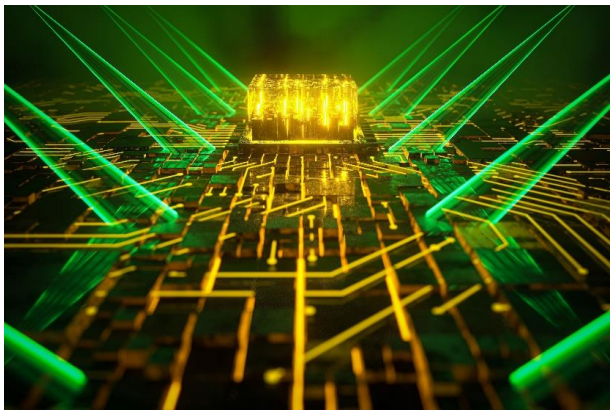
LES SYNTHÈSES DE L'OFFICE

OFFICE PARLEMENTAIRE D'EVALUATION DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES

Janvier 2022

La Stratégie quantique de la France



En 2019, l'Office parlementaire d'évaluation des choix scientifiques et technologiques s'était intéressé aux technologies quantiques en publiant quatre notes scientifiques : les enjeux, l'ordinateur quantique, la programmation quantique et la cryptographie quantique et post-quantique. Ce travail avait donné lieu à des recommandations soulignant l'importance stratégique et technologique du sujet.

Le rapport de Mme Paula Forteza, députée, publié en 2020, et les annonces du président de la République en janvier 2021 ont posé les bases d'un Plan quantique national ambitieux. Cependant, restaient à préciser les orientations du Plan ainsi que les modalités de mise en place des mesures et des financements annoncés. C'est pourquoi l'Office a organisé le 21 octobre 2021 une audition publique consacrée à la stratégie quantique française.

Le Plan quantique fait-il une place équilibrée aux différentes technologies ? Que pèsent la France et l'Europe sur la scène internationale ? Comment anticiper au mieux un monde « post-quantique » et les enjeux technologiques et stratégiques associés ? L'audition publique, qui a réuni le coordinateur de la stratégie nationale, des chercheurs et des dirigeants de grandes entreprises et de *start-up,* a permis d'approfondir nombre de questions essentielles pour l'avenir de l'informatique et la souveraineté numérique de notre continent.

Cédric VILLANI, député **Gérard LONGUET, sénateur**

L'audition a été introduite par une présentation générale de la stratégie quantique française avec l'intervention de Neil Abroug, coordinateur national de la stratégie quantique. Deux tables rondes ont suivi. La première a traité des avancées et enjeux liés à l'ordinateur quantique et aux capteurs quantiques. La seconde portait sur les communications quantiques et les méthodes de cryptographie post-quantique.

Présentation générale de la stratégie quantique française

Le coordinateur national de la stratégie quantique française, Neil Abroug, a commencé par présenter les enjeux et la structure de financement du plan quantique. Les 7 piliers de la stratégie quantique française sont :

- développer et diffuser l'usage des simulateurs et accélérateurs NISQ[1] [352 M€] ;
- développer l'ordinateur quantique passant à l'échelle LSQ[2] [432 M€] ;
- développer les technologies et applications des capteurs quantiques [258 M€] ;
- développer l'offre de cryptographie post-quantique [156 M€] ;
- développer les systèmes de communications quantiques [325 M€] ;
- développer une offre de technologies habilitantes[3] compétitive [292 M€] ;
- structurer transversalement l'écosystème.

Pour mettre ces chiffres en contexte, en 2018, l'Union Européenne avait prévu de consacrer un milliard d'euros sur 10 ans aux technologies quantiques, via un programme « *FET Flagship* »[4]. Les fonds proviennent du

[1] Noisy intermediate–scale quantum

[2] Large scale quantum

[3] Les technologies habilitantes ou capacitantes font référence aux technologies de pointe indispensables et pré-requises pour le développement des technologies quantiques. Par exemple la cryogénie, les lasers, l'ultra-vide, etc.

