clés quantiques dans un réseau avec des nœuds sécurisés avec un déchiffrage et un rechiffrage : un système sera opérationnel à l'horizon 2028, dans le cadre du programme EuroQCI. La seconde étape concerne l'échange de photons intriqués, autrement dit la téléportation photonique, qui est en maturation et un réseau opérationnel n'est pas attendu avant 2030-2035.

M. Sébastien TANZILLI. - Deux cas d'usages ont été identifiés par la communauté des chercheurs et consistent à mettre en relation des processeurs ou des capteurs quantiques via des procédés sécurisés d'échanges de données. La stratégie nationale s'appuie sur plusieurs piliers de développement et l'une des perspectives de cet outil de financement sera de réfléchir à une architecture permettant à des processeurs quantiques de communiquer les uns avec les autres pour en décupler la puissance, via une sécurisation des transmissions de données par cryptographie quantique – la même chose valant évidemment pour les capteurs.

M. Cédric VILLANI, député, président de l'Office. - La technologie est-elle stabilisée ou plusieurs types d'architecture sont-ils encore explorés ?

M. Sébastien TANZILLI. - La réponse est à la fois oui et non. On a identifié le photon comme le porteur d'information quantique privilégié : les photons intriqués tels que ceux produits à l'UCA par optique non linéaire, ou les photons uniques tels que ceux produits par le C2N ou par Quandela. D'autres plateformes technologiques que celles évoquées aujourd'hui permettent de générer des photons uniques ou intriqués. Les photons sont le véhicule principal pour établir des clés secrètes à distance, mais d'autres éléments des architectures de réseaux de communication quantique ne sont pas encore sortis des laboratoires, comme les mémoires quantiques qui sont des systèmes matériels à base d'atomes froids ou de défauts du diamant. À terme, il faudra pouvoir coupler génération et manipulation de photons pour établir des clés secrètes, mémoire quantique pour stocker, reproduire et distiller l'information quantique, en combinaison avec le segment spatial par satellite.

Mme Pascale SENELLART. - Des efforts sont également réalisés sur la cryptographie avec d'autres vecteurs lumineux, qui relèvent de ce que l'on appelle les variables continues, notamment par les équipes d'Eleni Diamanti et Philippe Grangier. Leur approche s'appuie sur des composants « sur étagères » permettant d'utiliser des objets plus faciles à produire et dès à présent de réaliser des échanges de clés cryptographiques. On a donc la chance, en France, d'avoir des acteurs travaillant selon deux approches techniques différentes, même si celle-ci permet l'échange de clés cryptographiques mais n'ouvre pas à l'internet quantique qui permettra peut-être un jour de mettre en réseau des ordinateurs quantiques.

M. Cédric OUDIETTE. - La transmission de clés mobilise deux familles de technologies, en variables continues ou en variables discrètes, et d'un point de vue industriel, l'enjeu est de réussir à obtenir des standards et de l'interopérabilité ; ceci n'empêche pas la coexistence de plusieurs technologies mais elles doivent se placer dans un cadre cohérent. La communication entre ordinateurs quantiques est plus disruptive, avec un aspect multiplicateur qui n'existe pas dans le monde des calculateurs standards. Lorsqu'on connecte deux ordinateurs quantiques, on obtient un facteur d'échelle exponentiel. Sur ce volet, les standards et les niveaux de performance n'ont pas encore été définis.

M. Thierry DEBUISSCHERT. - Nous avons réalisé une démonstration sur le terrain de distribution de clés par variables continues voici 10 ans entre Massy et Palaiseau, qui a fonctionné pendant 6 mois. Cette technologie, établie, est en phase d'être reprise par Thales Alenia Space qui possède un savoir-faire de distribution quantique de clés notamment pour les applications spatiales, sur les protocoles quantiques et également sur les stations au sol permettant de faire des communications optiques avec les satellites.

