Brunngasse 36
CH-3011 Bern
www.ta-swiss.ch

Mars 2021

# Document de réflexion « Les technologies quantiques »

## 1. Introduction

Les technologies quantiques abordées dans cet article sont souvent désignées comme formant la « deuxième révolution quantique ». Et de fait, beaucoup de personnes pensent que ce n'est qu'une question de temps avant que leur potentiel révolutionnaire pour notre société ne soit libéré [LEWIS18-1]. Ces technologies ont la particularité de reposer sur la création, la manipulation et la lecture active d'états quantiques *individuels* et d'utiliser des particularités quantiques telles que la superposition d'états, l'intrication et l'effet tunnel. En comparaison, la « première révolution quantique » reposait sur les effets de la mécanique quantique impliquant des *ensembles* de particules et a conduit au développement de dispositifs tels que les transistors (les éléments constitutifs des ordinateurs), les systèmes laser, le GPS ou les imageurs IRM, qui ont profondément marqué notre société.

L'intérêt pour les technologies quantiques s'est accru dans le monde entier au cours des cinq dernières années, comme en attestent une forte augmentation des demandes de brevets [GIBNEY2019] et des financements publics. Il règne également un esprit de compétition entre la Chine, les États-Unis, le Japon et l'Europe [SMITH19]. La Suisse s'engage activement dans le développement de cette technologie et occupe une position de leader mondial en matière de recherche [CSS20]. Dans cet article, nous allons examiner où en est le développement des technologies quantiques *appliquées* afin de cerner le meilleur moment pour lancer une étude d'évaluation technologique. L'objectif de cette étude sera alors d'identifier et d'analyser à un stade aussi précoce que possible les conséquences de ces nouvelles technologies sur notre société. À cette fin, nos lectrices et lecteurs sont invités à faire part de leurs réactions à TA-SWISS[1].

[1] info@ta-swiss.ch

# 2. Applications

Les technologies quantiques couvrent un large éventail de domaines d'application et ont été divisées en trois grandes catégories : (1) l'informatique et la simulation quantiques, (2) la communication quantique et (3) la détection et la métrologie quantiques. Les sous-sections suivantes vous donnent un aperçu de ces domaines. Pour plus d'informations sur les technologies quantiques ainsi que sur leurs développements techniques, le lecteur est invité à consulter le récent livre blanc du Conseil suisse de la science [CSS20].

## 2.1. Informatique et simulation quantiques

Les ordinateurs quantiques sont l'application la plus médiatisée de cette technologie. Ils promettent d'effectuer des calculs pratiquement impossibles avec l'informatique classique en raison de l'effort de calcul élevé qu'ils requièrent, comme la recherche dans de grandes quantités de données non structurées ou la factorisation de grands nombres. La première est essentielle, par exemple, pour l'apprentissage machine, la recherche génomique et la recherche sur les sites web, tandis que la seconde est généralement utilisée dans les systèmes de cryptographie classiques[2]. Fin 2019, certains affirmaient déjà avoir démontré la suprématie quantique[3] pour des problèmes spécifiques [ARUTE19]. Il est aujourd'hui possible d'acheter ou d'utiliser via le cloud des ordinateurs quantiques avec un nombre défini de qubits. Mais il faudra vraisemblablement attendre encore au moins une décennie avant de disposer d'un ordinateur quantique universel. Néanmoins, il n'est pas exclu que des ordinateurs quantiques, comme les simulateurs quantiques ou les recuits quantiques (quantum annealers), soient développés avant cela pour des applications spécifiques. Des ordinateurs quantiques permettant de simuler des systèmes physiques complexes pourraient notamment être utilisés pour découvrir de nouveaux matériaux, des interactions et des réactions chimiques (par exemple dans le cadre de la recherche de nouveaux médicaments), tandis que les recuits quantiques pourraient résoudre des problèmes d'optimisation complexes (par exemple en logistique).

Ainsi, l'informatique quantique devrait donner un coup d'accélérateur au big data, à l'intelligence artificielle ou à l'apprentissage machine et donc accroître les possibilités mais aussi les risques liés à ces technologies, tels que les menaces pour la protection des données, l'opacité des résultats ainsi que la distorsion due à des ensembles de données déséquilibrés, pour n'en citer que quelques-uns [CHRISTEN20]. Ces risques font déjà partie du débat concernant ces technologies, indépendamment de leur nature classique ou quantique. Toutefois, bien qu'à un

[2] Les ordinateurs quantiques ont longtemps été vus comme une menace pour la sécurité car ils peuvent résoudre les problèmes mathématiques sur lesquels repose la cryptographie classique. Cependant, il existe maintenant des algorithmes cryptographiques qui sont considérés comme inviolables même en cas d'attaque par un ordinateur quantique.

[3] La suprématie quantique se réfère à un dispositif quantique programmable capable de résoudre un problème qu'aucun ordinateur classique ne peut résoudre en un temps raisonnable (quelle que soit l'utilité du problème).

stade précoce, les simulateurs et recuits quantiques pourraient bien ouvrir de nouvelles voies et donc avoir des conséquences imprévues sur notre société avec un ensemble d'opportunités et de risques tout à fait nouveaux. Ceux-ci devront alors être évalué et discuté.

