# 21 Avril 2021 : Conférence AAT - 3AED :

# « La révolution quantique - enjeux pour la défense et la sécurité »

# Par Madame Valérie Gacogne

L'Association de l'Armement Terrestre et 3AED-IHEDN (ex-AACHEAr) ont eu le plaisir de présenter le 21 Avril 2021 une e-conférence qui, aurait pu s'intituler, pour paraphraser un film célèbre de Woody Allen

*« Tout ce que vous voulez savoir sur la Révolution quantique sans oser le demander ! »*

Le comité *Kantik* de la 55e Session nationale Armement et économie de défense de l'Institut des hautes études de défense nationale (IHEDN) a remis, en mai 2019, un rapport intitulé *la révolution quantique : enjeux pour la défense et la sécurité*. Ce rapport, le premier du genre en France, traitait de la nouvelle révolution en cours, celle des technologies quantiques. Le travail a consisté à dresser un panorama des technologies quantiques — dans les domaines du calcul, des communications et des capteurs — à mettre en perspective les développements et investissements dans les différents pays, à proposer des scénarios potentiels d'émergence de ces technologies et à formuler des recommandations stratégiques pour positionner la France au meilleur niveau face à cette nouvelle révolution quantique.

Les recommandations formulées ont été restituées par le comité au plus haut niveau de l'Etat, notamment par Valérie Gacogne en sa qualité de rapporteur : au cabinet du Président de la République, du Premier ministre, du cabinet de la Ministre des Armées et à Bercy. Ces travaux ont notamment servi de support au rapport de la mission interministérielle sur le quantique qui a été remis en janvier 2020 (*Quantique : le virage technologique que la France ne ratera pas*).

---

Notre e-conférencière était Madame Valérie Gacogne. Celle-ci est titulaire d'un doctorat de l'Ecole Nationale des Ponts et Chaussées et auditrice de la 55e SN AED. Elle a une expertise dans la modélisation et simulation des systèmes complexes. Elle a créé et dirigé la SARL Complexio pendant près de 14 ans, et a mis au service de diverses disciplines ses compétences en modélisation dans le cadre de projets de recherche et d'études en France et à l'international. Elle a également enseigné cette discipline pendant plus de 20 ans dans des écoles d'ingénieurs (Ecole des Ponts, Ecole Centrale Paris, Ecole des Mines…) en France et en Chine. Elle est aujourd'hui chargée de mission au cabinet de la Maire-Présidente de Quimper Bretagne Occidentale et cadre de comité de la 57e SN AED (Colonel réserviste spécialiste de l'Armée de Terre).

---

# Résumé

Tous les principes de la physique de l'infiniment petit ont été posés il y a déjà près d'un siècle ; la première révolution quantique a ainsi vu émerger lasers, transistors et circuits intégrés et a profondément modifié notre quotidien. Une deuxième révolution quantique est en cours. Elle promet l'avènement d'un ordinateur quantique aux puissances de calcul inégalées, susceptible notamment de mettre à mal la sécurité des systèmes d'information en attaquant les algorithmes de chiffrement à clés publiques couramment utilisés. Dans le même temps, les développements dans le domaine des communications quantiques promettent la sécurité absolue des communications par la voie de la cryptographie quantique et, en particulier, l'échange quantique de clés de chiffrement, dont l'interception non remarquée serait impossible. Enfin, des capteurs à des niveaux de précision et de sensibilité inédits sont en gestation, tels que des systèmes de positionnement si précis qu'il serait possible de s'affranchir des systèmes de navigation par satellite, et, affirment les Chinois, des radars quantiques si sensibles qu'ils rendraient caduque la notion de furtivité. Aux craintes soulevées se mêlent parfois des interrogations sur la faisabilité, voire la crédibilité, de certaines annonces.

La Chine affiche son ambition de devenir le chef de file des technologies quantiques en investissant massivement pour dépasser les États-Unis qui jusqu'à présent étaient le premier pays en termes de dépenses grâce à un niveau d'investissement public élevé, allié à un fort dynamisme de l'investissement privé. En Europe, un programme dénommé *Quantum Flagship*, lancé par la Commission européenne en 2018, tente de structurer la recherche, active dans quasiment tous les pays d'Europe.

La France est, quant à elle, reconnue au niveau mondial dans le milieu académique, mais elle est l'un des rares pays majeurs à ne pas disposer à ce jour d'une feuille de route. Elle présente un secteur atomisé, peu orienté vers l'industrialisation, même si elle compte quelques start-ups à la pointe.

