Opinions Libres
Le blog d'Olivier Ezratty
innovation, startups, médias numériques, marketing, & ...

Comprendre l'informatique quantique – stratégies industrielles

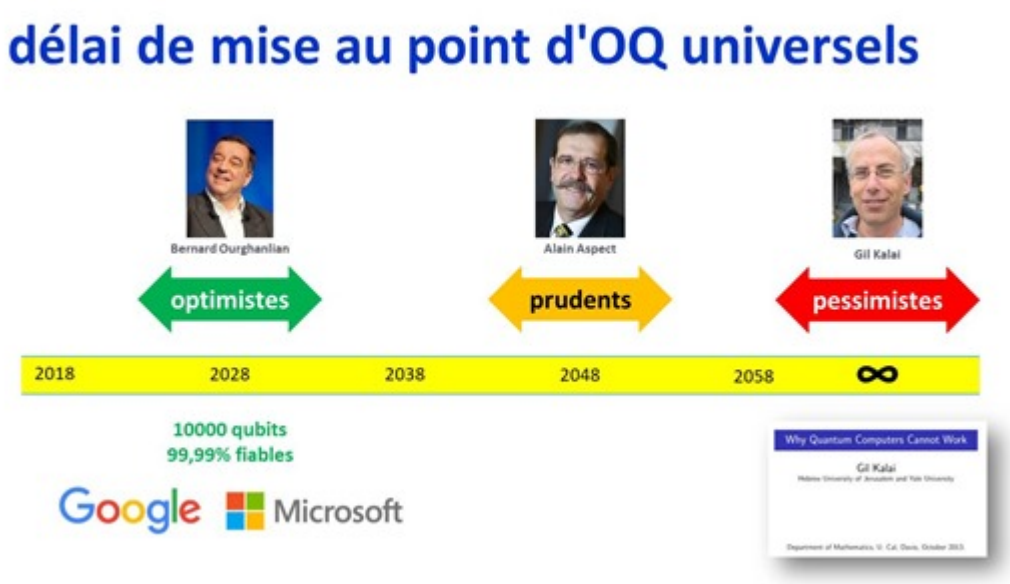
Cette 16e partie de la longue série pour comprendre l'informatique quantique **démarrée en juin 2018** est dédiée aux stratégies industrielles et aux activités par pays.

L'informatique quantique au sens large du terme est un secteur technologique stratégique à différents titres. Dans la cryptographie, il en va de la souveraineté avec l'enjeu de la protection des communications sensibles. Le calcul quantique est pour sa part porteur d'applications critiques qui vont étendre le champ du numérique au-delà de ce qui est faisable aujourd'hui, notamment dans le domaine de la santé, de l'environnement et de l'intelligence artificielle, prise dans une définition large.

En termes de maturité, la **cryptographie quantique et post-quantique** sont des champs plus établis avec des acteurs économiques et des solutions, même si la standardisation de la cryptographie post-quantique n'est pas achevée. Elle comporte cependant peu d'inconnues scientifiques fondamentales.

Le calcul quantique est moins mature. Si l'incertitude scientifique semble en partie levée pour ce qui est de la faisabilité des ordinateurs quantiques exploitables commercialement, les obstacles technologiques restent encore importants à surmonter pour y arriver, notamment l'épineuse question du **bruit dans les qubits et de la correction d'erreurs quantiques**.

Les avis sont partagés sur la vitesse de la levée de ces incertitudes : elle va de quelques années pour certains comme chez Google ou Microsoft, à quelques décennies pour des scientifiques comme Alain Aspect, pour atteindre le "jamais" pour des chercheurs tels que l'Israélien Gil Kalai.



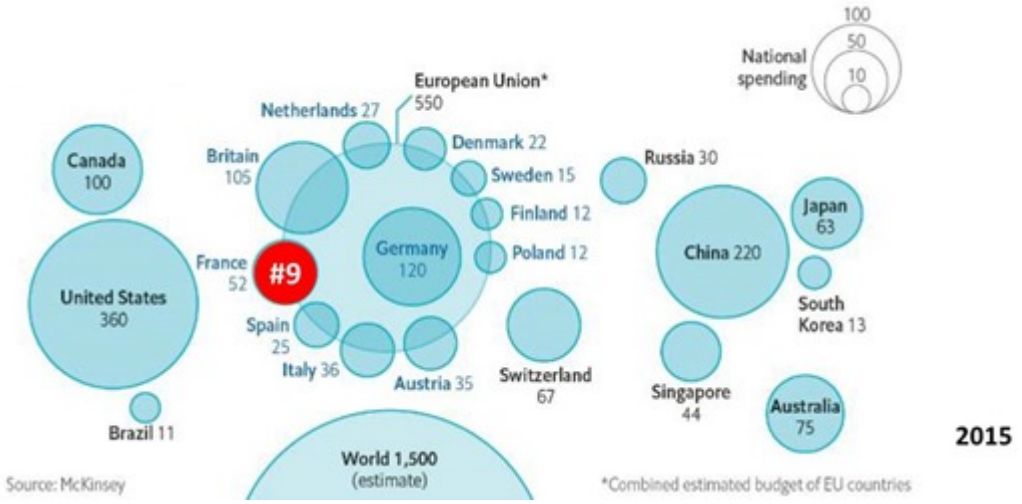
C'est donc un domaine à cheval entre l'incertitude scientifique et l'incertitude technologique. La recherche est pour l'instant issue essentiellement du secteur public dans les grands pays qui s'y investissent, puis de très grands acteurs du numérique qui ont de quoi faire plein de paris technologiques en parallèle (Google, Intel, Microsoft, IBM, Alibaba) puis de quelques startups plus ou moins bien financées ou avancées, essentiellement en Amérique du Nord (D-Wave, IonQ, Rigetti).

L'industrie des logiciels destinés aux ordinateurs quantiques est balbutiante. La majeure partie des "pure players" de ce secteur sont dédiés aux ordinateurs quantiques adiabatiques du Canadien D-Wave, tels que QxBranch et 1QBit qui sont respectivement Américains et Canadiens. Les grands acteurs et startups qui planchent sur les calculateurs quantiques ont tous investi dans le logiciel, à commencer par les outils de développement d'algorithmes et d'applications quantiques. Chacun ambitionne évidemment de créer des plateformes logicielles leaders. Certaines sont déjà disponibles dans le cloud, comme chez IBM. D'autres, tels le Français Atos et Microsoft proposent l'accès via le cloud à des simulateurs quantiques à base d'ordinateurs traditionnels.

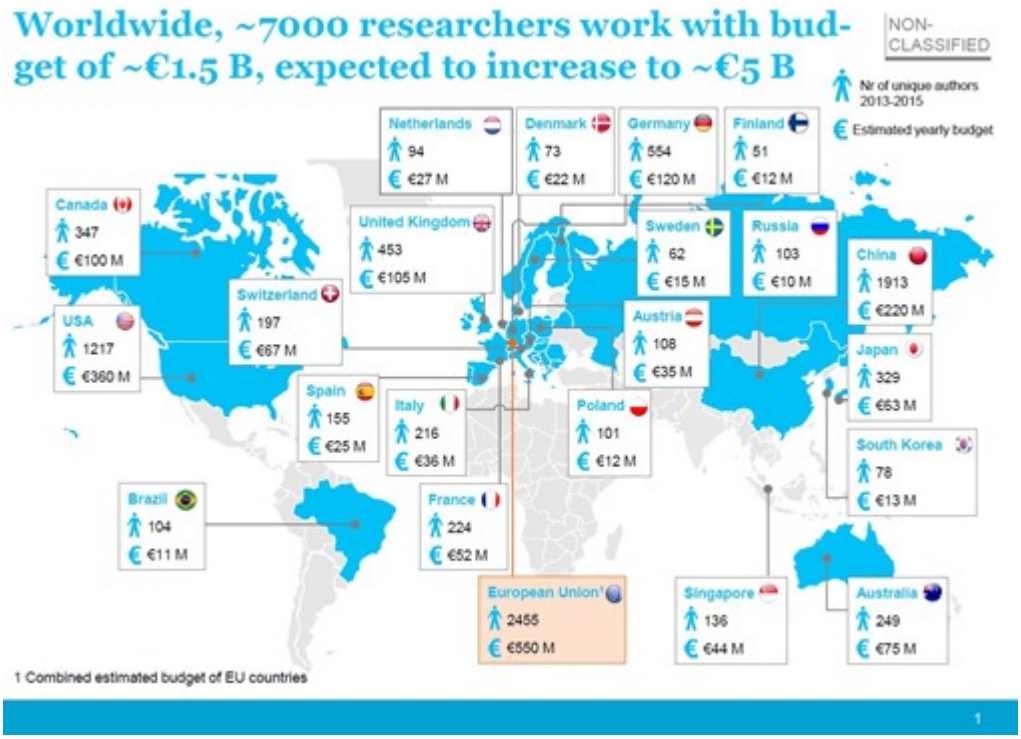
Les investissements mondiaux dans l'informatique quantique

Qu'en est-il des investissements mondiaux dans l'informatique quantique ? Une **étude de McKinsey de 2015** faisait un tour d'horizon des investissements qui compilaient sans doute des budgets de recherche publique. Il y avait alors 1500 chercheurs dans le monde dotés d'un budget total de $1,5B. Même si ce nombre dû augmenter depuis, il est très faible. Nous en sommes en 2018 à l'état où l'informatique traditionnelle en était en 1955 !

Les USA et la Chine y figuraient évidemment en tête. Mais la répartition de ces investissements, qui intègrent probablement aussi bien la cryptographie quantique que les calculateurs quantiques est intrigante pour les autres pays. La France y était en neuvième position, derrière l'Allemagne, le Royaume Uni, le Canada, le Japon la Suisse et l'Australie. Sachant que ces données ont dû évoluer depuis, avec, notamment, un accroissement significatif de l'effort de la recherche de la Chine.

