

LA SOUVERAINETÉ NATIONALE AU SEIN DU PLAN NATIONAL QUANTIQUE



NEIL ABROUG
coordonnateur national de la Stratégie
quantique - Secrétariat général
pour l'investissement

Le Plan national quantique français vise à placer notre pays en tête de la compétition internationale dans l'utilisation des technologies quantiques. Il en va de notre indépendance nationale.

Si les premières applications de la physique quantique, à l'image des transistors, des lasers, des cellules photovoltaïques et des LED, ont profité de la maîtrise du contrôle des flux de quanta, une nouvelle classe de technologies quantiques, reposant sur la capacité à isoler les objets quantiques pour les manipuler individuellement, est en train d'émerger aujourd'hui. L'exploitation, dans ce contexte, des propriétés étonnantes de superposition et d'intrication ouvre la voie à des ruptures technologiques majeures dans le domaine du calcul, de la métrologie, de la communication et de la cybersécurité, impactant fortement un large champ de secteurs économiques, ainsi que la sécurité nationale.

Un espoir de ruptures majeures

À long terme, la perspective de réaliser l'ordinateur quantique universel passant à l'échelle porte un espoir de ruptures majeures, dans des secteurs stratégiques à l'image de la santé, la lutte contre le réchauffement

climatique, l'alimentation, la pharmaceutique, l'énergie et la cybersécurité. Cette ambition représente un pari que la France est l'un des rares pays en mesure de relever. Les enjeux de souveraineté liés au développement des technologies quantiques sont élevés. Sans accélération immédiate, la France ne serait pas assurée d'un libre accès à ces technologies dans le contexte géostratégique d'aujourd'hui, d'autant plus que le marché sera étroit et pointu, du moins dans un premier temps.

Le choix français d'un environnement ouvert

Depuis quelques années, des écosystèmes très fortement intégrés se constituent autour de machines qui, bien qu'elles ne confèrent pas d'avantage quantique avéré, permettent d'anticiper les ruptures futures tout en fédérant et fidélisant un écosystème de développeurs autour d'outils de développements *hardware*-dépendants. Aujourd'hui, ces stratégies constituent un frein à l'adoption du calcul quantique par les secteurs aval qui appréhendent, au regard des différentes solutions technologiques en compétition, le risque d'une dépendance prématurée à une solution qui soit abandonnée à terme au profit des autres. Elles représentent plus largement un risque sur l'indépendance technologique nationale. Cet enjeu s'accompagne, également, d'une opportunité de développer un modèle ouvert, interopérable et *hardware*-agnostique. C'est ce choix qu'a fait la France à travers l'initiative HQI (Hybrid

HPC Quantum Initiative). Pilotée par le CEA, l'initiative HQI mobilise particulièrement GENCI (Grand Équipement national de calcul intensif) en charge du volet relatif aux acquisitions de simulateurs et calculateurs quantiques. Ce volet devrait être abondé au cours des prochaines années par des cofinancements européens et industriels. À plus long terme, la France vise à développer des ordinateurs quantiques tolérants aux défauts, capables de passer à l'échelle et de rendre possibles des calculs et modélisations de plusieurs ordres de grandeur plus complexes que ce qui est envisageable à court terme avec les supercalculateurs traditionnels.

Anticiper les risques de déchiffrement

S'il est peu probable à court terme, l'avènement post-2030 de l'ordinateur quantique capable de déchiffrer, éventuellement rétroactivement, des données protégées par des algorithmes à clé publique actuels n'est pas exclu. Pour faire face à ce risque, les agences de sécurité comme l'ANSSI recommandent de garantir la confidentialité et l'intégrité des systèmes d'information et des communications de l'État de manière anticipée, en développant et en déployant des schémas cryptographiques asymétriques, appartenant à la « cryptographie postquantique », résistant à une cryptanalyse quantique (e.g. CRYSTALS-Kyber et CRYSTALS-Dilithium récemment retenus comme prochains standards de cryptographie par le National Institute of Standards and Technology américain), d'une part, et en déployant, lorsque c'est pertinent, des schémas de cryptographie symétrique classique avec des tailles de clés adaptées, sur lesquelles un ordinateur quantique n'a pas d'impact connu (clés AES *Advanced Encryption Standard* en augmentant la taille de la clé de chiffrement), d'autre part.

Des technologies habilitantes au quantique

Quelle que soit l'issue de la course au développement de l'ordinateur quantique, l'ensemble des compétiteurs auront besoin d'accéder à des technologies classiques dites capacitances (cryogénie, lasers, isotopes stables, machines de dépôt sous vide, amplificateurs, filtres...). Ces technologies capacitances, si elles ne sont pas maîtrisées en France et en Europe, pourraient freiner nos développements, voire les bloquer. Elles pourraient *a contrario* apporter un impact économique à court terme pour l'ensemble de la stratégie quantique. C'est pour cela que, de manière assez singulière en comparaison avec les autres États, la stratégie quantique française accorde une attention particulière à développer les filières industrielles des technologies habilitantes au quantique,

à travers plusieurs programmes structurants visant à consolider les chaînes de valeurs industrielles, notamment dans le domaine de la cryogénie, des lasers, de l'électronique bas bruit et des lasers.

Une attention particulière est également accordée dans la stratégie quantique française à la standardisation, aussi bien *de jure* (normalisation) que *de facto* (consortia privés et stratégies de constitution d'écosystèmes). La standardisation permet, en effet, par l'homogénéisation des spécifications des produits et services, l'accès à l'ensemble des marchés mondiaux et leur offre un moyen d'accroître fortement l'impact économique d'une innovation ou d'un titre de propriété industrielle, lorsqu'elles savent se positionner dans l'élaboration des normes. Le Laboratoire national de métrologie et d'essais s'est ainsi vu confier par l'État la mission d'animer les travaux de standardisation relatifs aux technologies quantiques. ×

“Un pari que la France est l'un des rares pays en mesure de relever.”

Les objectifs clés de la Stratégie quantique française :

- › Maîtriser les technologies quantiques offrant un avantage stratégique décisif, dont les accélérateurs, simulateurs et ordinateurs quantiques, les logiciels métiers pour le calcul quantique, les capteurs, les systèmes de communication.
- › Dans le domaine du calcul, le thème central de la stratégie :
 - devenir le premier État à disposer d'un prototype complet d'ordinateur quantique généraliste de première génération dès 2023 ;
 - être un leader mondial dans la course à l'ordinateur quantique universel passant à l'échelle, en anticipant dès aujourd'hui les risques inhérents liés au faible niveau de maturité et à la complexité des technologies en cours d'exploration.
- › Maîtriser les filières industrielles critiques dans le domaine des technologies quantiques, incluant les technologies habilitantes.
- › S'affirmer comme l'un des leaders mondiaux en matière de cryogénie ou de lasers pour les technologies quantiques.
- › Être la première nation à disposer d'une filière complète productrice de Si 28 industriel, notamment pour les besoins de la production de qubits.
- › Développer les compétences et le capital humain, renforcer les infrastructures technologiques, créer un environnement favorable à l'intensification de l'entrepreneuriat, au transfert de technologie, et promouvoir l'attractivité vis-à-vis des acteurs internationaux et des meilleurs talents mondiaux.