Ce rapport, rédigé par le comité n° 3 « *kantik* » de la 55e session nationale « Armement et économie de défense » (AED) de l'IHEDN, dresse un état des lieux des nouvelles technologies quantiques et des enjeux pour la défense et la sécurité. Il apporte un éclairage sur les opportunités et menaces de la révolution quantique en cours, et propose des recommandations pour que la France en tire le meilleur parti, en considérant notamment les enjeux de souveraineté et les problématiques propres à la sécurité et à la défense.

# CR établi à partir des notes prises par M. Thomas Reydellet

**Introduction** :

Révolution ? pas tout à fait, car la physique de l'infiniment petit peuple notre quotidien (cf début du 20e avec les transistors, les lasers, …). Progrès années 70-80 => possible la manipulation de l'infiniment petit et donne des capacités de puissance de calcul, de com, des senseurs plus précis

Question de la vulnérabilité de certains de nos systèmes d'armes, de nos réseaux de communication vis-à-vis d'attaques cyber quantique … mais offre aussi de larges possibilités nouvelles !

Les US sont très avancés. La Chine est en position offensive. En Europe, les positions sont plus hétérogène. En Janvier 2020, publication du rapport de la mission interministérielle intitulé « Quantique le virage techno que la France ne rattrapera pas »

Notre conférencière, Mme Valérie GACOGNE, auditeur de la session 55 de l'IHEDN-AED (ex CHEAr), chargée de mission au cabinet de la Maire-Présidente de l'agglomération de Quimper Bretagne occidentale expose la problématique.

- Le rapport est arrivé dans une phase où beaucoup de rapports sortaient sur le sujet
- 3 piliers :
    - Cette révolution quantique nous promet des **ordinateurs quantiques** à la puissance de calcul inégalée avec des risques sur nos solutions. Il y a aussi les communications quantiques
    - La physique quantique promet aussi la sécu absolue car la **cryptographie quantique** = enjeu des communications
    - Les **capteurs** avec des niveaux de précision extrême
- Radar quantique chinois ? menaces/opportunités … vaste champ
- On vit la **seconde révolution quantique** très forte et porteuse de forts enjeux
- LA 1ère révolution quantique, tous les principes ont été posés il y a un siècle => elle a modifié notre quotidien. **La seconde révolution n'apporte pas de nouveaux principes**, mais utilise certaines des propriétés dont la superposition (cf. chat de Schrödinger mort & vivant à la fois)
- Un ordinateur / calculateur classique utilise des bits pour encoder l'info (0 ou 1). L'ordi quantique va utiliser des bits quantiques (**qubit**) et va prendre la valeur 0 ET 1 (état **superposé** qui permettra des calculs en parallèle). Ces qubits doivent parler entre eux (**intrication**). Quand plusieurs objets quantiques interagissent entre eux ou ont une origine commune, ils s'en trouvent intriqués (quelque soit la distance qui les sépare, ils **forment un tout indivisible et corrélé**). L'intrication dit que si on mesure l'un des objets, on connaîtra immédiatement la mesure de l'autre objet intriqué et ce quelque soit la distance qui les sépare
- 3 axes ont été étudiés, sur un **horizon de 30 ans** volontairement long car ces technos demandent un temps long pour le développement et l'industrialisation :
    - Les ordi, calculs et simulateur
    - Les communications
    - Les capteurs et la métrologie

- 60 interviews ont été menées pour alimenter ce rapport
- Cf la société IDQ dont le contrôle a été pris par une entreprise coréenne… alors que l'on a besoin d'un équipementier de confiance en Europe !