[4] FET : Technologies futures émergentes - http://www.horizon2020.gouv.fr/cid123504/1er-appel-du-fet-flagship-sur-les-technologiesquantiques.html

programme Horizon 2020 mais aussi de sources nationales.

Neil Abroug a rappelé qu'avant même la mise en place de ce plan national, des investissements publics, à hauteur d'environ 60 millions d'euros, existaient déjà et provenaient des organismes de recherche ou de l'Agence nationale de la recherche (ANR). Grâce à ces financements, la France se place au 6e rang des investisseurs mondiaux dans le domaine des technologies quantiques. Il faut donc voir la stratégie nationale comme un plan d'accélération avec trois enjeux majeurs identifiés : conquérir des parts du marché mondial dans les domaines du calcul, des capteurs, de la cryptographie et des technologies capacitantes ; développer des efforts de pédagogie et de communication pour créer un engouement sociétal ; encourager le rayonnement de la recherche et en faire « *le bras armé de la compétitivité des entreprises* ». Les pépites industrielles françaises sont, pour certaines, issues de la recherche académique et rivalisent déjà avec les géants américains tels que Google ou Intel. Il s'agit alors d'accélérer dans les domaines où la France possède déjà un avantage et peut tirer son épingle du jeu dans la concurrence mondiale.

Le plan inclut les technologies dites habilitantes dont l'industrie quantique a besoin et qui devraient assurer le premier retour sur investissement à court terme.

Le budget de la Stratégie quantique s'articule autour de plusieurs sources : Agence nationale de la recherche, Programme d'investissements d'avenir (PIA), Direction générale de l'armement (DGA).

L'ordinateur et les capteurs quantiques

- **L'ordinateur quantique : développement de qubits, passage à l'échelle et langage de programmation.**

Dans le cadre de la Stratégie quantique, 350 millions d'euros seront investis pour l'apprentissage et l'anticipation des futurs ordinateurs quantiques. Ils serviront à développer des simulateurs quantiques, des calculateurs NISQ et le premier ordinateur hybride doté de 100 qubits à l'horizon 2023 (via une coopération du CEA avec des centres situés en Allemagne, Italie, Irlande, Espagne et Autriche). Ils serviront aussi à former et recruter des développeurs.

400 millions d'euros supplémentaires sont fléchés vers le développement et le passage à l'échelle industrielle. Ils financeront la recherche publique et privée et les partenariats industriels avec Atos et Pasqal, pour développer le premier prototype complet d'ordinateur quantique LSQ.

Philippe Chomaz a rappelé que le principal verrou technologique à l'essor de l'ordinateur quantique reste la décohérence, ou l'incapacité de l'objet physique à demeurer dans son état quantique. Lever ce verrou permettrait d'exploiter pleinement les promesses des technologies quantiques mais le défi est immense. Le CEA explore actuellement deux voies : d'une part, il met à profit son expérience en microélectronique, notamment au centre LETI de Grenoble, pour chercher à intégrer un très grand nombre de qubits physiques permettant d'obtenir quelques qubits logiques fonctionnels ; cette perspective est un « *pari intéressant* », Philippe Chomaz ayant précisé que le record de transistors gravés sur une puce de silicium avoisine aujourd'hui 50 milliards. La seconde voie explorée vise à créer de nouveaux concepts de qubits robustes et intrinsèquement protégés d'un certain nombre de facteurs de décohérence ou capables de corriger leurs erreurs de manière autonome, sans redondance[5]. En parallèle de ces travaux, le CEA anticipe et prépare l'intégration de ressources de calcul quantique aux centres de calcul haute performance, notamment au centre de Bruyères-le-Châtel. L'ajout d'un processeur quantique, même peu avancé, peut aider sur un certain nombre d'applications et de calculs.

Une autre technologie de qubits, utilisant des photons, est développée par la société Quandela et a été présentée lors de l'audition par Pascale Senellart, confondatrice et conseillère scientifique. La *start-up* étant située sur le plateau de Saclay, un des trois centres régionaux dont la stratégie quantique souhaite le développement, Pascale Senellart a insisté sur l'enjeu de l'attractivité des centres de recherches régionaux ou *hubs*.

