

Les enjeux de la physique quantique et les ruptures à anticiper

David DESJARDINS

| Colonel (air), auditeur de la 69^e session du CHEM.

Comme l'a rappelé le président de la République Emmanuel Macron l'occasion de son discours sur la stratégie de défense et de dissuasion à l'École militaire, le 7 février 2020 : « l'émergence de nouvelles technologies, comme [...] les applications de la physique quantique [...], est porteuse de nombreuses opportunités, mais également source de futures instabilités ⁽¹⁾ ». Même si les principes quantiques font déjà l'objet d'applications très utiles comme le laser, l'imagerie médicale ou la navigation, les progrès de la recherche ces dernières années laissent entrevoir une nouvelle génération d'applications disruptives qui donneront à ceux qui les maîtriseront un avantage certain dans les domaines économique, financier et également militaire.

Dans ce dernier domaine, les ruptures technologiques en matière de détection, de communication et de calcul sont, d'ores et déjà, une certitude. Seule subsiste une incertitude sur le calendrier. La physique quantique recèle ainsi le potentiel pour fournir la supériorité opérationnelle dont toutes les armées modernes sont en quête permanente. Conscientes de cette réalité, les grandes puissances engagent des moyens considérables dans la recherche. L'Europe s'efforce de suivre le tempo imprimé par les États-Unis et la Chine car attendre placidement n'est pas une option. Aussi, une bonne appréhension du changement de paradigme que sous-tendent les principes quantiques doit permettre d'anticiper la portée des technologies associées ainsi que les obstacles à lever. Dans ce cadre, la France est sur le point de se doter d'une feuille de route quantique interministérielle. Il appartient désormais au ministère des Armées de développer son propre plan d'action « technologies quantiques » pour permettre aux armées de faire leur révolution quantique à l'horizon 2040.

Comprendre les principes de la physique quantique

Les théories électromagnétiques, les lois de la mécanique et les règles de la thermodynamique ne permettent pas d'expliquer les phénomènes se déroulant dans le monde de l'infiniment petit. Révélée dans les années 1920 par des physiciens ⁽²⁾ créatifs et audacieux, la mécanique quantique décrit le comportement de la matière à l'échelle

⁽¹⁾ MACRON Emmanuel, « Discours du président de la République sur la stratégie de défense et de dissuasion devant les stagiaires de la 27^e promotion de l'École de Guerre », 7 février 2020 (www.elysee.fr/).

⁽²⁾ Max Planck, Albert Einstein, Niels Bohr, Erwin Schrödinger, Werner Heisenberg, Max Born, etc.

subatomique. Sa formalisation constitua une révolution tant elle fut un défi pour l'entendement. Elle heurta le sens commun et suscita des visions parfois très divergentes ⁽³⁾. Ainsi, comme le disait un grand physicien enseignant les principes quantiques à ses élèves : « si vous m'avez compris, c'est que je n'ai pas été clair ⁽⁴⁾ ».

À l'échelle microscopique, les particules se comportent à la fois comme des corpuscules et des ondes. Les notions – contre-intuitives – de superposition, d'intrication, de tunnel quantique et de décohérence permettent d'appréhender l'essentiel des caractéristiques singulières du monde quantique.

La **superposition d'états** décrit l'aptitude d'une particule à exister dans plusieurs états au même moment. Il est possible de déterminer par le calcul la probabilité qu'elle se trouve dans un état précis. Pour le comprendre simplement, au lieu d'une particule, considérons une pièce de monnaie. Si la pièce repose à plat sur une table, il est possible de déterminer quelle face est visible. Imaginons maintenant la pièce qui tourne sur la tranche. Il n'est pas possible de définir si la face visible est pile ou face. Il semble que ce soit les deux en même temps.

Concernant le principe d'**intrication quantique**, il caractérise le fait que plusieurs particules peuvent être liées de telle manière qu'il est impossible de les décrire séparément même si elles sont physiquement séparées par une grande distance. En s'appuyant sur l'analogie avec une pièce de monnaie, l'intrication signifierait que faire tourner une pièce située à Paris ferait tourner une autre pièce à Tokyo exactement de la même manière, exactement au même moment et pour la même durée.