M. Damien STEHLÉ, Professeur à l'ENS Lyon. - Je souhaite apporter quelques corrections à certains propos que j'ai entendus sur les communications quantiques. Je suis spécialiste en cryptographie, mon domaine de recherche depuis une quinzaine d'années. Il faut être vigilant sur ce qui est dit de la sécurisation des données avec les communications quantiques : l'installation de nœuds pour déchiffrer et rechiffrer les données représente une faille de sécurité monumentale et il est dangereux de déployer ce type d'infrastructures. La sécurisation des données passe par deux propriétés fondamentales : la confidentialité (les données sont secrètes) et l'authenticité (je sais à quelle personne je parle). Dans certains cas de figure, le besoin d'authenticité ne s'accompagne pas nécessairement d'un besoin de confidentialité, par exemple pour la signature de documents, mais il est très rare d'avoir besoin de confidentialité sans avoir besoin d'authenticité. Les communications quantiques apportent une forme de solution pour la confidentialité, mais pas pour l'authenticité. Dans tous les cas, la sécurité du système repose sur celle du maillon le plus faible, en l'occurrence la sécurité de l'authenticité.

M. Thierry DEBUISSCHERT. - La question de l'authentification du canal en cryptographie quantique a été beaucoup étudiée et a notamment été prise en compte par le réseau Secoqc (*Secure Communication based on Quantum Cryptography,* soit Communication sûre fondée sur la cryptographie quantique) développé à Vienne, en Autriche, voici une dizaine d'années et qui regroupe plusieurs acteurs européens. Il utilise des fonctions de hachage et de sécurité inconditionnelle afin de garantir qu'Alice parle bien à Bob, sans espion dans le canal.

M. Henri GILBERT, responsable des laboratoires de Cryptographie de l'ANSSI. - L'ANSSI est l'autorité nationale en matière de cybersécurité. Je partirai d'une esquisse du domaine technique de la cryptographie post-quantique et j'évoquerai l'utilité et les modalités du déploiement de la cryptographie post-quantique. La menace quantique est celle que représente l'éventualité de l'apparition d'ordinateurs quantiques très puissants pour la sécurité des informations numériques. La cryptographie post-quantique est une branche de la cryptographie qui vise à prévenir la menace quantique par des moyens fondés sur des principes mathématiques. Il ne faut pas la confondre avec la cryptographie quantique qui vise à prévenir cette menace par des moyens fondés sur les principes de la physique quantique.

La cryptographie permet de protéger des informations numériques au moyen d'algorithmes cryptographiques en utilisant de manière combinée deux principales catégories d'algorithmes : les algorithmes symétriques (chiffrement des communications) et asymétriques (établissement de clés, signatures numériques). L'excellence française académique et industrielle est reconnue dans le domaine de la cryptographie et l'ANSSI a un rôle de conseil et d'autorité réglementaire.

Précisons la menace quantique. Si des ordinateurs quantiques à très grande capacité de calcul voient le jour, la cryptographie asymétrique actuelle s'effondrera car sa sécurité repose sur des problèmes mathématiques faciles à résoudre pour un ordinateur quantique ; la cryptographie symétrique sera plus faiblement affectée et il suffira pour restaurer sa sécurité d'adapter légèrement les paramètres.

M. Cédric VILLANI, député, président de l'Office. - Pouvez-vous rappeler quels sont les principes de la cryptographie asymétrique et de la cryptographie symétrique ?

M. Henri GILBERT. - La cryptographie symétrique repose sur le partage préalable par les interlocuteurs d'un secret commun, la clé. La cryptographie asymétrique échappe à la nécessité d'une possession préalable de secret et permet de régler de grands problèmes comme des échanges de données sécurisées dans de très grands réseaux.

Il est difficile de prédire si de tels ordinateurs existeront un jour et, dans l'affirmative, s'ils apparaîtront avant ou auprès 2035, mais la prudence commande de commencer à se prémunir dès maintenant contre les attaques de tels ordinateurs, afin notamment de prévenir les attaques rétroactives du type « *enregistrer maintenant sur des systèmes actuels, cryptanalyser n années plus tard* ». Pour des données hautement sensibles à protéger durablement, nous sommes dès aujourd'hui exposés à cette menace.