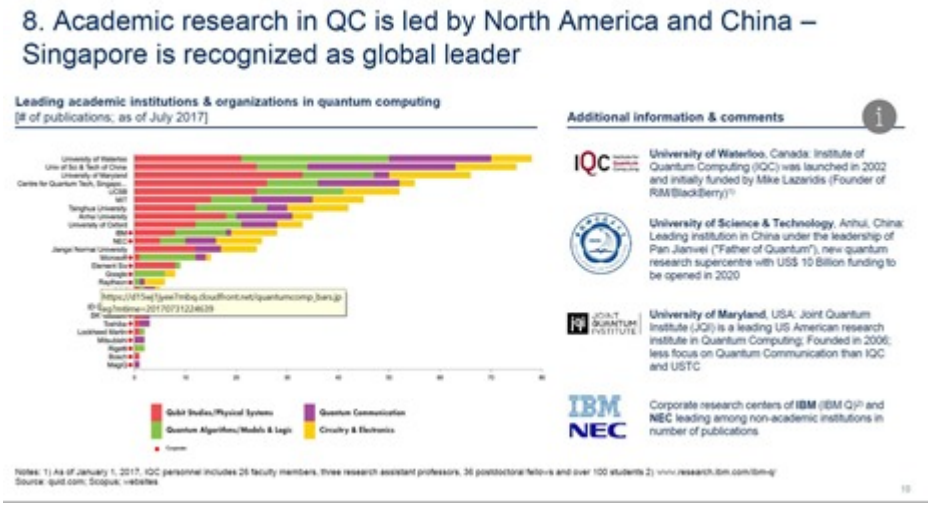


Une étude européenne produite en 2016 reprenait les mêmes chiffres en y ajoutant les effectifs. Avec donc 224 chercheurs en France à comparer à 1217 chercheurs aux USA, ce qui est un ratio tout à fait normal de 1 à 6.



Les pouvoirs publics de ces différents pays se sont mobilisés de manière très différenciée sur le quantique. La plupart des pays développés se sont mobilisés au niveau de leurs pouvoir publics pour coordonner les efforts dans le quantique. Un pays fait curieusement défaut dans ce panorama : la France. Nous verrons ce qu'il en est plus loin.

Une évaluation des publications scientifiques dans l'informatique quantique est présentée cette intéressante étude **VC investment analysis Quantum Computing**, produite par des étudiants de l'Insead en 2018 (18 slides). On y découvre sans surprise que les USA, le Canada et la Chine sont les premiers pays à publier. C'est l'effet de la masse. Mais la première Université est celle de Waterloo au Canada. Ce dernier pays est un véritable pionnier dans l'informatique quantique, et pas seulement grâce à D-Wave.



De son côté, l'**IDA**, l'Institute for Defense Analyses, une organisation parapublique US qui gère trois fonds d'investissements financés par l'état fédéral, a publié **Assessment of the Future Economic Impact of Quantum Information Science** en 2017 (133 pages). Ils y font un bon tour d'horizon des domaines d'applications du quantique, y compris dans le petit marché de la métrologie quantique.

On y trouve cet intéressant tableau qui classifie les principaux pays par dépense, publications scientifiques et dépôts de brevets, les données datant de 2016. La France y arrive en 8e à 10e position selon les indicateurs. C'est un classement habituel. On a cependant plusieurs pays dont le PIB est inférieur à celui de la France qui arrivent devant elle : le Canada et l'Australie ! Et la Corée du Sud est devant la France en termes de dépôt de brevets, ce qui n'est pas une grande surprise au vu de la force de son industrie électronique, dominée par Samsung qui représente près du cinquième du PIB du pays. Une bonne partie de l'inventaire des projets financés par les

gouvernements de nombreux pays cités dans cet article proviennent de ce document de l'IDA.

Table 5. World Ranking of Countries in Quantum Science and Technology

Country	World ranking based on spending	World ranking based on scientific publications	World ranking based on patent applications	Total world ranking
United States	1	2	1	1
China	2	1	2	2
Germany	3	3	6	3
United Kingdom	4	4	4	3
Japan	8	5	3	5
Canada	5	6	5	5
Australia	6	11	7	7
France	9	8	10	8
Italy	11	9	12	9
South Korea	17	10	8	10

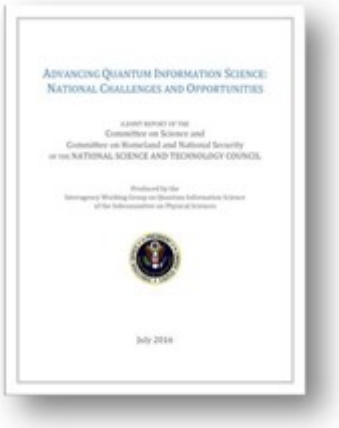
Source: U.K. Government Office for Science (2016).

La recherche dans le quantique est-elle juste une affaire de gros sous ? Pas seulement. Il ne suffit pas d'aligner des milliards de dollars pour résoudre les problèmes de la matière condensée des qubits supraconducteurs. La réussite dans le quantique est aussi une question d'intégration de disciplines scientifiques nombreuses, puis de valorisation industrielle.

Passons à une revue de détail pays par pays, continent par continent.

Aux **USA**, la mobilisation apparente des pouvoirs publics est plus molle ou discrète, même si elle dépasse celle de l'Europe en quantité, ne serait-ce que du fait des investissements des grands acteurs du privé dans la recherche fondamentale ou de ceux de la NSA, qui sont probablement massifs, mais confidentiels.

La coordination de la recherche dans les différentes branches du quantique a démarré en octobre 2014. A l'époque où l'on s'intéressait aux sciences à la Maison Blanche, avec un véritable conseiller scientifique du Président, John Holdren qui a traversé les deux mandats de Barack Obama, celle-ci avait produit le rapport **Advancing Quantum Information Science : National Challenges and Opportunities** (juillet 2016, 23 pages) suivie d'une **réunion de travail** en octobre de la même année. Le remplaçant de John Holdren vient d'être tout juste nommé par Donald Trump après 18 mois de Présidence, un certain Kelvin Droegemeier, un météorologiste qui a même obtenu l'aval de son prédécesseur ce qui est plutôt rare dans cette Administration.



Ce n'était pas un plan mais plutôt un inventaire de l'existant. Comme presque tous les pays, le découpage du quantique y est réalisé en quatre parties : la communication quantique, la métrologie quantique, le calcul quantique et les simulateurs quantiques, la distinction entre ces deux derniers étant subtile.

L'état fédéral finance des projets de recherche de startups avec des financements issus du programme SBIR, l'une des composantes du fameux Small Business Act. Cela concerne notamment **Axion Technologies** qui a créé un générateur de nombres aléatoires concurrent de ceux du Suisse IDQ.

Les laboratoires publics qui investissent l'informatique quantique traversent à peu près tout le complexe militaro-industriel fédéral avec de la recherche interne ou de la recherche externe subventionnée sur appels à projets :

- La **DARPA** finance trois programmes dans le quantique, dans les communications quantiques à longue distance, dans la métrologie quantique appliquée à l'imagerie ainsi que dans le diagnostic de traumatismes neurologiques et le PTSD. Les financements vont à des projets menés par des Universités, startups et entreprises établies.

- L'**IARPA** (Intelligence Advanced Research Projects Agency) que nous avons déjà eu l'occasion de citer plusieurs fois finance des projets tiers sur les calculateurs et les algorithmes quantiques, notamment dans l'entrainement de réseaux de neurones, dans le test de circuits. Leur programme LogiQ vise à améliorer la qualité des qubits. L'IARPA finance également des programmes conduits par des entités tierces.

- La **NSA** investit beaucoup dans le quantique à la fois dans la course à la mise en œuvre de l'algorithme de Shor pour décrypter les communications protégées par clés publiques de type RSA et pour protéger les communications sensibles avec clés et cryptographie quantiques. Ses travaux ne sont évidemment pas publics. La NSA sous-traite également une partie de sa recherche à des entreprises privées telles que Lockheed-Martin.

- L'**US Air Force** et son Quantum Communications qui est focalisé sur la cryptographie quantique (QKD). Un autre laboratoire fait de la recherche appliquée dans les qubits supraconducteurs et étudie l'application des algorithmes quantiques à ses besoins opérationnels.

- L'**Office of Naval Research** (ONR) travaille sur les usages des QKD pour la marine et sur l'exploitation d'algorithmes quantiques liés aux besoins opérationnels de la marine.

- L'**Army Research Office** a aussi son propre programme de recherche dans le quantique couvrant tout le spectre allant de la métrologie au calcul quantique en passant par la cryptographie et les communications quantiques.

- La **NASA** a créé en 2013 le Quantum Artificial Intelligence Laboratory (QuAIL) conjointement avec Google au Ames Research Center à proximité du siège de ce dernier à Mountain Views pour explorer le champ des algorithmes quantiques, en particulier sur un ordinateur quantique adiabatique de D-Wave qu'ils ont installé à cette époque là.

- Le **Los Alamos National Laboratory** (LANL) a un Quantum Institute (QI) lancé en 2002 qui investi aussi dans l'informatique et la cryptographie quantique. Ils financent notamment des recherches de l'UNSW en Australie ainsi que dans celle du Maryland. Ce laboratoire est financé par le Département de l'Energie (DoE). Ce dernier finance également le **Sandia National Laboratories** qui conduit aussi de la recherche appliquée tout azimut dans le quantique.