L'**effet tunnel**, quant à lui, traduit l'aptitude d'un objet quantique à franchir une barrière de potentiel sans posséder *a priori* l'énergie suffisante pour cela. Ce phénomène s'explique par le comportement ondulatoire de la particule qui peut se situer, de manière probabiliste, d'un côté et de l'autre de la barrière. Il trouve une application concrète dans certains microscopes (« à effet tunnel ») et dans certains appareils électroniques du quotidien (mémoire informatique, clé USB). En déplaçant les atomes un à un, il devient possible de les observer. De même, en utilisant un réservoir d'électrons, ils sont déplacés et constituent l'information (les bits dans la mémoire). Par ailleurs, ce principe est au cœur des nanosciences.

Ces propriétés quantiques disparaissent dès que l'on tente d'expliquer les phénomènes physiques observés au niveau macroscopique. Les objets quantiques doivent en effet être considérés comme interagissant fortement avec leur environnement. Il est possible de démontrer mathématiquement comment une interaction modifie les caractéristiques ondulatoires des différents états, les rendant ainsi incohérents les uns par

⁽³⁾ Einstein et Bohr se sont opposés avec force – mais toujours avec une grande bienveillance – sur la description de la physique quantique, incomplète pour le premier et complémentaire de la réalité pour le second. En exposant deux conceptions distinctes du monde physique, cette controverse revêtit une portée philosophique. Pour Einstein, qui rejette la description probabiliste, « Dieu ne joue pas aux dés ». PATY Michel, « Dieu joue-t-il au dé ? (La nature et les probabilités) », *Sciences et Avenir* n° 128, 2001, p. 6-7.

⁽⁴⁾ KLEIN Étienne, *Petit voyage dans le monde des quanta*, Flammarion, 2004, p. 14.

rapport aux autres. Cette démonstration forme la **théorie de la décohérence** ⁽⁵⁾ de tout système quantique. Elle met en évidence le caractère éphémère des états de superposition et d'intrication qui peuvent très vite disparaître sous l'effet d'interactions tant naturelles que provoquées par l'observation de l'objet quantique. Par exemple, la lumière ambiante ou celle émise par un dispositif de mesure contribue à la décohérence. La théorie permet de calculer avec précision le temps après lequel la probabilité des états superposés devient négligeable. La durée de superposition d'un système quantique doit donc être considérée comme limitée. Ainsi, la mesure d'une particule permet d'extraire l'information relative à son état au moment même de la mesure mais provoque également sa destruction.

En résumé, à l'échelle atomique, les particules se comportent comme des corpuscules et des ondes, elles sont dans plusieurs états à la fois selon des règles probabilistes. Elles peuvent être intimement liées entre elles sans aucun lien concret les reliant. Elles peuvent traverser des « murs » et, finalement, perdent toutes ces caractéristiques dès que soumises aux interactions extérieures. Cela étant posé, il est possible d'envisager tout le potentiel des principes quantiques pour réaliser, une fois surmontés quelques obstacles techniques, des actions à un niveau jusqu'alors hors d'accès.

Les applications et les freins technologiques

Les principes quantiques appliqués à des technologies permettent d'envisager de nouvelles méthodes de mesure, de traitement et de partage de données. Ces propriétés sont exploitées depuis les années 1950 avec la mise au point du laser, des transistors et des semi-conducteurs, ces derniers ayant permis de développer les ordinateurs. Aujourd'hui, il est possible d'aller encore plus loin dans l'utilisation des phénomènes quantiques en stockant, traitant et analysant un nouveau type de données. Là, réside la révolution en cours. Elle est de même nature que celle amenée par le traitement informatique de l'information.

L'extraordinaire précision des capteurs quantiques

L'exploitation des propriétés quantiques de certaines particules permet de détecter, de mesurer et de réaliser des images avec une extrême précision. Elles améliorent les capacités de systèmes existants tout en ouvrant la voie à de nouvelles fonctionnalités.