L'ANSSI recommande, comme la plupart des agences mondiales de sécurité, de commencer à prévenir cette menace quantique dès que possible, c'est-à-dire dans un délai de 1 à 4 ans, au moins dans deux cas : lorsque les informations sensibles nécessitent une protection de longue durée au-delà de 2030 ; pour les produits de sécurité susceptibles de continuer à être utilisés au-delà de 2030. Et cela, en déployant des solutions post-quantiques « hybrides ».

Un des grands avantages de la cryptographie post-quantique est d'être déployable dans les systèmes de communication numériques sans modifications majeures, tout en nécessitant quelques adaptations de la partie cryptographique. Elle enrichit la boîte à outils des algorithmes asymétriques actuellement déployés avec des algorithmes post-quantiques, dont la sécurité est fondée sur des problèmes mathématiques conjecturés comme résistant aux ordinateurs quantiques. Il existe 5 principales familles d'algorithmes asymétriques post-

quantiques fondés sur les réseaux euclidiens et les codes correcteurs d'une part, et sur les graphes d'isogénies, la cryptographie multivariée et le hachage de l'autre.

L'ANSSI considère que la cryptographie post-quantique est une réponse réaliste à la menace quantique. La France abrite une proportion substantielle des compétences mondiales sur les quatre premières familles d'algorithmes mentionnées ainsi qu'un écosystème riche de la sécurité numérique capable de développer des solutions allant de la recherche publique aux entreprises de la sécurité numérique en passant par des *start-up* pour le développement de briques logicielles ou matérielles.

La cryptographie quantique est une autre réponse à la menace quantique, mais elle nécessite une infrastructure spécifique de liaisons quantiques point à point. L'ANSSI a rédigé un avis scientifique et technique sur les possibilités ouvertes par la cryptographie quantique. En tant que cryptologue, je rejoins les commentaires de Damien Stehlé qui sont convergents avec le contenu de l'avis.

La cryptographie quantique ne fournit pas un équivalent fonctionnel complet de la cryptographie asymétrique, notamment en raison de fortes contraintes de déploiement. En milieu terrestre, on ne peut pas avoir l'équivalent des capacités de routage actuelles sur un grand réseau et elle n'est pas déployable à grande échelle avec une haute sécurité pratique, sauf en prenant le risque d'utiliser des nœuds de confiance, ce qui fait considérablement chuter la sécurité.

Les possibilités ouvertes restent proches de ce que permettent des architectures de gestion de clé fondées uniquement sur la cryptographie symétrique, que l'ordinateur quantique menace faiblement.

L'emploi de la cryptographie quantique est envisageable dans un nombre limité de cas. La recommandation sera de l'utiliser en complément à une protection cryptographique, à titre de défense en profondeur.

La campagne de normalisation du *National Institute of Standards and Technology* (NIST) vise à sélectionner des algorithmes symétriques post-quantiques et à établir des clés et des signatures en vue de leur normalisation par l'État américain. Plus de 80 algorithmes issus du monde entier ont été examinés : au troisième tour, il reste 7 finalistes, dont 2 seront probablement sélectionnés avant fin 2021, et 8 finalistes alternatifs. La légitimité du NIST pour mener ce genre d'opération est paradoxale, car il s'agit d'un organisme national de normalisation ; elle provient de sa capacité unique à mobiliser la communauté de recherche. Il joue un formidable rôle d'accélérateur de la maturation du domaine. La recherche académique et industrielle française est très fortement représentée dans le processus engagé, puisque 5 finalistes et 4 alternatifs ont au moins un co-auteur français.

Notre perception de la maturité des techniques post-quantiques est assez bonne, notamment grâce aux efforts du NIST, mais elle ne doit pas être surestimée. On manque encore de recul, davantage que pour la cryptographie actuellement déployée, sur la sécurité classique et post-quantique des algorithmes, sur leur intégration dans des protocoles plus complexes et sur la sécurité des implémentations.