Sur le volet des ressources humaines, Pascale Senellart appelle à la vigilance sur la formation des cerveaux et des talents, dont les effectifs sont aujourd'hui majoritairement absorbés par les jeunes pousses et peinent à s'orienter vers la recherche fondamentale qui doit être soutenue pour devenir plus attractive. Georges-Olivier Reymond a cependant nuancé en rappelant que les jeunes pousses restent essentielles pour attirer des talents nationaux ou internationaux, mettre en valeur l'écosystème et faire grossir les parts de marché.

Sur ce dernier point, le PDG de Pasqal appelle à se souvenir que « *la première évolution quantique a été développée par des physiciens européens, mais le marché est essentiellement positionné aux États Unis. Pour la deuxième révolution, essayons d'en conserver un plus grand morceau !* »

Pasqal concurrence aujourd'hui les géants américains dans la course au prototype industriel et propose actuellement plus de qubits que Google par exemple. Avec un processeur à 200 qubits, il est en mesure de faire la démonstration de résolution de cas d'usage et de mettre en avant une plus-value du calcul quantique sur le calcul classique, même haute performance.

En complément de ce point de vue « jeunes pousses », le groupe Atos a pu donner sa vision du paysage quantique actuel et du rôle que les grands groupes peuvent avoir dans son développement.

[5] La technologie dite « des qubits de chat » constitue le cœur d'activité de la *start-up* française Alice & Bob et repose sur des travaux scientifiques de premier plan (Lescanne, R., Villiers, M., Peronnin, T. *et al.* Exponential suppression of bit-flips in a qubit encoded in an oscillator. *Nat. Phys.* 16, 509–513 (2020). https://doi.org/10.1038/s41567-020-0824-x

Leader européen dans les domaines du HPC (*high performance computing* – calcul haute performance) et de la cybersécurité, Atos a rapidement investi dans les technologies quantiques. Sa position consiste à se focaliser sur la partie dite « *software* » ou logiciel en utilisant du « *hardware* » ou des processeurs développés par d'autres, notamment Pasqal. Depuis 2017, son *Quantum learning machine* (QLM) simule dans le *cloud* le fonctionnement de quelques qubits et permet aux divers utilisateurs de tester les langages de programmation propres au quantique. Toutes ces avancées s'inscrivent dans une stratégie précise qui consiste à financer des activités de R&D – Atos est premier déposant européen de brevets sur le calcul quantique – et à entretenir des partenariats avec la recherche académique ou des jeunes pousses aux niveaux français ou européen.

Atos prépare aussi le calcul dit hybride qui consiste à ajouter un processeur quantique à des centres de calcul haute performance. À terme, et selon les cas d'usage, il sera intéressant de basculer entre différents modes de calcul selon les profils du problème à résoudre : processeur classique ou quantique, sur le même modèle des ordinateurs actuels qui utilisent des GPU[6] ou autres selon les usages.

De manière plus générale, au sujet des ordinateurs quantiques, il convient de rappeler que les annonces concernent toujours un nombre de qubits physiques et non-logiques et restent encore au stade de démonstrateur. Georges-Olivier Reymond prévient « *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.* »

Des cas d'usage ont été mis en avant, tels que des travaux de calcul en optimisation combinatoire pour EDF. Là où les calculateurs classiques montrent des faiblesses, une accélération quantique peut s'avérer bénéfique, notamment au-delà d'un seuil estimé à environ 1 000 qubits et pour des calculs à forte composante combinatoire.

▪ Les capteurs quantiques

La première table ronde s'est également intéressée au thème des capteurs quantiques avec les interventions de Thierry Debuisschert, de Thales, et de Jean Lautier-Gaud, de iXblue Quantum Sensors. Les capteurs quantiques reposent sur la sensibilité du système quantique à l'échelle du système unique (atome, ion, photon…). Concrètement, il s'agit d'effectuer des mesures de grande précision (champ électrique, magnétique, de gravité…) en manipulant des systèmes isolés presque individuellement. Les capteurs quantiques ont connu de nombreux développements depuis la première révolution quantique et les progrès techniques ont permis d'améliorer leur sensibilité et d'élargir la gamme d'applications potentielles. Dans le plan de stratégie quantique, 250 millions d'euros ont été fléchés vers le développement et l'intégration des capteurs, en leur ouvrant d'abord le marché de la défense puis en cherchant des marchés civils. Le rapport de Paula Forteza recommande de s'intéresser plus particulièrement aux capteurs à base d'impuretés (appelées centres NV) dans le diamant qui sont l'objet d'étude de Thierry Debuisschert.