En utilisant des systèmes quantiques intriqués, il est possible de détecter d'infimes variations de l'environnement. Des dispositifs existent pour mesurer finement le temps, les champs gravitationnel et magnétique terrestres ainsi que les variations de lumière. Ils offrent, d'ores et déjà, des facteurs d'amélioration de 10 à 100 (et bientôt à 1 000) par rapport aux instruments de mesure classiques. Ainsi, au cœur de chaque

⁽⁵⁾ La théorie de la décohérence a été introduite par Heinz-Dieter Zeh en 1970. Elle a reçu ses premières confirmations expérimentales en 1996.

satellite *GPS* ⁽⁶⁾, se trouve une horloge, elle-même constituée d'atomes ⁽⁷⁾ superposés. Ce système quantique permet d'obtenir une référence temporelle extrêmement stable. Elle ne perd qu'une seconde en 100 millions d'années mais les scientifiques espèrent exploiter la technologie quantique pour faire encore mieux. De nouvelles générations d'horloges ne perdront qu'une seconde en un milliard d'années. Ce type de stabilité permet aux horloges d'être utilisées comme capteurs qui réagissent à de minuscules changements gravitationnels ou électromagnétiques. En intégrant de tels capteurs, il devient possible de développer des instruments de mesure comme des magnétomètres ⁽⁸⁾, des gravimètres ⁽⁹⁾, des accéléromètres ⁽¹⁰⁾ et des gyromètres ⁽¹¹⁾ d'une précision et d'une stabilité ⁽¹²⁾ accrues. Des entreprises, notamment européennes, commercialisent certains de ces dispositifs. Ils préfigurent de nouvelles solutions pour la navigation et la détection sous-marine ou celle de cavités souterraines.

L'imagerie constitue un autre domaine où l'apport des propriétés quantiques présente un fort potentiel d'amélioration. Des capteurs d'image utilisant l'effet tunnel, rendent possible l'observation à l'échelle moléculaire. Au niveau macroscopique, l'utilisation de photons intriqués de longueurs d'onde différentes permet, en réduisant les contraintes liées aux perturbations extérieures, de s'affranchir des conditions météorologiques pour observer une source lumineuse lointaine et ainsi réaliser une image à distance.

Enfin, un principe analogue utilisant des photons intriqués permet d'envisager la détection d'objet à distance. Une source émet un photon vers une cible. Lorsqu'il l'atteint, la modification de son état peut être observée à travers celui de son double. Tel un radar, la télédétection par laser (*LIDAR* ⁽¹³⁾) détecte un mobile distant. Toutefois, la mesure ne renseigne ni sur la forme ni sur la taille du mobile ; seule sa présence est détectée et des informations sur sa vitesse et sa distance peuvent être recueillies. L'imagerie et le radar quantique restent des domaines expérimentaux car les systèmes disponibles autorisent difficilement une utilisation hors d'un laboratoire.

L'avènement du calcul quantique

L'informatique classique utilise les « bits » pour produire le résultat de calculs. Les bits sont binaires car l'électronique s'appuie sur des composants traversés par une charge électrique ou pas. Ils prennent donc les valeurs discrètes de 1 ou 0. Les ordinateurs quantiques fonctionnent grâce à des *quantums bits* ou *qubits*. En combinant les

⁽⁶⁾ Le principe de fonctionnement d'un récepteur *GPS* (*Global Positioning System*) repose sur la mesure des écarts de temps entre les signaux reçus de différents satellites pour déterminer sa position.

⁽⁷⁾ Césium ou rubidium.

⁽⁸⁾ Le magnétomètre est un appareil qui sert à mesurer l'intensité et la direction d'un champ magnétique, Wikipédia.

⁽⁹⁾ Le gravimètre est un instrument de mesure destiné à quantifier le champ gravitationnel terrestre, Wikipédia.