En conséquence, le remplacement direct des algorithmes asymétriques classiques existants par les nouveaux algorithmes asymétriques post-quantiques entraînerait un risque significatif de régression de la sécurité face aux attaquants actuels. Ce constat ne doit toutefois

pas servir d'argument pour retarder le début de la migration, mais appelle certaines précautions afin de prévenir toute régression. Une courte phase d'apprentissage pourrait être tolérée afin que ces techniques deviennent un jour une solution de substitution complète.

Les préconisations de l'ANSSI sur la transition post-quantique sont les suivantes :

- respecter le principe de non-régression de la sécurité classique : tout « saut direct » vers un algorithme post-quantique asymétrique utilisé isolément est proscrit. La seule exception est celle des signatures fondées sur le hachage ;

- l'hybridation : afin d'assurer une sécurité post-quantique, il convient de recourir à des mécanismes hybrides combinant un algorithme asymétrique post-quantique avec un algorithme asymétrique classique éprouvé. Le surcoût par rapport à un « saut direct » vers l'algorithme post-quantique est faible ;

- la migration rapide, si possible dans un délai de 1 à 4 ans, dans les cas suivants : pour les informations sensibles nécessitant une protection de longue durée au-delà de 2030 et pour les produits de sécurité susceptibles de continuer à être utilisés au-delà de 2030, en utilisant des solutions hybrides.

L'ANSSI publiera avant la fin de l'année un avis sur la cryptographie post-quantique où il sera question de migration et qui définira les grandes lignes d'un schéma de migration en 3 phases. La phase 1, au moins jusqu'en 2025, correspondra au début de la migration et à une phase d'apprentissage. La phase 2, jusqu'en 2030, visera un renforcement des exigences. La phase 3, après 2030 verra la finalisation de la migration.

M. Cédric VILLANI, député, président de l'Office. - Je vous remercie pour cette présentation et je propose d'entendre M. Damien Stehlé.

M. Damien STEHLÉ, Professeur à l'ENS de Lyon. - Merci M. le président, Mesdames et Messieurs les parlementaires de votre invitation. Je me suis présenté précédemment. Je souhaite appuyer un propos très important de Pascale Senellart. Nous lançons actuellement des projets ambitieux et de grande envergure sur du long terme et la formation des étudiants est essentielle pour les construire sur des bases solides et pérennes.

Face à la menace quantique, la plupart des protocoles à clé publique déployés aujourd'hui reposent sur des variantes des problèmes suivants :

- la factorisation d'entier : étant donné $N=p\times q$, trouver p et q, ceux-ci étant des nombres premiers ;

- le logarithme discret, dans des corps finis ou sur des courbes elliptiques : étant donnés g et $k\times g$, trouver k (g étant dans un certain groupe algébrique).

Ces problèmes sont toutefois faciles à résoudre pour un ordinateur quantique suffisamment puissant. Dès aujourd'hui, un attaquant peut stocker les communications pour les déchiffrer plus tard avec un ordinateur quantique.

Qu'est-ce que la cryptographie post-quantique ? Alice et Bob veulent communiquer de manière sécurisée, avec confidentialité et authenticité, et sont classiques en ce sens qu'ils ne disposent pas de ressources quantiques. En revanche, l'attaquant a accès à un ordinateur

quantique et interagit classiquement avec Alice et Bob. La principale différence par rapport à la situation actuelle est donc la capacité de calcul de l'adversaire.

Il est nécessaire de choisir des hypothèses de difficulté calculatoire sur lesquelles on peut faire reposer la sécurité post-quantique. Pour cela, il faut identifier des problèmes algorithmiques à la fois quantiquement difficiles et suffisamment expressifs, malléables, pour permettre la construction de primitives cryptographiques. Il est rare que ces propriétés soient simultanément présentes dans les problèmes issus de la théorie de la complexité : de nombreux problèmes semblent être quantiquement difficiles, mais parmi eux peu sont suffisamment malléables pour conduire à des développements intéressants du point de vue de la cryptographie.