- La **NSF** finance des projets de recherche divers, un peu comme l'ANR en France. A noter deux initiatives de recherche collaborative aux USA : la **National Photonics Initiative** lancée en 2013 et la proposition d'une **National Quantum Initiative** évoquée en 2017 avec un financement fédéral demandé par les scientifiques de $500M sur cinq ans.

En 2018, la communauté scientifique US s'inquiétait toutefois d'un risque de perte de leadership des USA sur le sujet comme le soulignait cette **note de l'Ambassade de France aux USA** d'avril 2018. Vis à vis de l'Europe ? Non ! De la Chine qui investit massivement dans le quantique.

La Chambre des Représentants US a même organisé autour de ce sujet une audition en octobre 2017 (**vidéo**). Durant trois heures, on y voit des élus interroger une brochette de scientifiques dont James Kurose de la NSF et John Stephen Binkley du Département de l'Energie, qui leur expliquent les basiques des qubits et les enjeux de souveraineté associés. Les élus démocrates s'y inquiétèrent des coupes budgétaires proposées par l'administration Trump dans le financement de la recherche civile, au profit d'augmentations du budget de la défense et de réductions d'impôts.

In fine, le Congrès US a au contraire solidement augmenté les budgets de la recherche fédérale sur l'année fiscale 2018 (**source**), sachant que ceux-ci sont ensuite fléchés pour l'essentiel vers des organismes privés, notamment les laboratoires des grandes universités américaines. Avec +8,3% pour le NIH (santé), +3,9% pour la NSF (recherche généraliste), +15% pour la recherche au DoE (énergie), +,7,9% pour les programmes scientifiques de la NASA et +26% pour le NIST qui gère les standards et travaille notamment sur la cryptographie quantique. C'est un des rares cas où le Congrès contrôlé par les Républicains s'est opposé à l'administration Trump.

La commission des sciences de la Chambre des Représentant introduisait le 26 juin 2018 le **National Quantum Initiative Act** (**H.R. 6227**) qui ambitionne de sédimenter les objectifs, les responsabilités et les moyens publics autour du quantique. Une **proposition équivalente** était déposée au Sénat le même jour.

Ce projet de loi propose de mobiliser $1,275B sur cinq ans pour financer la R&D civile dans le quantique, répartis au Département de l'Energie ($625M), à la NSF ($250M) et au NIST qui est focalisé sur les questions de cryptographie ($400M). Lorsque l'on fait les comptes, cela ferait passer les investissements annuels de $200M à $255M, ce qui semble modeste, mais ce dernier montant n'intègre pas les fonds alloués à la NSA et au Département de la Défense.

Ce National Quantum Initiative Act propose la création d'un National Quantum Coordination Office au sein de l'Office of Science and Technology Policy qui a maintenant son nouveau dirigeant en place. Il demande au Président des USA de créer un plan à 10 ans sur le quantique, avec une première étape devant être un plan de 5 ans livrables un an après le vote de la loi.

Ce projet n'est évidemment pas tombé du ciel. Il résulte d'une proposition, le **National Quantum Initiative—Action Plan**, préparée par des intervenants de la recherche publique et du privé (IBM, Google, Rigetti). Elle comprend d'ailleurs une promesse un peu délirante sur le calcul quantique, qui permettrait un jour de trier des bases de données trop grandes pour être stockées dans des ordinateurs conventionnels. Une erreur magistrale quand on sait que les qubits n'ont pas les capacités de stockage d'information qu'on leur prête comme je l'avais **expliqué ici** et **là** ! On confond toujours abusivement la notion de superposition d'états des qubits avec une supposée capacité de stockage d'information.

En fait, ce projet de loi a été poussé par les élus car ils craignent que la Chine prenne le dessus sur le quantique, notamment dans la sécurité informatique. Les USA aiment se faire peur. Mais dans le domaine du quantique, ils n'ont pas à rougir : ils ont une densité de laboratoires de recherche publics et privés sans égal, leurs grands acteurs ont une capacité d'industrialisation à grande échelle que quasiment aucun pays ne peut concurrencer et leur marché intérieur reste le plus grand au monde pour les applications informatiques d'entreprise, là par où le quantique va démarrer.

Il faut préciser cependant que le projet de loi de la Chambre des Représentants et du Sénat doit être voté par les deux chambres puis ratifié par le Président. Je souhaite tout le courage à celui ou ceux qui auront le plaisir d'expliquer le quantique à Donald Trump ! Ils y arriveront sans doute, démontrant par là le fait que l'on peut comprendre les enjeux du quantique sans pour autant saisir les raffinements de la physique quantique !

On peut faire un parallèle entre l'intelligence artificielle et l'informatique quantique pour ce qui concerne ce pays. Dans les deux cas, son influence du secteur est bien plus grande que le poids économique du pays, aussi bien au niveau de la recherche fondamentale que des entreprises.

Le Canada se distingue par un fort investissement dans la recherche fondamentale dans l'informatique quantique, notamment à l'**Université de Waterloo**, proche de Toronto et celle de **Sherbrooke**, près de Montréal ainsi que dans son tissu entrepreneurial, avec en tête de pont, le fameux **D-Wave** ainsi que le spécialiste des logiciels quantiques, **1QBit**. L'Université de Waterloo a obtenu en 2017 un budget de $120M pour ses différents instituts de recherche dans le quantique. Etonnamment, elle a aussi obtenu un financement australien de $53M provenant de l'UNSW, de l'opérateur Telstra et de la Commonwealth Bank of Australia.

IQC Institute for Quantum Computing

Les financements privés notables comprennent surtout les donations de Michael Lazaridis, un des cofondateurs de RIM BlackBerry, avec $75M à l'**Institute for Quantum Computing** de l'Université de Waterloo et $128M en 1999 au **Perimeter Institute for Theoretical Physics** qui est aussi situé à Waterloo. Avec Doug Fregin, également cofondateur de RIM, ils ont également créé le Quantum Valley Investment Fund avec un financement total de $100M.

L'IQC fait à la fois de la recherche et de l'enseignement. Ils proposent notamment des formations courtes de une à deux semaines en été sur la crypto et le calcul quantiques.

L'**Australie** est un pays qui s'investit aussi dans le quantique à différents niveaux. Le plan **National Innovation and Science Agenda** annoncé en 2015 comprend 24 initiatives et $820M de financement sur 4 ans dont $19M sont alloués au Center for Quantum Computation and Communication Technology (CQCCT) sur 5 ans dans l'informatique quantique. Le pays est aussi prolixe en projets partenariaux public-privé et associant l'Australie à d'autres pays.

L'UNSW (Université de Nouvelle Galle), la Commonwealth Bank of Australia et l'opérateur télécom Telstra financent à hauteur de de $52M les efforts de création d'un processeur quantique CMOS. On pourrait espérer qu'Orange fasse la même chose en France avec le CEA et/ou une startup !

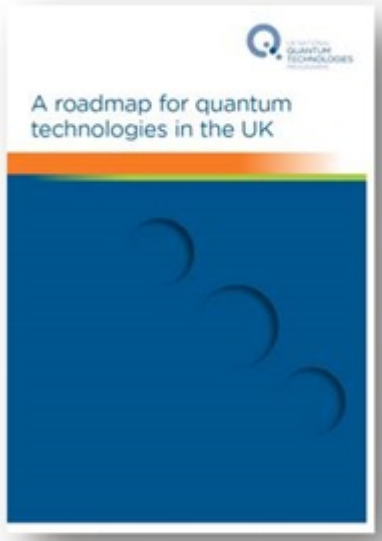
UNSW SYDNEY

Côté partenariats internationaux, le pays est associé avec l'Université de Singapour pour la création de satellites de télécommunication quantique. L'Université de Sydney fait partie d'un consortium international intégré dans le programme **LogiQ** de l'IARPA US. Enfin, l'UNSW est partenaire du CEA-LETI dans la recherche appliquée de qubits CMOS. Le partenariat entre le CEA et l'UNSW a été signé en mai 2018 en présence d'Emmanuel Macron et du Premier Ministre australien Malcolm Turnbull. Ce partenariat associe aussi la société **Silicon Quantum Computing** (SQC) issue de l'UNSW, créée par **Michelle Simmons**, et dont les actionnaires comprennent le gouvernement australien ainsi que l'opérateur Telstra. Il porte sur le développement de technologies quantiques CMOS. Il associe aussi Andrew Dzurak, un physicien de l'UNSW spécialisé dans les CMOS quantiques.

Du côté entrepreneurial, on compte trois startups australiennes dans le domaine du quantique avec **QuintessenceLabs** (clés optiques QKD), **QxBranch** (logiciels et conseil) et **Silicon Quantum Computing** (qubits CMOS) que nous venions de citer.

C'est le **Royaume-Uni** qui semble s'être mobilisé le premier en Europe, et ce, dès 2013 avec le plan **The UK National Quantum Technologies Programme Current and Future Opportunities** de Derek Gillespie (**version print**), de l'Engineering and Physical Sciences Research Council (EPSRC), un organisme non gouvernemental financé par les derniers publics et sous la supervision de l'exécutif. C'est une sorte d'équivalent britannique de notre Agence Nationale de la Recherche et qui finance des projets de recherche. Le plan UK vise tous les marchés habituels du quantique : métrologie, calcul, sécurité et imagerie médicale.

Son **rapport d'étape de 2015** montre que l'approche est assez symbolique avec des montants publics investis assez modestes, de l'ordre de 100M€ étalés sur plusieurs années et sur plusieurs hubs d'innovation. Mais le timing est plutôt bon ! Le plan initial prévoyait d'investir £270M sur 5 ans avec un objectif de valoriser les travaux de recherche dans de startups aussi rapidement que possible. Le gouvernement anglais se préoccupe surtout du transfert de technologies des laboratoires vers les entreprises.