⁽¹⁰⁾ L'accéléromètre est un capteur qui, fixé à un mobile, en mesure l'accélération linéaire, Wikipédia.

⁽¹¹⁾ Le gyromètre est un instrument qui mesure une vitesse angulaire. Une centrale inertielle qui élabore des informations de cap, d'attitude et de position utilise trois gyromètres et trois accéléromètres, Wikipédia.

⁽¹²⁾ Les capteurs quantiques n'ont quasiment pas besoin de réétalonnage. Ils peuvent ainsi effectuer des mesures pendant de longues périodes.

⁽¹³⁾ *Light Detection and Ranging*.

principes de superposition et d'intrication, ces systèmes quantiques sont capables d'être à la fois 0 et 1 en même temps, et d'interagir entre eux. Un *qubit* correspond à deux bits, il devient donc possible avec n *qubits* de coder 2^n bits. Ainsi, l'ordinateur quantique à 53 *qubits* que Google a déclaré avoir fait fonctionner le 23 octobre 2019 équivaut à une capacité de calcul de neuf millions de milliards (2^{53}) de bits. Ce dernier est parvenu à exécuter (avant de se détruire, voir *infra*) un calcul en 3 minutes et 20 secondes contre 10 000 ans pour l'ensemble des plus puissants calculateurs actuellement disponibles ⁽¹⁴⁾. De plus, l'intrication des *qubits* permet de réduire le nombre d'opérations logiques accélérant encore les calculs. Le traitement d'un grand nombre d'opérations en même temps devient possible alors qu'un processeur classique les réalise successivement. L'informatique quantique constitue une évolution exponentielle de la puissance de calcul dans un contexte où la loi de Moore ⁽¹⁵⁾ est sur le point de ne plus être valide. Le calcul quantique introduit de nouvelles méthodes qui permettront de résoudre des problèmes complexes inaccessibles pour les ordinateurs classiques actuels les plus avancés.

Cependant la conception de calculateurs quantiques pose deux défis majeurs. Le premier a trait à la conception des *qubits* et le second touche à leur manipulation. Pour fabriquer ces systèmes quantiques, plusieurs technologies existent ⁽¹⁶⁾. Dans l'état actuel de la recherche aucune d'entre elles ne domine. De grandes incertitudes subsistent quant à la technologie qui ouvrira la voie de la suprématie quantique. De même, pour réaliser des calculs, il est nécessaire de manipuler les *qubits* en modifiant leurs états ou en les intriquant. Pour cela, des impulsions laser ou électromagnétiques sont utilisées afin de former des portes quantiques en regroupant plusieurs *qubits*. Ces portes permettent de générer les fonctions essentielles au calcul quantique. Le *qubit* doit être isolé du « bruit » extérieur pour conserver sa cohérence. Cela exige de maintenir, lors des calculs, une très basse température (proche de 0 K, soit environ - 273 °C) et d'isoler les *qubits* de toute vibration et onde électromagnétique. Dans l'état actuel des capacités techniques, les perturbations extérieures ne peuvent être totalement évitées. Elles produisent, en conséquence, des décohérences quantiques et génèrent des erreurs dans les résultats obtenus. Il faut donc corriger ces erreurs en utilisant des architectures redondantes, ce qui exige de disposer d'un grand nombre de *qubits*. Par ailleurs, il est impossible de cloner ou dupliquer un *qubit*. Ce dernier est également détruit dès qu'il est lu ; il ne peut donc pas être lu deux fois. Cela signifie que la lecture du résultat doit se faire à la fin du calcul par le biais d'un algorithme quantique spécifique, très différent des algorithmes classiques. Cet algorithme ne peut être lancé qu'une seule fois compliquant ainsi sa mise au point. Par conséquent, les méthodes classiques de programmation, consistant à recopier la valeur d'une variable, sont inadaptées au calcul quantique.

⁽¹⁴⁾ LAROUSSERIE David, « Google annonce une percée majeure dans le calcul quantique », *Le Monde*, 23 octobre 2019.