Plusieurs étapes sont nécessaires à la fabrication d'un capteur diamant avec centres NV et la France possède sur son territoire tous les acteurs requis à la chaîne de fabrication. Elle possède ainsi tous les atouts pour se positionner au niveau mondial. Des partenariats européens viennent renforcer et compléter cette position.

Les propriétés remarquables des centres NV leur permettent de trouver une large gamme d'applications potentielles notamment en navigation, en communication mais aussi dans le domaine médical. Thierry Debuisschert estime que « *la progression [du marché des capteurs quantiques] sera de l'ordre de 1 milliard de dollars sur les 10 prochaines années* ».

Le degré de développement des capteurs quantiques a pu être apprécié par l'intervention de Jean Lautier-Gaud puisque le défi actuel de la société iXblue Quantum Sensors consiste à mettre au point un capteur commercial utilisable par des non-spécialistes, hors du laboratoire. Elle fournit des gravimètres mais aussi des horloges atomiques.

L'industrialisation de ces capteurs et leur utilisation par le grand public implique de les rendre plus fiables sur des temps longs, ainsi que les technologies habilitantes associées (laser, refroidissement…).

C'est pourquoi Jean Lautier-Gaud propose de renforcer l'écosystème français des technologies habilitantes. Il recommande aussi l'affichage direct des industriels dans les appels à projets PEPR. Enfin, il incite à regarder sur le long terme, au-delà du plan quantique et du programme *Flagship* européen afin de rendre les capteurs quantiques plus fiables et de répondre à des besoins spécifiques de potentiels clients.

Les questions des parlementaires à la fin de la première table ronde ont permis d'aborder différents points.

Tout d'abord, le rôle et l'investissement du monde de la défense, notamment dans le domaine des capteurs quantiques a été débattu. La DGA participe aujourd'hui à hauteur de 5 % au plan quantique, somme jugée insuffisante par le sénateur André Guiol. Neil Abroug a cependant rappelé que la DGA était soumise à la loi de programmation militaire (LPM) qui fige ses investissements sur le long terme. Le monde de la défense reste pleinement conscient des enjeux stratégiques liés aux technologies quantiques, notamment en ce qui concerne les capteurs et les menaces de la cryptographie post-quantique.

Neil Abroug a aussi rebondi sur les propos de Jean Lautier-Gaud en insistant sur la nécessité de trouver d'autres marchés pour les capteurs quantiques, au-delà des applications militaires, et d'en assurer la viabilité

[6] Graphics Processing Unit ou unité de traitement graphique, qui sert à optimiser le traitement et l'affichage d'images ou de vidéos sur ordinateur.

économique dans le monde civil. Il ne faut donc pas compter sur les seuls investissements de la DGA.

Le sénateur André Guiol a ensuite insisté sur la nécessité de ne pas se laisser distancer au niveau mondial et sur le risque de perte des compétences, comme ce fut le cas dans le passé pour les microprocesseurs. Développer la partie processeur (*hardware*) en France est crucial, d'autant plus que les compétences en programmation (*software*) ne pourront s'étendre sans support physique à disposition.

Les discussions ont enfin porté sur la place de la Chine dans la course mondiale aux technologies quantiques. Tous les intervenants ont confirmé sa place prépondérante, dotée de moyens exceptionnels et inégalables. Les capacités d'anticipation du gouvernement chinois lui ont permis de se placer en précurseur, par exemple sur les communications quantiques satellitaires : pendant que l'Europe et les États Unis hésitaient à inscrire un programme quantique au sein de leurs agences spatiales, la Chine lançait son premier satellite dédié à des communications quantiques en 2016.