Certains problèmes sont issus de la cryptographie symétrique, comme les fonctions de hachage, et fournissent des signatures assez grosses (environ 30 ko), utilisables en pratique.

D'autres problèmes sont dits « algébriques » et reposent sur des objets mathématiques : codes correcteurs d'erreurs, systèmes d'équations quadratiques, isogénies sur les courbes elliptiques, réseaux euclidiens, qui fournissent du chiffrement à clé publique et des signatures de plus petite taille (moins de 2 ko).

Je suis spécialisé dans les réseaux euclidiens. Un tel réseau est l'ensemble des combinaisons linéaires entières d'une matrice, que l'on peut visualiser comme une grille dans un espace euclidien. Les réseaux euclidiens sont un objet mathématique utilisé depuis longtemps, notamment en théorie des nombres et depuis une quarantaine d'années en cryptanalyse, en optimisation, en théorie des communications ; cet objet transverse à de nombreux domaines a été étudié de façon approfondie notamment pour son intérêt en algorithmique. Avec ces réseaux, on peut construire non seulement des protocoles cryptographiques traditionnels comme les signatures ou les chiffrements, mais aussi des protocoles cryptographiques avancés qui permettent l'externalisation des calculs tout en préservant la confidentialité – je fais référence ici aux chiffrements homomorphes, procédés qui permettent d'effectuer des calculs sur des données chiffrées sans pour autant devoir les déchiffrer.

Le problème central lié aux réseaux euclidiens est formulé ainsi : étant donné B et $t = B \times k + e$ avec e petit, trouver $B \times k$. Connaissant une base B du réseau et la donnée transmise t, qui est l'information cryptée, le problème consiste à déterminer $B \times k$, le « point » du réseau le plus proche de la donnée transmise, choisi lors du cryptage ; on en déduira alors e, qui est représentatif de l'information non cryptée, le message à transmettre.

Concernant la maturité de la cryptographie post-quantique, le projet de standardisation du NIST date de 2015. La soumission des candidatures a été clôturée en novembre 2017 et plus de 80 candidatures ont été recueillies, issues de nombreux pays. La deuxième phase de sélection en janvier 2019 a fait tomber le nombre de dossiers retenus à 26 et depuis l'été 2020, la troisième phase de sélection a identifié 7 finalistes et 8 semi-finalistes. Un des objectifs annoncés par le NIST est d'aboutir fin 2021 à des premiers choix de standards. Il se laisse le choix de sélectionner plusieurs standards ou non et éventuellement de rouvrir une phase d'étude pour d'autres choix de candidats. Parmi les 7 finalistes on trouve 4 candidats aux chiffrements (Kyber, McEliece, NTRU et Saber) et trois candidats aux signatures (Dilithium, Falcon et Rainbow).

Un premier point est à signaler : la contribution des chercheurs français est importante, car ils font partie de 5 des 7 équipes finalistes. Si l'on tient compte de l'ensemble des chercheurs qui ont travaillé ou ont été formés dans des équipes françaises, la part de l'école française de cryptographie est encore plus importante. Le deuxième point intéressant est que les réseaux euclidiens semblent être le type d'objet algébrique qui se prête le mieux, à ce stade, à la cryptographie post-quantique.

Pour conclure, le processus de standardisation touche à sa fin. On peut regretter que les discussions actuelles gravitent essentiellement autour de la propriété intellectuelle alors qu'elles devraient se focaliser sur la sécurité. À plus long terme, il est nécessaire de continuer à étudier les hypothèses algorithmiques sous-jacentes, ce travail relevant de la conception d'algorithme et de l'expérimentation, classique ou quantique ; dès qu'il y aura un ordinateur quantique, les cryptographes et les cryptanalystes s'attacheront certainement à tester la puissance de calcul via-à-vis des hypothèses utilisées. Il faudra enfin concevoir des protocoles post-quantiques avancés incluant le chiffrement homomorphe, le calcul multipartite sécurisé, avec des applications plus courantes comme la monnaie électronique, le vote électronique, etc.