⁽¹⁵⁾ Énoncée en 1965 par Gordon E. Moore, physicien américain cofondateur de la société Intel, cette loi empirique prédit le doublement de la puissance de calcul des ordinateurs à prix constant tous les 18 mois. Or, aujourd'hui, la taille des composants électroniques semble avoir atteint une limite.

⁽¹⁶⁾ Les supraconducteurs, les cavités de diamants et les ions piégés sont les technologies les plus avancées. La technologie à base de photons offre une plus grande facilité de manipulation des *qubits* mais la maîtrise de leurs interactions est complexe. Les spins d'électrons, les atomes neutres et les fermions de Majorana, enfin, sont des technologies exploratoires.

Face à ces difficultés de conception et de mise au point, la simulation de calculateur quantique offre une piste concrète d'amélioration du fonctionnement des ordinateurs classiques tout en constituant un laboratoire pour développer le calcul quantique. Avant l'avènement de l'ordinateur quantique, il reste de nombreux problèmes à résoudre. Cela crée une véritable incertitude sur le point d'aboutissement des recherches en cours ⁽¹⁷⁾.

La sécurité absolue des communications

De façon générale, la sécurité des communications est assurée par le chiffrement des données échangées et le partage de clés de codage. Les principes de la physique quantique ouvrent la voie à de nouveaux protocoles encore plus sûrs. En effet, les photons, largement utilisés dans les communications optiques, offrent des méthodes cryptographiques spécifiques au monde quantique. En utilisant les phénomènes de superposition et d'intrication, il est possible de faire circuler un message qui pourra être décodé uniquement par l'émetteur et le récepteur. De plus, s'il est intercepté pendant son transfert, la mesure réalisée par un tiers aura pour effet d'annihiler la superposition et l'intrication informant ainsi l'émetteur de l'intrusion tout en rendant le message indéchiffrable. Le piratage d'une communication quantique est détecté et détruit la clé de chiffrement, instantanément ; le message arrive à son destinataire mais ne peut être lu. Cela reproduit, dans une certaine mesure, le principe du sceau en cire utilisé au Moyen-Âge pour identifier l'émetteur d'un message écrit et vérifier que celui-ci n'a pas été lu pendant le trajet vers le récepteur.

Cependant, compte tenu de l'atténuation de la lumière dans les fibres optiques, les taux de transfert de données quantiques et les distances de transmission restent assez faibles. La transmission de messages entiers n'est donc pas pleinement exploitable. Pour réduire ces contraintes, une pratique consiste à envoyer uniquement la clé cryptographique selon les principes quantiques. La distribution de clés cryptographiques quantiques (*Quantum Key Distribution* ou *QKD*) permet de coder et de décoder un message chiffré de manière classique et de les transmettre *via* des réseaux de télécommunication optique existants. Pour améliorer les performances, il est nécessaire d'utiliser des dispositifs optiques refroidis, encore au stade expérimental. Il est par ailleurs possible de générer des nombres aléatoires quantiques pour constituer les clés de chiffrement.

Outre l'interception, le décodage ⁽¹⁸⁾ des clés de chiffrement classiques représente un risque d'autant plus grand que le calcul quantique pourrait fournir une puissance de calcul telle, qu'elles n'y résisteront pas. Là encore, la distribution de clés

⁽¹⁷⁾ « Rien ne permet d'affirmer que le développement d'ordinateurs quantiques sera possible d'ici 2030. », SECRETARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE (SGDSN), *Chocs futurs : Étude prospective à l'horizon 2030 : impacts des transformations et ruptures technologiques sur notre environnement stratégique et de sécurité*, 2017, p. 181 (www.sgdsn.gouv.fr/uploads/2017/04/sgdsn-document-prospectives-v5-bd.pdf).

⁽¹⁸⁾ Mathématicien américain, Peter Shor a développé en 1994 un algorithme quantique capable de résoudre le problème de factorisation, utilisé dans la majorité des systèmes de sécurité informatique. Il permettra à l'informatique quantique de décoder la plupart des clés de chiffrement classique.