Le plan UK prévoit la création d'un réseau de hubs d'innovation dans le quantique, avec les thématiques habituelles : métrologie (avec les Universités de Birmingham, Glasgow, Nottingham, Southampton, Strathclyde et Sussex), les télécommunications quantiques et le calcul quantique. Il se distinguait avec un effort préemptif dans la formation avec notamment celle de doctorants financée à hauteur de $210 sur deux ans.

Côté recherche, de nombreux laboratoires sont impliqués dans le quantique, notamment à **Oxford** (avec le hub NQIT, sur le calcul et la sécurité et l'initiative **QuOpaL** – Quantum Optimisation and Machine Learning financée par Nokia et Lockheed Martin), **Cambridge** (Centre for Quantum Information and Foundations, qui planche sur la partie physique comme mathématique du quantique), **Glasgow** (avec le hub Quantic, spécialisé dans l'imagerie), **York** (avec un hub sur la communication quantique, donc sur des QKD) et **Bristol** (Quantum Engineering Centre for Doctoral Training, focalisé sur la formation ainsi que sur la photonique).

Du côté entrepreneurial, on peut citer **Oxford Instruments** (cryogénie), **Oxford Quantum Circuits** (qubits supraconducteurs), **Quantum Motion Technologies** (qubits CMOS), **Cambridge Quantum Computing** (système d'exploitation, logiciels, services), **TundraSystems** (qubits photoniques) et **River Lane Research** (logiciels). Aucune grande entreprise UK ne semble y être particulièrement investie dans l'informatique quantique.

La **Suisse** est aussi mobilisée sur le quantique, notamment à l'**Université ETH** de Zurich qui collabore d'ailleurs avec IBM et surtout autour de la cryptographie quantique, notamment avec sa startup **IDQ** qui est leader de la génération de nombres aléatoires utilisée dans la crypto quantique.

Le pays a publié un manifeste de promotion de ses efforts de recherche et industriels dans le

quantique, **Switzerland: At the Quantum Crossroads**.

L'initiative **Quantum Science and Technology** (QIST) commune à l'ETH Zurich et l'Université de Bâle et qui associe aussi l'Université de Genève et l'EPFL de Lausanne comprend 34 enseignanst et 300 étudiants. Elle a été financée à hauteur de $120M entre 2010 et 2017. Elle couvre tous les domaines habituels du quantique avec, semble-t-il, un effort plus particulier dans les télécommunications quantiques.

En **Allemagne**, l'agence fédérale qui protège les systèmes d'information homologue de l'ANSSI française a publié en mai 2018 le rapport **Entwicklungsstand Quantencomputer** (*état des lieux de l'informatique quantique*) qui fait un point sur l'informatique quantique, focalisé notamment sur les questions de cybersécurité (231 pages, en anglais). Cet excellent document a été créé par une demi-douzaine d'universitaires allemands faisant de la recherche à l'Université de Saarland à Sarrebruck et à l'Université de Floride à Boca Raton aux USA. Ce sont des physiciens spécialistes de la matière condensée et des qubits supraconducteurs, des mathématiciens et des spécialistes de la cybersécurité.

C'est l'un des meilleurs tours d'horizon de la recherche mondial en informatique quantique que j'ai pu consulter. Il fait un inventaire étonnamment précis des efforts dans le domaine, notamment dans la recherche publique US. Il met d'ailleurs en évidence que la recherche en Allemagne n'est pas bien active sur l'informatique quantique avec seulement deux laboratoires de recherche impliqués, le **Max Planck-Institute for Quantum Optics** (MPQ) et l'**Institut für Quanteninformation** d'Aix La Chapelle. Comme le CEA français, ce dernier fait de la recherche au niveau de la physique dans les qubits supraconducteurs et en silicium quantum-dots. Le MPI est quant à lui engagé dans une voie plus originale avec des qubits à base d'atomes neutres.

Par contre, l'Allemagne est assez pauvre du côté entrepreneurial. Je n'y ai identifié que deux startups dans le quantique : **InfiniQuant** (cryptographie CV-QKD) et **PicoQuant** (compteurs de photons) et rien dans le calcul quantique, une situation voisine de celle de la France.

Les **Pays-Bas** sont aussi actifs dans le quantique, principalement autour de l'Université de Delft (**TU Delft**). Le gouvernement lançait en 2015 un plan de création d'ordinateur quantique étalé

sur 10 ans et doté de 135M€. L'investissement était fait dans **QuTech**, le centre de recherche quantique de TU Delft dont le budget sur 10 ans est de 145M€. Cf le **rapport d'activité 2017** de QuTech. Qutech occupe plus de 180 personnes en tout dont 37% de Hollandais.

QuTech est aussi associé à **Intel** et **Microsoft**. QuTech a reçu un financement de $50M en 2015 d'Intel dans le cadre d'un partenariat sur leurs qubits supraconducteurs. Microsoft est aussi partenaire de QuTech, ce depuis 2010, qu'ils ont d'ailleurs déplumé en embauchant Leo Kouwenhoven dans leur laboratoire de Microsoft Research qui est sur place et planche sur le quantique topologique et le fermion de Majorana en liaison avec une équipe de QuTech dédiée au même sujet.

On peut dire que les Pays-Bas se positionnent donc pour l'instant comme réservoir à cerveaux pour l'industrie quantique américaine. Dans la pratique, c'est à cela que mènent leurs investissements dans la recherche.

Les approches de recherche collaborative vont bon train, notamment dans l'optique de récupérer des financements européens. En octobre 2017, QuTech lançait un partenariat avec l'Institute of Photonic Sciences, l'Université d'Innsbruck en Autriche et le Paris Centre for Quantum Computer. QuTech est aussi partenaire de l'Université d'Aix la Chapelle dans le qubit CMOS.

D'autres initiatives aux contours flous ont été lancées comme **Quantum Helix**, qui ambitionne d'être financée dans le cadre du programme flagship quantique européen et Horizon 2020. Un autre programme dénommé **Quantum Software Consortium** devant durer 10 ans à partir de 2017 a reçu 18,8M€ de financements publics du pays dans le cadre du Gravitation Program. Il associe divers laboratoires hollandais : **TU Delft**, **QuTech** (qui fait partie de cette dernière), **QuSoft** (laboratoire de recherche dédié aux logiciels quantiques, lancé par CWI, UvA et VU en 2015), **CWI** (*Centrum Wiskunde & Informatica*, l'équivalent hollandais de l'INRIA français), l'**Université de Leiden**, **UvA** (Université d'Amsterdam) et **VU** (Université libre d'Amsterdam) pour mener de la recherche en logiciels quantiques et en cryptographie.

Sinon, côté entreprises, j'ai juste identifié une startup, **Delft Circuits**, spécialisée dans la fabrication de circuits supraconducteurs.

L'investissement de l'**Autriche** dans l'informatique quantique est concentrée dans l'**IQOQI**, l'Institut für Quantenoptik und Quanteninformation d'Innsbruck et Vienne. Il se focalise en particulier dans la conception de qubits à base d'ions piégés. En est issue la startup **Alpine Quantum Technologies**, créée par Rainer Blatt de l'IQOQI, pour commercialiser des ordinateurs quantiques à ions piégés. Elle a bénéficié de financements publics à hauteur de 12,3M€. Elle concurrence la startup américaine **IonQ** issue de l'Université de Maryland qui est positionnée sur le même créneau des qubits à ions piégés.

L'Autriche est aussi investie dans la cryptographie quantique et associée avec la Chine, avec qui elle a mené des expériences d'envoi de clés quantiques par le satellite Micius pour mettre en place une communication vidéo sécurisée. L'**IQOQI** collabore aussi avec le **Centre Spatial**

Universitaire de Grenoble (CSUG) dans la mise au point d'un satellite de relai de clés quantiques de type CubeSat, similaire à celui de Singapour, dans le projet **Nanobob** (**présentation**, 13 slides).

La recherche dans le quantique au **Danemark** est organisée autour du Center for Quantum Devices (**QDev**) de l'Institut Niels Bohr de l'Université de Copenhague. C'est un laboratoire de qualité focalisé notamment sur les qubits topologiques, avec son dirigeant Charles M. Marcus qui travaille aussi pour Microsoft Research dans cette filière conjointement avec les équipes de MSR de Leo Kouwenhoven aux Pays-Bas. QDev est un laboratoire de physiciens focalisé sur l'étude de la matière condensée, à savoir les couches basses physiques des qubits, comme on peut l'observer dans **leurs publications**.

L'équipe semble ne faire qu'une dizaine de personnes. Ils ne peuvent malheureusement pas s'appuyer ensuite sur des industriels danois ou européens pour envisager le transfert de leur recherche dans la production d'ordinateurs quantiques. C'est un problème français mais aussi européen !

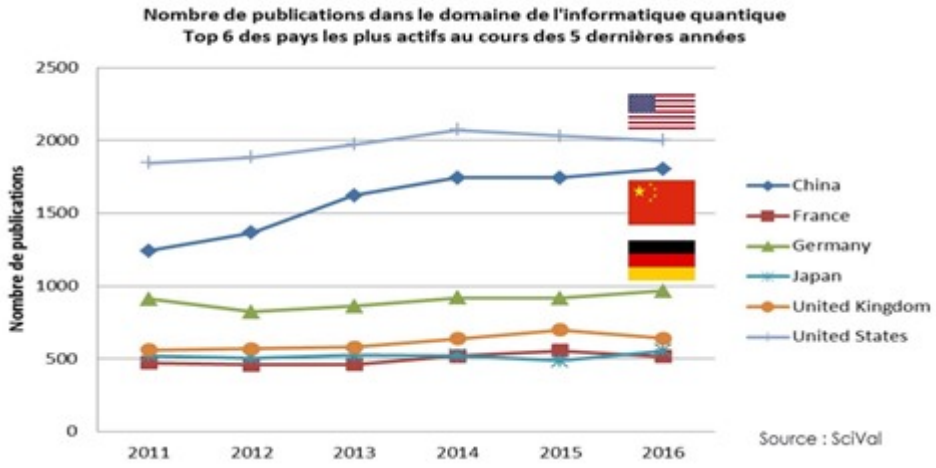
Le quantique est un domaine où l'**Union Européenne** se mobilise collectivement. Initié en 2016, un "flagship project" qui regroupe les entités citées ci-dessus a germé en 2016 et était formellement lancé en 2018 pour financer de la recherche collaborative sur l'ensemble des pans de l'information quantique : métrologie, communications, calcul et simulation quantiques.