**L'ORDINATEUR :**

- L'ordinateur quantique était déjà évoqué dès 1982. La course effrénée trouve une origine dans **l'algorithme de Schor** (1994) mathématicien américain => cet algorithme qui ne peut fonctionner que sur un ordinateur quantique pourra hacker les clefs de cryptage actuelles en cassant les clefs de chiffrement basées sur la factorisation de nombres entiers (qui demande des temps de calculs gigantesques avec des ordinateurs classiques ; mais pas avec un ordinateur quantique qui calcule en parallèle). Des nations stockent pour pouvoir déchiffrer plus tard quand l'ordinateur quantique sera pleinement développé et disponible.
- **Différentes technos de fabrication des qubits** mais nombreux verrous technos à lever. L'ordi quantique existe (cf IBM avec un ordi quantique de 50 qubits mais fiabilité obtenue qu'avec 4 qubits) mais pas encore suffisamment fiable du fait des **phénomènes de décohérences** (les états en parallèles sont très fragiles aux conditions extérieures. Il faudrait **au moins 100 qubits pour améliorer cette fiabilité mais cela signifierait 100 000 à 1 Million qubits** ! Du coup l'algorithme de Schor ne sera pas disponible avant 10 ou 20 ans … Pas de consensus cependant sur la technologie qubit. Certains pensent l'obtenir dans 10 ans, d'autres pas avant 20 ou plus car butent sur des verrous technos ! **Les premiers qui arriveraient à avoir un ordi quantique n'auraient aucun intérêt à le révéler …**
- Diverses technos :
    - Qubit à bases de silicium (solution française).
    - IBM et la plus avancée avec les **qubits supra-conducteurs** mais butent sur des soucis de fiabilité (et la dimension est beaucoup plus importante que le qubit à base de spin d'électrons isolés par ex ! et c'est important pour ne pas tomber dans la décohérence qui met à mal la fiabilité).
    - **Spin d'électron isolé**
    - **Ions piégés**
    - **Photons**.
- Les simulations quantiques : permettent de résoudre des problèmes bien définis et spécifiques.
- Algorithme et programmation quantique : cf le **simulateur quantique d'Atos** (quantum runing machine). Il faut **penser les algorithme de manière différente** car on doit attendre la fin de tous les calculs pour mesurer le résultat, sinon on perturbe le phénomène quantique de la superposition des états en mesurant en cours. Le simulateur d'Atos simule un ordi quantique de 40 qubits. Avantage : Cet émulateur est neutre par rapport à la technologie de qubits qui pourrait finalement émerger.
- Mais **l'ordinateur quantique ne remplacera pas l'ordinateur classique**, il ne pourra pas répondre à tous les problèmes. On pourrait imaginer de **développer un co-processeur quantique intégré dans un ordi** classique pour résoudre certaines tâches spécifiques.

**Les COMMUNICATIONS** :

- Le **codage quantique est par nature inviolable** => les communications quantiques promettent la sécurité absolue (dans l'état actuel des réflexions). On est plus avancée sur les communications quantiques (et l'échange quantique de clefs de chiffrement), tirées par la **QKD** (**quantum Key ditribution**). Les 2 interlocuteurs construisent ensemble la clef de chiffrement par échange de photon. Toute interception sera décelée car **l'informatique quantique est non-duplicable (cf théorème de non-clonage)**
- La QKD techno expérimentée depuis 20ans mais **défi de la distance** (perte avec celle-ci et il faudrait ré-amplifier le signal via des **répéteurs quantiques qui n'existent pas (à ce jour)**. Aujourd'hui on est de point à point). Il y a aussi le taux de génération limité de la clef quantique)
- Un **Satellite en orbite basse pourrait servir de répéteur quantique** (cf expérience chinoise avec l'Autriche) ce qui permettrait l'emploi de la QKD sur de longues distances
- + **enjeu de la confiance** (preuves de sécu & standards)
- Cf Smart quantum et SECURE NET (start-up françaises qui ont fermé faute de marché et faute d'avoir été soutenues)
- Option de **l'algorithme post quantique** pour la cryptographie = il s'agit d'un **algorithme classique mais construit pour pouvoir repousser des attaques quantiques** (à encourager !). Pas de consensus scientifique sur le sujet

**Les CAPTEURS :**

· Pilier mature : ça fait très longtemps que les capteurs utilisent la physique quantique (cf horloge atomique)

· **Très nombreuses applications** (imagerie avec IRM, mesure gravimétrie, radar, horloge, centrale, centrale inertielle, qui nous permettrait de s'affranchir de positionnement satellitaire !)

· **Défi du passage à l'industrialisation** (cf réussite du gravimètre absolu de la société Muquans)

**AU NIVEAU MONDIAL** :

· Bouillonnement d'idées et d'initiatives au niveau mondial avec des investissements très importants.

· 21 janvier 2021 : annonce par la France de la stratégie quantique (1,8 Milliard € sur 5 ans – Mais l'Allemagne investi 2 Milliard € sur 2ans) qui fait suite au rapport de la mission interministérielle

· Le rapport IHEDN proposait plusieurs recommandations, reprises par la mission inter-ministérielle dont par ex 2 laboratoires quantiques, de soutenir financièrement, et de créer une instance interministérielle de pilotage.