Les enjeux de la physique quantique et les ruptures à anticiper

quantiques apporte une parade efficace. Toutefois, une alternative consiste à développer des algorithmes mathématiques résistant au calcul quantique. Ce dernier n'étant capable d'effectuer que des calculs à base de factorisation, certains problèmes mathématiques restent insolubles pour l'ordinateur quantique. De tels algorithmes constituent le fondement de la cryptographie *post*-quantique.

Des défis techniques à relever

La conception et la mise au point de dispositifs utilisant des systèmes quantiques se heurtent à de nombreux obstacles. En effet, la nature complexe et évanescence des propriétés quantiques rend tout particulièrement difficile le développement de technologies les employant. Un système quantique est extrêmement sensible aux perturbations extérieures bien plus que les systèmes électroniques classiques. Des variations mécaniques, thermiques ou encore électromagnétiques perturbent les objets quantiques et génèrent des erreurs qu'il est nécessaire de corriger. Cela freine, notamment, le développement de l'informatique quantique. Pour pallier ces contraintes, des dispositifs complexes souvent volumineux et lourds doivent accompagner les systèmes quantiques. En outre, des sources d'énergie de grande capacité sont requises pour faire fonctionner ces ensembles. Ainsi, la plupart des systèmes ne fonctionnent que dans l'environnement d'un laboratoire. Dans ce contexte, une large utilisation des technologies quantiques reste une perspective plus ou moins lointaine, 2030 semblant marquer un tournant pour certains spécialistes ⁽¹⁹⁾. Enfin, le fonctionnement singulier des systèmes quantique requiert de développer des algorithmes et une couche logicielle spécifiques dont la conception porte son propre lot de défis.

La recherche quantique ressemble donc plus à un marathon qu'à un sprint. Les États qui dominent sur la scène économique mondiale ont pris la mesure du caractère stratégique que revêt aujourd'hui la recherche quantique. Ils se sont résolument lancés dans cette course afin de tirer un avantage décisif des technologies issues de l'univers quantique.

L'écosystème mondial, européen et français du quantique

Aux États-Unis, le Congrès a adopté, en décembre 2018, le *National Quantum Initiative Act*. Il prévoit une forte croissance du secteur quantique et identifie le besoin de chercheurs à former. Il a été décidé de stimuler la recherche avec un premier plan quinquennal de plus d'un milliard de dollars. En parallèle, le *National Institute of Standards and Technology (NIST)* est chargé de piloter et de contrôler les sujets relatifs à la définition des normes et à la standardisation des applications quantiques ⁽²⁰⁾. L'écosystème quantique américain regroupe ⁽²¹⁾ 40 *start-up*, 50 fonds de capital-risque,

⁽¹⁹⁾ « McKinsey estime qu'il existera entre 2 000 et 5 000 ordinateurs quantiques dans le monde d'ici 2030 » in BERGOUNHOX Julien, « L'informatique quantique pèsera 1 000 milliards de dollars en 2035 », *L'Usine Digitale*, 9 mars 2020 (www.usine-digitale.fr/).

⁽²⁰⁾ Cf. NIST, « Quantum information science » (www.nist.gov/topics/quantum-information-science).

⁽²¹⁾ FORTEZA Paula (dir.), *Quantique : le virage technologique que la France ne ratera pas*, rapport parlementaire, janvier 2020, 64 pages.

4 grandes sociétés industrielles (Google, IBM, Microsoft et Intel). À cela s'ajoutent les efforts considérables consentis par le secteur de la défense et orchestrés par la *DARPA* ⁽²²⁾. Les États-Unis sont à la pointe de la recherche quantique, notamment dans le domaine de l'ordinateur quantique. Ainsi, IBM, Microsoft et Google se livrent une compétition effrénée pour atteindre en premier la suprématie quantique.