M. Cédric VILLANI, député, président de l'Office. - Aujourd'hui, la majorité des cyberattaques et cyber-incidents ne repose pas sur le décryptage d'un problème algorithmique, mais le plus souvent sur des failles systémiques.

M. Damien STEHLÉ. - Tout à fait.

M. Cédric VILLANI, député, président de l'Office. - De ce fait, l'objectif du post-quantique est-il d'éviter que s'ajoute à ces problèmes systémiques une faille encore supérieure susceptible de briser des protocoles ?

M. Damien STEHLÉ. - Quand on évoque la sécurité cryptographique, on est au fondement le plus bas de l'infrastructure de sécurité. S'il est cassé du point de vue mathématique, tout le reste tombe. L'effort de standardisation du NIST vise à aboutir à un standard universel utilisé à moyen ou long terme pour assurer la sécurité de l'ensemble des infrastructures d'Etat, commerciales, de communication.

M. Cédric VILLANI, député, président de l'Office. - Nous avons évoqué la question de la suprématie quantique et Mme Senellart a indiqué que l'on savait dans certains cas que l'ordinateur quantique a un avantage par rapport à l'ordinateur classique. Cet avantage n'est toutefois pas démontré dans de nombreux cas. A contrario, certains problèmes ont été identifiés dans lesquels on sait que l'ordinateur quantique n'apportera pas un avantage établi ou que les algorithmes resteront trop complexes pour être vulnérables à une attaque quantique.

M. Damien STEHLÉ. - Votre question fait référence à la théorie de la complexité en informatique. On ne sait pas à ce stade prouver que des problèmes sont impossibles ou très difficiles à résoudre, même classiquement. Cela rejoint le problème P = NP, fondamental en informatique théorique. En cryptographie, l'objectif est d'avoir une bien meilleure résistance que celle permettant de faire face à des attaquants polynomiaux. Pour savoir si des problèmes sont quantiquement difficiles, il reste nécessaire de déployer des hypothèses.

M. Henri GILBERT. - Il y a présomption qu'un certain nombre des problèmes sur lesquels repose la cryptographie symétrique soient peu affectés par l'algorithmique quantique. Cette question fait l'objet de recherches, et elle le mérite car il n'y a pas de preuve absolue de résistance aux algorithmes.

M. Damien STEHLÉ. - Dans les familles algébriques que j'ai mentionnées – codes correcteurs, réseaux euclidiens et système polynomiaux –, des problèmes sont connus comme étant NP-complets. La cryptographie ne repose pas directement sur eux, mais sur des problèmes qui en sont très proches.

M. Cédric OUDIETTE. - Nous devons rester collectivement humbles face à la difficulté du défi technique et à la vitesse du progrès technologique. Le passé a montré que le progrès peut être important. Il existe une grande complémentarité entre l'exploration de la filière de transmission de clés quantiques et la consolidation des technologies de cryptographie post-quantique. Dans un cas, la technique est inviolable mais rencontre des problèmes délicats de déploiement opérationnel – par exemple la relation inverse entre élongation et débit –, ce qui fait qu'elle peut fonctionner pour des applications très précises et hautement sécurisées, mais pas, par exemple, pour sécuriser des cartes bleues. Dans l'autre cas, nous ne sommes pas à l'abri, par la connexion quantique entre ordinateurs quantiques, d'un saut qui augmenterait fortement le facteur d'attaque.

M. Cédric VILLANI, député, président de l'Office. - La cryptographie post-quantique deviendra donc un standard universel, alors que la cryptographie quantique restera probablement limitée à quelques centres ou personnes de hautes responsabilités et ne sera pas disponible pour le tout-venant ?