Il est doté *en théorie* de 1,2 Md€ servant aux programmes de développement et de diffusion des

technologies quantiques, étalés sur 10 ans. En théorie car les budgets n'ont pas été véritablement alloués à ce niveau par l'Union Européenne. Ils le seront dans le meilleur des cas par tranches étalées dans le temps. Le flagship est surtout focalisé sur les couches physiques fondamentales de l'informatique quantique. Il est dommage qu'il ne prenne pas aussi bien en compte la dimension algorithmique et logicielle de l'informatique quantique qui est un domaine où l'Europe pourrait se distinguer.

L'approche européenne est de manière traditionnelle focalisée sur le financement de programmes de recherche collaborative avec les lourdeurs administratives que cela génère. Dans le même temps, de nombreux industriels américains collaborent avec les laboratoires européens. Microsoft a recruté à l'Université de Delft des spécialistes du quantique, notamment dans les qubits topologiques. Intel a aussi chassé à Delft. Et IBM a une partie de ses équipes dans le quantique qui sont basées dans son laboratoire de recherche de Zurich, près de l'ETH Zurich qui abrite pas mal de spécialistes du quantique. Bref, nous avons ici la reproduction d'un scénario assez classique avec une excellence de recherche européenne qui se transforme en produits via les grands acteurs américains. Ceci dit, les grands acteurs américains exploitent aussi abondamment la recherche fondamentale issue de leur propre pays. Ainsi, Google et IBM collaborent-ils avec l'Université de Santa Barbara en Californie. Le poids relatif de l'apport des laboratoires de recherche US vis à vis des laboratoires européens aux acteurs américains dépend des acteurs. Il semble plus faible pour Microsoft que pour Google et IBM.

La note de l'ambassade de France met en évidence un point notable : l'**Allemagne** arriverait en troisième position mondiale en termes de publications scientifiques dans le secteur de l'informatique quantique, après les USA et la Chine et devant le Royaume Uni et le Japon. Cela ne se traduit visiblement pas en un écosystème entrepreneurial sur le domaine ni par une action particulière des grands acteurs du numérique du pays, sauf peut-être avec **Infineon**, la spin-off de semiconducteurs de Siemens qui s'intéresse à la cryptographie quantique. Ce syndrome est voisin en France avec une recherche assez active sur le sujet mais un côté plutôt atone du secteur privé, à l'exception notable d'Atos.



C'est lié au traditionnel différentiel entre recherche et entreprises. L'absence de grands acteurs du numérique en Europe à même de prendre le relai de la recherche est pénalisante. Qui plus est, le tissu de startups n'est pas assez bien financé et ne peut donc pas miser sur le long terme comme le fonds les homologues d'Amérique du Nord. D-Wave a été lancé en 1999 a produit son premier qubit en 2007, huit ans après et a commercialisé ses premiers ordinateurs quantiques vers 2012, donc 13 ans après sa création. Soit bien plus que la durée de vie moyenne d'un fonds d'investissement (à ne pas confondre avec celle des sociétés de gestion) !

L'Europe est par ailleurs assez active dans l'organisation de conférences scientifiques sur l'informatique quantique. Avec quelques exemples : la conférence **QIP** en janvier 2018 à l'Université de Delft aux Pays-Bas suivie de la conférence **Quantum Europe** 2018 des 17 et 18 mai 2018, également aux Pays-Bas. D'autres **conférences de 2018** sur l'informatique quantique ont eu lieu ou vont avoir lieu en Suisse, au Portugal, en Espagne, en France, en Allemagne, en Autriche et même en Grèce. Parfois, la présence d'intervenants français y est négligeable, comme à **Quantum Simulation & Computation** de Bilbao en février 2018.

Dans le benchmark mondial, la France se distingue d'une manière encore plus radicale que dans l'intelligence artificielle. Nous avons une recherche de qualité mais pas assez de transformation de sa production en richesse entrepreneuriale. Les stars françaises de la physique quantique sont Alain Aspect et Serge Haroche, le premier ayant invalidé les inégalités de Bell en 1982 et vérifié le principe de non localité de quantum intriqués, un élément clé servant notamment à la cryptographie quantique. Prix Nobel de physiques en 2012, Serge Haroche est spécialisé dans l'optique linéaire. Il continue de plancher sur la création de qubits à base de photons. Ancien collègue d'Alain Aspect, Philipe Grangier est un spécialiste mondial de la cryptographie quantique. Bref, comme d'habitude, les cerveaux brillants ne manquent pas. Outre-Atlantique, Michel Devoret est le "Yann LeCun" du quantique, à savoir qu'il travaille maintenant à l'Université de Yale aux USA (vs l'Université de New York) et dans la startup qu'il a cofondée aux USA, QCI. Mais nuance, il n'est pas (encore) dans un GAFA !

Nombre de laboratoires de recherche planchent sur les différentes briques du quantique, que ce

soit au CEA, au CNRS ou à l'INRIA, et dans plein de régions, notamment à Toulouse, Montpellier, Bordeaux (LaBRI) et Grenoble, en plus de l'Ile de France. Au **CEA**, l'**équipe Quantronics** de Daniel Estève de Saclay planche sur les qubits supraconducteurs. La laboratoire de Daniel Estève comprend une quinzaine de personnes. Son homologue à l'Université de Yale aux USA en comprend une trentaine. Selon lui, il ne suffit pas d'aligner en parallèle plus de chercheurs pour accélérer la recherche dans ce domaine !

L'équipe de Maud Vinet au **CEA-LETI** de Grenoble est à l'origine de la technologie FD-SOI utilisée par STMicroelectronics pour produire des composants électroniques à basse consommation. Elle cherche à créer des qubits en technologie CMOS. L'équipe de Maud Vinet a fédéré les efforts de plusieurs laboratoires du CEA et du CNRS dans l'initiative **Quantum Silicon Grenoble**, un groupe pluridisciplinaire travaillant sur les qubits CMOS (équipe *ci-dessous*, photo du CEA). Comme vu dans le chapitre sur l'Australie, le CEA a lancé en 2018 un partenariat avec l'UNSW australienne et la startup Silicon Quantum Computing (SQC) pour créer des processeurs quantiques CMOS. Le CEA et Quantum Silicon Grenoble apportent un double atout : une équipe chevronnée de physiciens qui complètent celles des Australiens et un outil industriel que les Australiens n'ont pas avec la plateforme de production de wafers expérimentaux du CEA-LETI à Grenoble.

Les efforts de l'**INRIA** sont concentrés dans l'équipe Quantic de Maziar Mirrahimi qui travaille aussi sur la mise au point de qubits supraconducteurs.

Le **SIRTEQ** (Science et Ingénierie en Région Ile de France pour les Technologies Quantiques) est focalisé de son côté sur la recherche en technologies de communications quantiques.

On note aussi parmi diverses équipes projets, celle de l'Initiative de Projet Stratégique **IQUPS** (Ingénierie Quantique à l'Université Paris-Saclay) qui est répartie sur plusieurs sites de l'Université Paris-Saclay aussi bien côté Palaiseau/X que côté Orsay. Elle regroupe une dizaine d'UMR (Unités mixtes de recherche) associant notamment le CNRS, le CEA, l'Institut Mines Télécom, l'Ecole Polytechnique.

Le **CNRS** a regroupé informellement ses efforts avec le **groupe de travail Informatique Quantique** qui travaille plutôt sur la dimension algorithmique. Il y a aussi un groupe **Paris Center for Quantum Computing** (PCQC) qui associe 22 chercheurs franciliens issus de divers laboratoires, dont Philippe Grangier. Comme nous l'avons déjà vu, le **Centre Spatial Universitaire de Grenoble** collabore depuis 2017 avec l'**IQOQI** autrichien sur l'envoi de clés

quantiques par satellite dans le projet Nanobob.

Enfin, l'**ANR** a clôt en février 2018 un **appel à projets de recherche**, lancé dans le cadre d'un partenariat de recherche avec le Japon (CREST). Et il existe une autre collaboration internationale sur le quantique associant la France, les Pays-Bas (QuSoft) et la Lettonie.

Du côté des entreprises, il n'y a pas foule. Nous avons quelques acteurs des couches basses physiques comme **Muquans** et ses outils de métrologie quantique, **CryoConcept** et ses systèmes de cryogénie et **Quandela** avec ses sources de photons.

Seul **Atos** sort du lot. Leur stratégie lancée en 2016 consiste à se préparer à devenir un acteur du cloud dans le calcul quantique en prenant le problème "par le haut", par le logiciel. Ils développent donc des compétences dans les algorithmes et la programmation de calculateurs quantiques, notamment avec le langage aQasm qui peut fonctionner sur tout ordinateur quantique présent ou futur.