Enfin, sur la question des cas d'usage et des problèmes sur lesquels le quantique pourrait présenter un avantage, il semble établi que chercher aujourd'hui à définir une liste de cas, en amont du développement des technologies, est inutile, voire contre-productif. Selon Pascale Senellart, *« 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 »*. Quelques exemples ont été évoqués tels que le calcul des permanents, la résolution d'équations différentielles pour la chimie, l'équation de Navier-Stokes, l'optimisation combinatoire avec des problèmes type « voyageur de commerce ». Les méthodes de calcul classiques atteignent leurs limites sur ces problèmes aujourd'hui, mais elles peuvent toujours s'améliorer. Au-delà des capacités techniques à résoudre un problème, la comparaison calcul quantique *versus* calcul classique repose aussi sur le possible gain énergétique, le HPC étant de plus en plus énergivore. À fidélité de calcul égale, il serait pertinent d'établir une comparaison précise entre les deux technologies lorsqu'un processeur quantique logique sera prêt, les résultats préliminaires montrant un réel avantage énergétique coté quantique.

Les communications quantiques et la cryptographie post-quantique

▪ Les projets de communications quantiques : des premiers tests à l'internet quantique européen de demain.

Depuis la publication des notes scientifiques de l'OPECST en 2019, les projets de communication quantique ont évolué et en sont aujourd'hui au stade de premier démonstrateur. Un des projets les plus aboutis, le réseau Quantum@UCA, se trouve en région Provence-Alpes-Côte d'Azur (PACA) et est développé conjointement par l'Université de Côte d'Azur (UCA) et Orange, sous le pilotage de Sebastien Tanzilli. Plus précisément, il s'agit d'un banc d'essai de réseau quantique opérationnel entre trois sites séparés de quelques dizaines de km. Les échanges de clés secrètes s'effectuent via un réseau de fibres optiques dépourvues de répéteurs classiques. Le débit de clés secrètes actuel atteint 10 millions de bits secrets par heure (un kilobit par seconde), avec un objectif à court terme d'atteindre le mégabit par seconde. Si ces travaux concernent pour le moment la mise en place d'un réseau de communication sécurisé au sol, les objectifs à plus long terme visent à articuler ce réseau avec un segment spatial, dont la source quantique serait embarquée à bord d'un satellite. Le premier marché des communications quantiques sera très probablement institutionnel, avec un niveau de fiabilité et de robustesse critique. Dans cette optique, les deux dimensions – spatiale et au sol - deviennent indispensables pour répondre à ces critères.

Pour mémoire, les équipes chinoises ont été précurseurs sur ce segment avec le lancement d'un satellite équipé d'une source quantique photonique dès 2016.

Le sursaut provoqué a amené les agences européennes à monter des projets similaires, avec notamment le projet EuroQCI, qui vise à poser les premiers éléments du futur internet quantique européen. Airbus étant acteur de ce consortium, Cédric Oudiette était présent pour présenter les principaux éléments liés à la dimension spatiale.

Le calendrier s'articule autour d'un démonstrateur prêt d'ici 2024, puis un système opérationnel avec échange de clés quantiques d'ici 2028. La dernière étape, un internet quantique inviolable et complet, est prévue pour 2035.

S'il reste quelques défis à relever, surtout en terme d'interopérabilité et d'interconnexion entre les différents réseaux locaux, Cédric Oudiette estime que la France possède toutes les ressources et compétences dans ses laboratoires et universités pour se positionner fortement et aboutir à une autonomie maximale. Il rappelle que *« le fait que l'État se positionne en utilisateur de ce système est un fort élément de crédibilité apporté aux futurs utilisateurs »*.

À terme, un internet quantique pourra aussi servir à mettre en réseau des processeurs ou des capteurs quantiques pour en décupler la puissance de manière totalement sécurisée, ce qui peut constituer une menace de premier plan sur les méthodes de cryptographie actuelles.

▪ La cryptographie post-quantique ou les protocoles de cryptographie à l'épreuve de l'ordinateur quantique.