## 2.2. La communication quantique

La communication quantique implique une communication intrinsèquement sûre basée sur une distribution de clés quantiques. La mise sur écoute de ces canaux à cryptage quantique est impossible car une interférence externe détruirait les informations quantiques. Elle est envisagée dans les domaines des télécommunications, de la finance, des assurances, de la santé, des transports, de la défense, de l'aéronautique et des infrastructures sensibles. Cette application a un impact sur les gouvernements et les entreprises autant que sur les consommatrices et consommateurs. Il existe déjà des solutions de déploiement commercial mais sur des distances limitées car certains points techniques restent à résoudre. Cependant, ceux qui doutent de cette technologie soulignent qu'elle requiert de nouvelles infrastructures et pensent que la cryptographie standard est appelée à évoluer pour rester sûre [LEWIS18-1]. Par exemple, la cryptographie dite « post-quantique » est en cours de développement et repose sur des algorithmes cryptographiques censés résister aux attaques des ordinateurs classiques et quantiques [BERNSTEIN19].

Une autre application bien établie dans le domaine de la communication est le générateur de nombres aléatoires quantiques, qui est capable de générer des clés complètement aléatoires et qui est utilisé pour augmenter la sécurité de la communication. Ici aussi, il existe des produits commerciaux dotés de cette technologie, comme par exemple l'un des smartphones Samsung sorti en 2020 [WINDER20].

En matière de sécurité des communications, on retrouve le conflit d'intérêts bien connu entre, d'une part, les avantages sociétaux de la protection des données et de la vie privée et, d'autre part, la menace potentielle pour la sécurité, ce indépendamment du contexte classique ou quantique.

## 2.3. La détection et la métrologie quantiques

La détection quantique ouvre de nouvelles plages de sensibilité et de précision en termes de mesure, offrant de nouvelles possibilités pour un large éventail d'applications. Il existe déjà des dispositifs utilisant la détection quantique qui ont été déployés, et d'autres qui sont en cours de développement. Parmi les applications, l'on compte les gravimètres quantiques, les capteurs magnétiques quantiques ou les horloges quantiques. Les gravimètres quantiques sont capables de cartographier le sous-sol, de voir dans un coin ou derrière un mur ou d'annoncer une éruption volcanique. Ils peuvent être utilisés dans les secteurs de la construction, du pétrole et du gaz, ainsi que pour la sécurité ou la surveillance. Les technologies de détection magnétique quantique sont, quant à elle, principalement développées à des fins d'imagerie et pourraient apporter une aide dans le cadre des diagnostics médicaux, des véhicules autonomes ou de la

surveillance. Enfin, les horloges quantiques fournissent une mesure du temps plus précise qui impacte les domaines de la finance, de l'énergie, des télécommunications ou du génie militaire.

Ce domaine est en pleine expansion [MARKET20]. À ce stade, les applications existantes alimentent les débats actuels en matière de vie privée et de sécurité. Les nouvelles applications encore à venir pourraient toutefois soulever de nouvelles controverses.

## 3. Évaluation technologique

L'objectif de TA-SWISS est d'évaluer, d'identifier et d'analyser le plus tôt possible les conséquences des technologies émergentes et de proposer des plans d'action viables. Les technologies et leurs conséquences sont étudiées dans une approche multidisciplinaire et interdisciplinaire, sous les angles juridiques, sociaux, éthiques, politiques, économiques et écologiques. Le Parlement et le Conseil fédéral s'appuient sur les recommandations des projets TA-SWISS pour prendre des décisions, en particulier pour des sujets technologiques controversés. Les résultats des projets s'adressent également aux responsables politiques, aux spécialistes des sciences et de l'administration, ainsi qu'aux médias et aux citoyennes et citoyens intéressés.

Dans le cas des technologies quantiques, nous avons passé en revue les applications existantes et potentielles en mettant l'accent sur les défis qu'elles sont susceptibles de poser à notre société. À ce jour, ces défis « quantiques » sont pour la plupart du même ordre que ceux dits « classiques ». Pour cette raison, et parce que ces technologies commencent tout juste à faire émerger de nouvelles applications avec leurs opportunités et leurs risques, TA-SWISS estime qu'il est encore trop tôt pour lancer une étude sur leur impact à ce stade. Nous poursuivons cette veille technologique passionnante afin de lancer une telle étude au bon moment. Vos commentaires et réactions sont les bienvenus[4].

[4] info@ta-swiss.ch

## Sources :


ARUTE19 Arute, F., Arya, K., Babbush, R. et al. Quantum supremacy using a programmable superconducting processor. Nature 574, 505–510 (2019), doi:10.1038/s41586-019-1666-5

BERNSTEIN19 Bernstein, D., Lange, T. Post-quantum cryptography. Nature 549, 188–194 (2017), doi.org/10.1038/nature23461

GIBNEY19 Gibney E., Nature 574, 22-24 (2019), doi: 10.1038/d41586-019-02935-4, Technology Race, Forbes 10 Oct. 2019

LEWIS18-1 Lewis, A. M., Ferigato, C., Travagnin, M and Florescu, E; The Impact of Quantum Technologies on the EU's Future Policies: Part 3 Quantum Computing; EUR 29402 EN (2018), doi:10.2760/737170

LEWIS18-2 Lewis, A. M., Travagnin, M MT, Quantum communications:from science to policies, EUR 29017 EN (2018), doi:10.2760/881896

MARKET20 Market Reports World, Global quantum sensors market report, 22 Jul. 2020

CSS20 Mahon J.C. et le Conseil suisse de la science, Livre blanc: Les technologies quantiques en Suisse, Réflexions et recommandations du Conseil suisse de la science CSS, Octobre 2020

SMITH19 Smith-Goodson, P., Quantum USA Vs. Quantum China: The World's Most Important

CHRISTEN20 Christen M. et al., Wenn Algorithmen für uns entscheiden: Chancen und Risiken der KI, TA-SWISS, 2020, ISBN: 978-3-7281-4001-2

WINDER20 Winder, D., Samsung Surprise As World's First Smartphone With Quantum Technology Launches, Forbes, May 22 2020