Pour tenir le coup avant que celui-ci ne voit le jour, ils ont développé un simulateur quantique sur serveurs à base Intel, le **Atos Quantum Learning Machine**. Des supercalculateurs dont Bull s'est fait une spécialité. Lancé en septembre 2017, le simulateur aQML a été notamment adopté par le centre de recherches américain d'Oak Ridge du Département de l'Energie, qui teste de nombreux types de supercalculateurs. Il est aussi installé au CEA, à l'Université de Reims et depuis juillet 2018, dans le département de recherche en cybersécurité de l'Université de Sciences Appliquées de Haute-Autriche à Hagenberg.

Atos est en contacts avec divers laboratoires de recherche dont le CEA de Saclay et l'équipe de Daniel Estève qui travaille sur les qubits supraconducteurs. En mai 2018, Atos et le CEA lançaient aussi une chaire industrielle sur l'informatique quantique, cofinancée par l'ANR. Dirigée par Daniel Estève, elle est baptisée **Nasniq** pour "Nouvelle architecture de spins nucléaires pour l'information quantique". Donc, avec un axe portée sur un type spécifique de qubit. Par contre, l'annonce de cette chaire évoque des recherches pour faire "*face à l'explosion des données entraînée par le Big Data et l'Internet des Objets*". Pourquoi pas, mais l'informatique quantique ne semble pas vraiment adaptée à court et à moyen terme à l'exploitation de très gros volumes de données. On est dans la complexité algorithmique plutôt que dans le traitement de gros volumes de données, tout du moins compte-tenu de l'état de l'art des algorithmes et architectures quantiques.

Le français conduit par Thierry Breton **ambitionne** de construire à terme un ordinateur quantique une fois la technologie mise au point. Mais il n'est pas évident qu'ils se dotent

suffisamment rapidement de la capacité à concevoir et fabriquer de bout en bout des ordinateurs quantiques complets. Il est plus probable qu'ils se fournissent à terme auprès des constructeurs leaders qui seront probablement Américains si ce n'est Chinois. Atos s'intéresse aussi à la cryptographie post-quantique, un sujet que nous évoquerons dans une partie séparée de cette série.

L'enjeu principal pour Atos est de pousser ses outils de développement auprès d'un maximum de développeurs, décrits dans la **partie idoine de cette série**. Pour ce faire, il serait bon qu'ils en proposent rapidement l'utilisation via une offre ouverte en cloud exploitant leur machine aQML, comme le font IBM, Google, Microsoft, Rigetti et même D-Wave, avec un simulateur quantique classique (IBM, Google, Microsoft) ou avec un ordinateur quantique de leur cru (IBM, Rigetti, D-Wave). La bataille des plateformes et des écosystèmes a déjà démarré !

Atos s'est doté d'un conseil scientifique de compétition avec Cédric Villani, Alain Aspect, Serge Haroche, Daniel Estève, David DiVicenzo (IBM) et Artur Ekert (inventeur des clés quantiques QKD). C'est un très beau panel. Malheureusement entièrement masculin.

En juillet 2018, Atos faisait sinon l'acquisition de Syntel pour $3,4B aux USA, un prestataire de services spécialisé dans le développement et le déploiement d'applications dans le cloud faisant $923M de CA avec 22 500 collaborateurs créé en 1980 par des Indo-Américains. Cela ne semble pas avoir de rapport avec le quantique.

Parmi les grands comptes français ayant publiquement annoncé s'intéresser à l'informatique quantique, on peut citer **Airbus** qui, depuis 2015, et Seaport dans le Pays de Galles, étudie diverses domaines d'applications aussi bien côté cryptographie que côté calcul quantiques. Les banques sont aussi intéressées, au moins sur la partie crypto quantique ! Du côté des startups, j'ai pour l'instant identifié l'intérêt de **Prevision.io** pour l'intégration d'algorithmes quantiques dans son offre d'automatisation de recherche d'algorithmes de machine learning dans le cloud. D'autres suivront sans doutes, mais prudemment.

Terminons ce tour du continent européen avec la **Russie**. Elle n'est pas très visible dans la bataille industrielle qui se prépare autour de l'informatique quantique. Cependant, s'est créé en 2012 le **Russian Quantum Center**, un centre de recherche dédié aux différents domaines d'applications de l'informatique quantique, cryptographie quantique comprise comme il se doit. Il occuperait en tout environ 200 chercheurs. Ses travaux couvrent de nombreuses branches de l'informatique quantique : les supraconducteurs, la photonique et les cavités de diamants. Ils travaillent aussi dans le domaine de la métrologie quantique. Ils collaborent avec de nombreux organismes de recherche internationaux aux USA (MIT), Canada (Université de Calgary), Allemagne (Max Planck Institute for Quantum Optics), UK (Université de Bath), etc. Ces informations proviennent de **Evaluation Report of Russian Quantum Center**, 2017 (7 pages).

Il ne serait pas étonnant que l'on voit émerger de tout cela au moins quelques startups dans la cryptographie quantique, ne serait-ce que pour des raisons de souveraineté pour ce pays qui tient

à sa position dans le monde, face à la Chine, aux USA autant que face à l'Europe.

Passons à l'Asie en démarrant avec le **Japon**. Une note de l'ambassade de France au Japon de fin 2017 faisant le point de l'**informatique quantique au Japon** (27 pages) illustrait un investissement de long terme du pays dans l'exploration de l'informatique quantique, dans la lignée de leurs efforts dans les supercalculateurs, pilotés notamment par **Fujitsu**. C'est une approche qui n'est pas sans rappeler celle de la France avec Atos. A noter que le fonds d'investissements de Softbank abondé par de l'agent de la famille Saoud et doté de $100B doit aussi investir tout azimut dans le quantique (**source**).

Le pays lançait la création des **National Institutes for Quantum and Radiological Science and Technology** (QST) en avril 2016 dotés de $487M de budget annuel. Ce montant impressionnant n'est pas dédié à l'informatique quantique. Il semble qu'il le soit bien plus au vaste secteur de la métrologie quantique et en particulier dans celui de l'imagerie médicale.

En 2017, le **NICT** (National Institute of Information and Communication Technologies) réalisait une démonstration de télécommunication quantique exploitant un microsatellite. Cela ressemble à l'expérience chinoise avec le satellite Micius réalisée la même année. En juillet 2017, le NICT (National Institute of Information and Communication Technologies) a réalisé une démonstration de communication quantique à l'aide d'un microsatellite qui constitue une première mondiale.

Le **JFLI** est un laboratoire franco-japonais basé à Tokyo créé en 2009 et qui associe des chercheurs des Universités de Tokyo, de Keio et du National Institute of Informatics avec ceux du CNRS, de l'UPMC (Pierre et Marie Curie), de l'INRIA et de l'Université Paris-Sud. Ils travaillent de concert avec l'équipe de Michelle Simmons Center à Sydney en Australie (comme le CEA-LETI à Grenoble) ainsi qu'avec l'**IQOQI** autrichien. Cette équipe pluridisciplinaire va de la physique fondamentale à l'algorithmique et étudie la faisabilité du calcul quantique à grande échelle tout comme la cryptographie quantique.

Dans le privé, les grands groupes industriels japonais sont surtout focalisés sur les télécommunications et la cryptographie quantiques, un peu comme en Chine et en Corée du Sud. C'est le cas de **Toshiba Corporation** qui s'est lancé dans la cryptographie quantique dès 2003. Ils travaillent dessus avec le Quantum Information Group (QIG) à l'Université de Cambridge, UK. Ils ont réalisé une première démonstration de communication quantique en 2014, en envoyant 878 gbits de données sécurisées sur une fibre de 45 km entre deux zones de la région de Tokyo

sur une durée cumulée de 34 jours, à raison de 300 kbits/s. Ils poursuivaient les expérience en 2016 et avec British Telecom au Royaume-Uni.

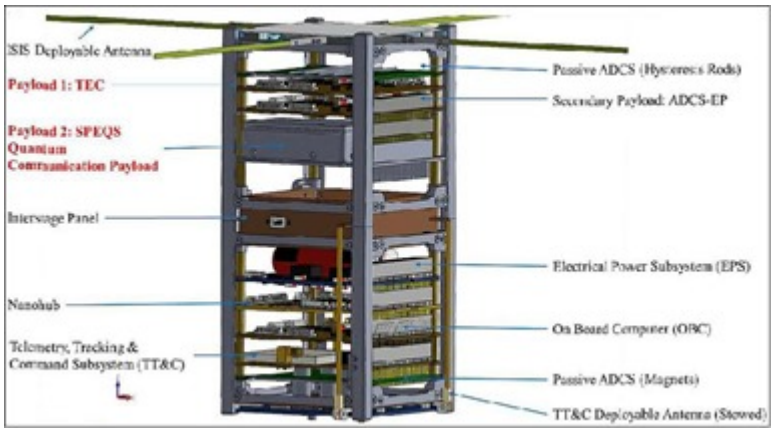
Hitachi a aussi un laboratoire de recherche situé à l'Université de Cambridge qui planche sur les clés quantiques, l'informatique quantique et la création de composants SQUID pour qubits supraconducteurs. **NEC** est aussi versé dans les clés quantiques (QKD).

NTT entretient quatre laboratoires de recherche appliquée dans le quantique, focalisés dans les télécommunications et la cryptographie quantiques. Ils travaillent aussi dans la filière des qubits CMOS à quantum dots. Le tout avec une quarantaine de chercheurs. En novembre 2017, ils annonçaient mettre au point **QNNcloud**, un ordinateur quantique utilisant l'optique linéaire (photons) mis en service dans le cloud pour simuler des réseaux de neurones avec un boucle optique alimentée par des impulsions laser (**vidéo**). Le procédé qui ne s'appuie pas sur la notion de qubits est décrit dans **Universal Quantum Computing with Measurement-Induced Continuous-Variable**, 2017 (5 pages). Il serait très peu consommateur d'énergie, de l'ordre de 1 KW/h. C'est en fait plutôt un concurrent de D-Wave. QNNcloud est un projet financé dans le cadre du programme d'innovation ImPACT et en partenariat avec le National Institute of Informatics (NII), l'Université de Stanford, celles de Tokyo, Osaka et Tohoku. Le projet avait démarré en 2011.