L'ANSSI, autorité nationale en matière de cybersécurité, anticipe l'arrivée d'un ordinateur quantique qui pourrait compromettre les protocoles de cryptographie actuels.

Aujourd'hui, le chiffrement des données repose sur deux catégories d'algorithmes : les algorithmes symétriques, qui nécessitent un partage préalable de clés de sécurité et concernent principalement le chiffrement de communications, et les algorithmes asymétriques, qui échappent à cette nécessité et concernent les échanges de données sur de grands réseaux (chiffrement des cartes bancaires, etc.).

Selon les hypothèses, les capacités de calcul supposées d'un ordinateur quantique pourraient compromettre majoritairement les protocoles asymétriques mais relativement peu les protocoles symétriques.

S'il est encore difficile d'anticiper la date d'arrivée sur le marché d'un ordinateur quantique opérationnel et en capacité d'effectuer de telles opérations, l'ANSSI estime qu'il est plus prudent de travailler dès maintenant à la mise au point et l'adoption de nouveaux protocoles post-quantiques ou résistants à l'ordinateur quantique. Cela permettra aussi d'empêcher des attaques dites rétroactives qui visent à enregistrer les données maintenant pour les décrypter plus tard, quand la technologie sera à disposition.

Un certain nombre de problèmes mathématiques ont été certifiés résistants au calcul quantique et forment les nouvelles méthodes de cryptographie post-quantique. Cela comprend, par exemple, les fonctions de hachage, les réseaux euclidiens, les isogénies de courbes elliptiques, etc. Cette résistance dépend cependant d'un certain nombre d'hypothèses sur les compétences présumées des ordinateurs quantiques. Il conviendra d'actualiser ces hypothèses au fur et à mesure des développements technologiques à venir, notamment si les travaux de mise en réseau d'ordinateurs quantiques aboutissent.

Au niveau national, l'ANSSI recommande de déployer, à court terme (sous 1 à 4 ans) des solutions dites hybrides qui ajoutent une surcouche de protection post-quantique aux méthodes de cryptographie classiques actuelles. Cette solution permet de protéger les données des attaques classiques, de mettre à l'épreuve des méthodes post-quantiques et surtout d'éviter toute régression de sécurité. Elle concerne principalement les données demandant une protection de longue durée, au-delà de 2035.

L'ANSSI se prononce plutôt en défaveur des méthodes de communication quantique. Les contraintes liées au déploiement et à l'utilisation de nœuds de répétition constituent, pour elle, des failles de sécurité importantes. Leur emploi n'est envisagé qu'en complément de méthodes de cryptographie.

Au niveau international, le bureau des standards américain, le *National Institute of Standards and Technology* (NIST), est chargé de sélectionner le prochain standard de cryptographie post-quantique, après un appel à candidatures qui a fortement mobilisé la communauté internationale. La France est très bien représentée dans cet appel à projets, notamment dans les dernières phases de sélection qui se déroulent actuellement (5 finalistes sur 7 sont français).

Les spécialistes de la cryptographie post-quantique et des méthodes mathématiques de chiffrement appellent à porter une attention toute particulière aux deux phases indispensables à la protection des données : d'une part la confidentialité (les données restent secrètes), d'autre part l'authentification (la certitude pour le destinataire de communiquer avec le bon expéditeur). Les communications quantiques ne permettent pas d'assurer la partie authentification et selon Damien Stehlé « *le mot inviolable [...] semble totalement inapproprié [...]. Tant que ce problème ne sera pas résolu, la confidentialité complète de la création de clés est inutile dans un cas d'usage général* ». Thierry Debuisschert a rappelé l'existence de travaux qui visent à combler cette faille en combinant des méthodes de sécurité quantique à des fonctions de hachage pour garantir l'authentification.

Il semble indispensable de faire travailler les différentes communautés ensemble pour combler cette faille de sécurité et garantir une authentification et une confidentialité des moyens de communication destinés à un potentiel usage institutionnel. L'ajout d'une brique post-quantique à des lignes de communication quantique semble nécessaire et doit être anticipée dès aujourd'hui.