M. Sébastien TANZILLI. - On entend beaucoup dire que le déploiement de la technologie quantique pour faire de la cryptographie quantique est complexe et coûteux, mais les technologies impliquant des sources de photons et les plateformes qui permettent de les générer, de les manipuler ou de les détecter ont fait des progrès considérables au cours des dix dernières années. On peut installer une source de photons uniques dans un petit cryostat et une source de paires de photons intriqués dans un appareil de la taille d'une boîte à chaussures. L'efficacité des détecteurs de photons dépasse aujourd'hui les 90 %, au lieu de 20 % il y a 10 ans. Des solutions de cryptographie quantique sont basées sur des variables continues qui ne nécessitent pas de détecteurs de photons, mais des détecteurs classiques qui sont des produits standardisés de l'industrie des télécommunications. Ce déploiement nécessitera certes un effort, mais ne me semble pas avoir une portée aussi lointaine que M. Gilbert l'a indiqué.

M. Damien STEHLÉ. - Le mot « inviolable » me semble totalement inapproprié, car il met de côté l'aspect authentification des communications. Tant que ce problème ne sera pas résolu, la confidentialité complète de la création de clés est inutile dans un cas d'usage général.

M. Cédric VILLANI, député, président de l'Office. - Pendant la Seconde Guerre mondiale, une ligne secrète a été installée entre le QG britannique et le QG américain et il n'y avait donc pas de problème d'identification, car l'émetteur et le récepteur étaient connus. Turing et d'autres ont beaucoup travaillé sur la confidentialité.

M. Sébastien TANZILLI. - Des pays voisins de la France ont commencé à travailler sur des programmes d'hybridation de cryptographie quantique et post-quantique dans lesquels le post-quantique serait dédié à l'authentification des partenaires à distance. Il faut adopter une vision plus large du quantique et du post-quantique : dans certains pays, les gens commencent à travailler ensemble et à créer des synergies entre le quantique et le post-quantique. Il serait pertinent que la France anticipe les choses pour ne pas être à la traîne dans les prochaines années.

M. Henri GILBERT. - J'ai davantage parlé de perspective limitée que de perspective lointaine, mais « lointaine » reste quand même assez vrai, car nous manquons de recul sur des aspects comme la sécurité des dispositifs de cryptographie post-quantique vis-à-vis d'attaques. Un apprentissage se fera. Les limites sont plus préoccupantes. Il ne faut pas être borné, car les efforts de R&D auront beaucoup d'autres retombées en recherche fondamentale, dans la maîtrise des techniques quantiques. Il faut toutefois être très prudent dans l'emploi de termes comme « très haute sécurité » accolés au domaine, car cela peut créer des illusions.

M. Thierry DEBUISSCHERT. - La cryptographie quantique ne prétend pas authentifier le canal entre Alice et Bob. Pour cela, on utilise des fonctions de hachage, qui ont d'ailleurs été mentionnées comme des fonctions de sécurité post-quantique. En combinant les algorithmes de cryptographie quantique et les fonctions de hachage, on réussit à garantir la sécurité de l'établissement et de la transmission des clés entre Alice et Bob. Ceci a notamment été étudié par le projet Secoqc que j'ai précédemment mentionné.

M. Sébastien TANZILLI. - La communauté de la communication quantique foisonne de nouvelles idées visant notamment à faire de la cryptographie quantique indépendante du matériel employé. Si l'on peut définir un témoin de sécurité, bien sûr basé sur l'intrication, selon le niveau de complexité du lien (pertes dans les fibres optiques ou dans l'atmosphère, détecteur), on peut borner l'action de l'espion. Dès lors que l'on garantit un certain niveau d'intrication sur le lien, on peut se déclarer totalement indépendant du matériel. Cela peut ouvrir des perspectives de haute sécurité conceptuellement nouvelles, mais qui nécessiteront des années de recherche et d'efforts supplémentaires.

M. Cédric VILLANI, député, président de l'Office. - Je remercie l'ensemble des intervenants. Nous arrivons au bout des questions. Ces quelques heures nous ont permis d'aller sur des terrains variés et d'apprécier toute la richesse des programmes de recherche quantique. Je vous remercie pour votre disponibilité et pour la qualité de ces échanges.

La réunion est close à 13 h 35.