En **Corée du Sud,** l'opérateur télécom **SK Telecom** investit dans les télécommunications quantiques. Ils sont partenaires de la Florida Atlantic University. Ils ont aussi investi en 2016 dans la startup suisse ID Quantique. Ils sont partenaires depuis 2017 avec Nokia dans le domaine des QKD tout comme avec Deutsche Telekom avec qui ils ont établi une "Quantum Alliance" pour créer des télécommunications sécurisées. De son côté, **Samsung** investi aussi dans les QKD et la cryptographie quantiques.

Le petit état de **Singapour** est connu pour son dynamisme économique et entrepreneurial. Au sein de l'Université de Singapour, la recherche dans le quantique est assurée depuis 2007 dans le **Center for Quantum Technologies** (CQT) avec un financement d'environ $15M annuels. Il est comme c'est souvent le cas investi à la fois dans le calcul quantique et la cryptographie

quantique. Côté partenariats, Singapour est notamment associé à la Chine voisine.



Singapour a lancé en 2015 son nano-satellite Galassia-2U, créé par le CQT et servant à expérimenter des communications quantiques cryptées via QKD. Galassia est intégré dans un format CubeSat à deux unités (deux cubes l'un sur l'autre, cf *ci-dessus*). Il ne fait que 3,4 Kg au total. Il a été lancé avec 5 autres satellites dont le satellite de télécommunications TeLEOS-1 (400 kg) fin 2015 par un **lanceur indien**. La durée de vie de ce genre de satellite est de 6 mois. Voir **Quantum Tech demos on CubeSat nanosatellites** (41 slides). Ces expériences ont mené, visiblement, à la création de la startup **S-Fifteen Space Systems**. Mais, il reste à trouver des solutions pour que ces satellites durent plus longtemps sur leur orbite basse et ne contribuent pas encore plus à poubelliser l'espace autour de la Terre.

Auparavant, le CQT avait eu l'occasion de tester involontairement l'envoi d'un satellite (ComX-2) dans une fusée ayant explosé en 2014 après le décollage. Non sans humour, ils explique que ComX-2 n'a pas survécu à l'expérience dans **Extreme Environmental Testing of a Rugged Correlated Photon Source**, 2015 (2 pages). Mais ils ont récupéré un ComX-2 après un autre lancement raté.

Comme dans pas mal de secteurs technologiques, la **Chine** affirme haut et fort ses ambitions et sa puissance dans le secteur du quantique. Elle s'est aussi lancée dans des efforts tout azimut, touchant la cryptographie, les télécommunications, la simulation et le calcul quantiques.

De même qu'au Royaume-Uni, cet investissement a été pris en main assez tôt par l'exécutif et dès 2013 avec l'implication de Xi Jinping, le président Chinois, lors d'une visite du laboratoire d'Anhui, portant surtout sur la cryptographie quantique, associée à une session de formation. Dès 2015, Xi Jinping intégrait la communication quantique dans les priorités scientifiques du pays. L'informatique quantique était intégrée de son côté dans les priorités du 13ième plan couvrant la période 2016-2020. Une roadmap quantique de la Chine datant de 2016 est disponible dans "Quantum Leap: The Strategic Implications of Quantum Technologies de Elsa Kania" et John Costello (**part 1** and **part 2**). Voir aussi **Chinese QC Funding** de Xiaobo Zhu, 2017 (35 slides). Les montants investis dans le quantique étaient respectivement de $160M dans le 11e plan couvrant la période 2006-2010, de $800M dans le 12e plan couvrant 2011-2016 et de $320M

dans le 13e plan démarrant en 2016, complétés par $640M de financement des régions. Le financement total de la recherche publique en quantique depuis 2006 se monte donc à près de $2B.

Depuis, le projet le plus ambitieux est l'annonce d'un centre de recherche "à 10 milliards de dollars" qui doit ouvrir en 2020, le **National Laboratory for Quantum Information Sciences**, situé à Hefei, à près de 500 km à l'ouest de Shanghaï (maquette *ci-dessous*). Le montant est à prendre des pincettes car, même sur 10 ans, un Centre de Recherche aussi grand soit-il ne couterait pas cette somme là. Ce laboratoire sera focalisé sur l'informatique et la métrologie quantiques, aussi bien pour des applications militaires que civiles.

Jusqu'à présent, l'entité la plus active dans l'informatique semblait être l'**University of Science and Technology of China** (USTC) de l'Académie des Sciences Chinoises (CAS). Elle annonçait avoir préparé et mesuré l'état de 600 paires de qubits intriqués en 2016 (**source**) puis avoir développé des portes quantiques avec un faible taux d'erreurs. Il est difficile d'évaluer l'intérêt d'avoir 600 paires de qubits si ceux-ci ne sont pas reliés entre eux. En 2017, ce même laboratoire annonçait la réalisation d'un système de test de 10 qubits supraconducteurs intriqués en aluminium et saphire (**source**). Le taux d'erreurs serait élevé, à 0,9% pour les portes à deux qubits. Le leadership de ce laboratoire semble assuré par un certain **Jian-Wei Pan**. Son équipe prévoit de créer un ordinateur quantique universel à base de 50 qubits d'ici 2023 ! Et il pense qu'il faudra attendre 30 à 50 ans pour qu'un ordinateur quantique universel voit le jour.

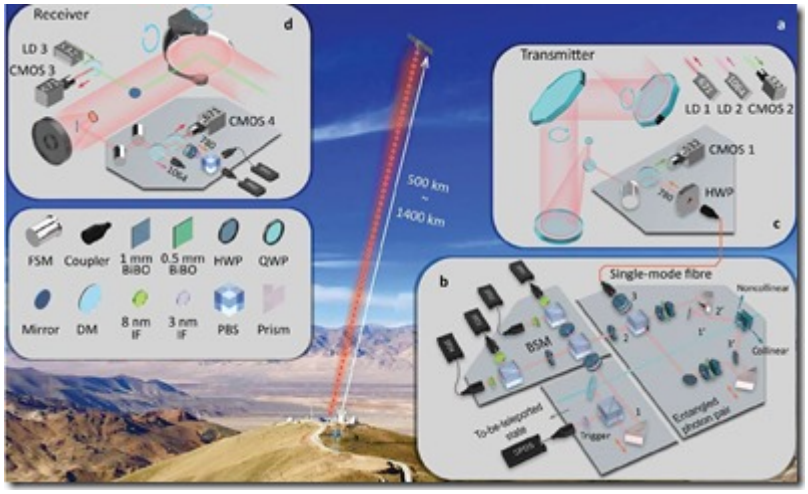
En mai 2017 était annoncée la création d'un prototype d'ordinateur quantique photonique par l'**Institute for Quantum Information** de l'Académie des Sciences Chinoise de Shanghaï (**source**). Petit détail : il ne comporte qu'un seul qubit à base de photon unique (*ci-dessous*) (**source**). La branche "optique linéaire" de l'informatique quantique est prometteuse mais pour l'instant a bien du mal à "scaler". Il est cependant tout à fait normal que, comme bien d'autres pays, plusieurs voies de création de qubits physiques soient explorées.

En août 2018 était annoncée une autre prouesse dans la lignée de la précédente avec deux qubits manipulant des photons, fabriqués en technologie CMOS, dans **Large-scale silicon quantum photonics implementing arbitrary two-qubit processing**, août 2018 (7 pages). La nouveauté résidait dans l'exploitation de portes quantiques opérant sur ces deux qubits. Mais contrairement à la couverture presse qui s'enthousiasme sur la question (par exemple, dans **Des chercheurs chinois sur la voie du processeur quantique 'ultime' ? Effectivement ça sent bon !** de

Bruno Cormier dans Tom's Hardware), il faut raison garder. Il est difficile d'intriquer correctement ces qubits à grande échelle et leurs taux d'erreurs sont largement supérieurs à 1% alors qu'il faudrait être situé entre 0,001% et 0,1% pour que cela soit intéressant. Qui plus est, la technologie n'est pas si facile que cela à miniaturiser. Comme son taux d'erreurs est très élevé, il faudra créer des qubits logiques avec un très grand nombre de qubits physiques pour qu'un tel ordinateur quantique soit pratiquement utilisable. Petits détails utiles : ce projet conduit par plusieurs laboratoires de recherche chinois a été mené en partenariat avec le laboratoire de photonique de Jeremy O'Brien à l'Université de Bristol et un laboratoire australien à Brisbane.

Des partenariats public-privé sont aussi établis en Chine, le plus connu étant celui d'**Alibaba** qui a investi 1 Md$ dans l'USTC de Jian-Wei Pan pour lancer en 2015 l'**Alibaba Quantum Computing Laboratory** à Shanghai, qui s'intéresse à la crypto quantique et à l'ordinateur quantique. La crypto quantique pourrait servir à sécuriser certaines transactions de commerce en ligne et de liaisons entre data centers. Alibaba lançait même en janvier 2018 la mise en ligne dans le cloud d'un ordinateur quantique de 11 qubits développé par l'USTC, faisant suite au lancement d'un simulateur quantique à base d'ordinateurs traditionnels de 22 qubits fin 2017. Cette offre de tests d'algorithmes quantiques dans le cloud est très similaire à celle que propose IBM depuis 2016, sachant néanmoins qu'il est difficile de les comparer sans un benchmark précis des caractéristique des qubits en termes de temps de cohérence.