Recommandations

L'audition publique du 21 octobre 2021 a permis de faire le point sur la mise en place de la Stratégie quantique française quelques mois après les annonces du Président de la République. Les avancées scientifiques et technologiques présentées ont confirmé la place importante de la France dans la course mondiale ainsi que les défis qu'il reste à relever.

La Stratégie nationale a bien identifié les enjeux des technologies quantiques et les axes sur lesquels les efforts doivent être portés ; elle est associée à des moyens financiers substantiels qui rendent crédible l'atteinte des objectifs qu'elle s'est fixés. Une vigilance devra être maintenue sur la formation et l'attractivité, notamment pour les acteurs de la recherche fondamentale.

Les recommandations de l'Office, dont certaines ont été émises par les parties prenantes, visent à renforcer le rôle de la France dans un domaine hautement stratégique et à faciliter la diffusion des technologies quantiques dans les usages présents ou futurs. Elles s'adressent tant aux pouvoirs publics qu'aux acteurs académiques et industriels concernés, tant l'imbrication des enjeux reste forte au stade actuel de développement de ces technologies.

Elles s'articulent autour de trois objectifs :

Maintenir une veille scientifique et technologique sur l'émergence de ces technologies et les évolutions qui accompagneront leur développement:

- les capteurs quantiques sont encore largement financés par le monde de la Défense. Il convient d'en développer les usages et les marchés civils, afin d'assurer la viabilité économique de ce secteur sur le long terme ;
- les algorithmes de cryptographie post-quantique actuellement étudiés reposent sur des hypothèses de fonctionnement et de performance d'un futur ordinateur quantique. Ces hypothèses doivent faire l'objet d'une veille rigoureuse afin d'anticiper de potentielles failles ou difficultés en matière de sécurité.

Anticiper l'arrivée – même lointaine - des ordinateurs quantiques et leurs potentiels atouts :

- la maîtrise des processeurs quantiques (conception, développement et fabrication) est essentielle pour garantir les souverainetés française et européenne dans de nombreux domaines. Il faut donc conforter les efforts des acteurs impliqués dans ces activités. Cela assurera aussi un environnement propice à la communauté qui travaille sur la programmation et les développements de logiciels associés, et permettra de conserver un avantage dans les deux domaines, matériel et logiciel ;
- les centres de calcul HPC consomment de plus en plus d'énergie. Les processeurs quantiques actuels présentent un avantage en termes de consommation d'énergie mais restent imparfaits. À terme, lors d'un éventuel passage à l'échelle et de la mise au point d'une technologie LSQ, il conviendra de prendre en compte de potentiels gains énergétiques dans les comparaisons de performance entre processeurs classiques et processeurs quantiques.

Favoriser la création d'écosystèmes vertueux et dynamiques :

- l'écosystème scientifique et industriel des technologies quantiques ne peut croître que si des talents en nombre suffisant procurent à la fois à la recherche académique, aux *start-up* et aux grands groupes les forces vives dont ils ont besoin. Il est donc indispensable de faire émerger ces talents par une politique de formation dynamique appuyée sur des financements spécifiques ;
- la sécurité d'une communication électronique repose à la fois sur la confidentialité des données échangées et sur l'authentification des intervenants connectés. Les communications quantiques offrent intrinsèquement de fortes garanties en matière de confidentialité mais n'ont pas d'avantage comparatif vis-à-vis des technologies classiques en matière d'authentification. Pour mettre au point des systèmes de communication offrant les meilleurs garanties d'inviolabilité, il est indispensable de faire travailler de concert les communautés de la cryptographie quantique et de la cryptographie post-quantique.

Pour consulter le rapport :
www.senat.fr/opecst
www.assemblee-nationale.fr/commissions/opecst-index.asp

Assemblée nationale - 101 rue de l'Université - 75355 Paris 07 SP – Tél : 01 40 63 26 81 – Mél : secretariat-opecst@assemblee-nationale.fr
Sénat - 15 rue de Vaugirard - 75291 Paris Cedex 06 – Tél : 01 42 34 25 58 – Mél : opecst-secretariat@senat.fr