Tout cela est très bien mais pas spécialement plus au point que ce que l'on trouve aux USA ou en Europe. Par contre, la Chine est en avance du côté de la cryptographie quantique, au moins au niveau du livre des records. Cela commence avec une expérience record d'intrication de photons à longue distance menée mi 2017. La téléportation d'un photo dupliqué était réalisée à 5100 m d'altitude à Ngari au Tibet vers le satellite Micius qui orbite à 500 km d'altitude, et à une distance maximale de 1400 km. Les photons émis provenaient d'un laser opérant dans l'ultraviolet. Ce genre d'expérience avait déjà été faite sur Terre avec des distance allant jusqu'à 100 km correspondant à la longueur maximale d'une fibre optique sans répéteur (**source du schéma et détails de l'expérience**). En gros, la performance chinoise revenait à reprendre à longue distance l'expérience d'Alain Aspect de 1982. Elle permet notamment d'envoyer des clés quantiques protégées contre les interceptions.



L'expérience a été renouvelée début 2018 avec l'organisation d'une vidéoconférence entre la Chine et l'Autriche utilisant une clés d'encryption quantique envoyée toutes les minutes (**source**). La Chine prévoit en fait de lancer d'ici 2030 une nuée de satellites dédiée à l'envoi de clés quantiques en reprenant ce processus. Enfin, une liaison en fibre optique protégée par clé quantique de 2000 km a été déployée entre Shanghaï et Beijing. En tout cas, on voit que la Chine prendre très au sérieux cette histoire de sécurisation des communications !

Du côté des entreprises, on peut citer **ZTE** et les startups **QuantumCTek** et **Qasky Science** qui sont spécialisés dans la cryptographie quantique. Les deux dernières ont rejoint avec le Suisse ID Quantique and l'Américain Battelle le **Quantum-Safe Security Working Group**, qui fédère l'industrie de la cryptographie quantique. Bref, la Chine met le paquet sur le quantique dans toutes ses dimensions, mais surtout dans la cryptographie quantique !

Sur le calcul quantique, la Chine semble par contre un peu en retrait. Ils ne semblent pas avoir d'influence dans le monde académique sur la partie algorithmique et programmation. Aucun outil de développement ou framework de développement d'application quantique n'est proposé au monde par la Chine. Même pour la sécurité, ils mettent le paquet sur la QKD pour la gestion de clés symétriques alors que la communauté scientifique de la sécurité considère que c'est une chimère et qu'il vaudrait mieux se focaliser sur la cryptographie post-quantique et des architectures de clés publiques résistantes aux ordinateurs quantiques. Là encore, cela repose plutôt des mathématiques et du logiciel.

Il ne faut jamais oublier le rôle stratégique du logiciel et des plateformes dans les batailles économiques du numérique ! J'ai l'impression que l'Histoire se répète en Chine de ce côté-là.

Quelles stratégies industrielles pour le quantique ?

Le marché potentiel de l'informatique quantique est et restera probablement assez longtemps un marché de niche. Les prévisions des analystes qui sont d'habitude tout feu tout flamme sur les marchés émergents comme sur l'**Internet des objets** sont assez prudents, et à juste titre, sur la taille de ce marché. Il serait de $553M en 2023 selon **MarketsandMarkets**, une prévision datant d'aout 2017. Il serait de $1,9B en 2023 selon **CIR** et de $2,64B en 2022 selon **Market Research Future**, une prévision datant de 2018. **Homeland Security Research** voit plus large avec $8,45B en 2024 (en 2018), intégrant produits et services, auxquels s'additionneraient $2,24B de financements publics.

Une étude de **Morgan Stanley** de 2017 évalue la taille du marché de l'informatique quantique à

plus de $10B en 2028 tout en la comparant au marché de l'informatique grand public ($590B, en y intégrant les PC, les smartphones et les tablettes) et d'entreprise ($185B). Les marchés visés mis en avant sont souvent celui des transports, de la défense et de la lutte contre le cybercriminalité. Ces prévisions intègrent parfois le marché de la cryptographie quantique. Par comparaison, le marché des supercalculateurs était situé aux alentours de $5B à $6B en 2017. En juillet 2018, ABI Research évaluait pour sa part le marché du quantique à $15B d'ici 2028.

Le marché de l'informatique quantique est en fait bien moins mature et prêt à être lancé que celui de la cryptographie quantique. L'ordinateur quantique est incertain et assez éloigné dans le temps. Cela explique l'investissement de presque tous les pays en parallèle dans l'informatique quantique, la cryptographie quantique et la métrologie quantique, cette dernière ayant un marché cible très professionnel et limité. Les états sont motivés à investir sur le quantique pour des raisons stratégiques : à la fois dans l'idée de pouvoir décrypter les télécommunications existantes ou passées dans le cadre de l'activité de leurs services de renseignement (Direction Technique de la DGSE en France, NSA aux USA, GCHQ au Royaume-Uni…) et de protéger les leurs via la cryptographie quantique. Le quantique est donc, plus que presque toute autre technologie numérique, un outil de souveraineté stratégique des états.

Les partenariats dans l'informatique quantique sont de nature différente : entre laboratoires de recherche intra-pays (comme dans l'initiative Quantum Silicon Grenoble), inter-pays (comme le CEA-LETI et USNW, ou les Chinois avec les Australiens et les Britanniques), puis entre la recherche publique et le privé au sein du même pays (CEA et Atos) ou entre pays différents (Intel avec Qutech). La raison d'être de tous ces partenariats est identifiable : l'informatique quantique est un sujet scientifique complexe qui ne peut pas être maitrisé par un seul laboratoire ou une seule entreprise. La collaboration est nécessaire pour rassembler des talents de spécialités différentes, entre la physique de la matière condensée, les technologies de capteurs et de contrôle, l'optronique, la cryogénie, la production de semiconducteurs, l'algorithmie et le développement logiciel.

Au-delà de cet aspect stratégique se posent des questions sur la vitesse à laquelle le secteur privé pourrait et devrait prendre le relai de la recherche fondamentale publique. C'est un enjeu technologique au long cours qui relève d'un risque presque aussi grand que le risque et l'incertitude scientifique. Quel serait le meilleur timing de l'investissement privé et la capacité de le faire avec une incertitude technologique très forte ? Il existe quelques "best practices" comme ID Quantique, lancé en Suisse par le chercheur Nicolas Gisin.

Malgré la belle dynamique autour des deep techs que l'on sent en Europe et en France, ce type de financement semble pour l'instant accessible uniquement en Amérique du Nord. Il nous faut inventer des modèles entrepreneuriaux et de financement permettant de conduire des aventures au long cours dans le secteur privé, à l'image de la longue histoire de D-Wave.

Comme d'habitude, nombre de pays se demandent comment encourager la création de startups par des chercheurs ou l'exploitation de leurs travaux par des entrepreneurs qui ne sont pas des chercheurs. A part ATOS qui s'est déjà engagé sur le quantique, quelles autres entreprises établies et orientée "produits" pourraient se lancer sur le quantique ? On pense au complexe militaro-industriel avec des entreprises comme Thalès. Le quantique est peut-être le seul endroit où un "CloudWatt" aurait eu du sens avec un financement public/privé, voir même une approche transnationale européenne.

La situation actuelle met en lumière une autre déficience française : l'absence d'un office

scientifique rattaché à l'exécutif comme il en existe aux USA ou en Israël. Lorsque l'exécutif a besoin de lumières pour comprendre les enjeux scientifiques du moment, vers qui se tourne-t-il ? Comme on l'a vu sur l'intelligence artificielle, il doit lui-même jouer le rôle d'intégrateur et enquêter auprès de centaines de personnalités et organisations représentatives. C'est long, séquentiel, souvent biaisé et réalisé de manière ponctuelle alors que cela devrait être une tâche permanente et centralisée quelque part et piloté par une personnalité reconnue par la communauté scientifique. Ce n'est cependant pas le rôle d'une Académie comme celle des sciences celle des technologies.

Ainsi, aux USA, l'Académie des Sciences est une organisation privée distincte de l'Office Scientifique et Technologique du Président (OSTP) établi par le Congrès en 1976. L'OSTP s'appuie sur le National Science and Technology Council, créé sous la Présidence Clinton en 1993.

Enfin, nous avons aussi l'opportunité de créer un écosystème logiciel avec des outils de modélisation, de développement et des applicatifs métiers. La cartographie des acteurs privés de l'informatique quantique que j'ai compilée à partir de sources diverses est encore éparse (dans les articles sur les **startups** et sur la **cryptographie**). Une industrie nouvelle va probablement émerger de l'informatique quantique, même si elle sera plus modeste en taille que le marché de l'informatique d'entreprise actuel. L'un des enjeux clés me semble être celui de la création d'applications "grand public" du quantique. A savoir, des applications qui pourraient générer des économies d'échelle et permettre à ce marché de dépasser le cadre d'un marché étroit dédié à la recherche et à quelques applications b2b.

Nous avons aussi besoin de mathématiciens et d'une nouvelle génération de développeurs qui vont devoir tout apprendre ou réapprendre pour créer et utiliser des algorithmes quantiques.

Bref, il faut se bouger si l'on veut éviter de se voir une fois de plus dominés par des acteurs américains, canadiens si ce n'est chinois. Le syndrome de la dominance des GAFA peut se reproduire facilement dans le quantique si l'on n'y prend gare. Si la France annonçait la couleur sur le sujet, il vaudrait mieux que cela se fasse très rapidement. Pas dans 5 ans avec un "plan de rattrapage" comme l'est le Rapport Villani pour ce qui est de l'intelligence artificielle.

Dans la **partie suivante**, nous sortirons temporairement du champ du calcul quantique en nous intéressant à la médecine quantique et à la manière dont elle récupère très approximativement les connaissances de la physique quantique.

Cet article a été publié le 10 septembre 2018 et édité en PDF le 16 septembre 2018.