Concernant la **Chine**, la recherche quantique représente une priorité stratégique assumée qui doit contribuer à l'objectif général de devenir la première puissance du monde en 2049. Le quantique est, en effet, érigé en priorité du 13^e plan quinquennal de la Chine (2016-2020) ⁽²³⁾. Ainsi, les domaines de la communication, de la détection et du calcul quantique sont l'objet d'expérimentations de grande ampleur. La Chine est particulièrement active dans le domaine de la distribution quantique de clés de chiffrement (*QKD*), en témoignent le nombre de brevets déposés ⁽²⁴⁾ et les expérimentations de démonstrateurs terrestres et spatiaux. En 2016, le programme *QUESS* (*Quantum Experiments at Space Scale*) établit une ligne de communication quantique avec le satellite *Micius*, reliant ainsi Pékin et Vienne pour diffuser des clés de chiffrement d'images et d'une conversation vidéo. Le satellite a également permis de transmettre, à l'aide de lasers, des paires de photons intriqués entre deux stations sol distantes de 1 200 km ⁽²⁵⁾. Une liaison quantique par fibre optique entre Pékin et Shanghai (2 000 km) a par ailleurs été ouverte en 2017. L'objectif annoncé consiste à disposer d'un réseau mondial de communication quantique à des fins civiles et militaires à l'horizon 2030, posant ainsi les bases d'un *Internet* quantique chinois ⁽²⁶⁾.

Dans un autre domaine stratégique, des chercheurs chinois ⁽²⁷⁾ annoncent l'avènement du premier prototype d'ordinateur quantique constitué de composants exclusivement chinois d'ici fin 2020. Ils considèrent que la maîtrise de cette technologie donnera un avantage identique à celui de la machine à vapeur sur la voiture à cheval. En matière de recherche fondamentale, la Chine semble en passe de rattraper son retard sur les États-Unis.

Concernant les capteurs quantiques, la Chine communique et met en scène son avance en matière de détection. Elle se serait ainsi dotée d'un radar quantique fonctionnel ⁽²⁸⁾ rendant obsolète le concept de furtivité des vecteurs aériens. La compétition quantique dans laquelle sont engagés Américains et Chinois semble se jouer également sur le terrain de la communication.

⁽²²⁾ *DARPA* : *Defense Advanced Research Projects Agency*. Aucune information ne filtre sur les budgets et les recherches dédiés au quantique au sein du secteur de la défense.

⁽²³⁾ WANG Yiwei, « XIII^e Plan quinquennal : des opportunités pour l'Europe », *La Chine au présent*, 8 mars 2016 (www.chinatoday.com.cn/french/picnews/article/2016-03/08/content_716714.htm).

⁽²⁴⁾ « In 2018, China registered 517 quantum communications and cryptography patents; the US registered 117 and Europe only 31 » in BURTON Charlie, « How China become a subatomic superpower with quantum technology », *GQ UK edition*, 2 août 2019 (www.gq-magazine.co.uk/article/quantum-technology-china).

⁽²⁵⁾ CASTELVECCHI Davide, « China's quantum satellite clears major hurdle on way to ultrasecure communications », *Nature*, 15 juin 2017.

⁽²⁶⁾ KHALATBARI Azar, « L'*Internet* quantique sera chinois », *Sciences et Avenir*, 13 août 2017 (www.sciencesetavenir.fr/).

⁽²⁷⁾ « La Chine intensifie la compétition quantique avec les États-Unis », *French.China.org*, 11 novembre 2019 (http://french.china.org.cn/business/txt/2019-11/11/content_75396319.htm).

⁽²⁸⁾ IKONICOFF Román, « Les Chinois auraient construit un "radar quantique" », *Science&Vie*, 14 juillet 2018.

Les enjeux de la physique quantique et les ruptures à anticiper

Depuis 2010, de nombreux brevets liés aux capteurs et à l'informatique quantiques sont par ailleurs déposés par la Chine. Le budget consacré à la recherche quantique est estimé à 2 milliards d'euros pour les cinq années du plan en cours ⁽²⁹⁾. Toutefois d'autres sources évoquent plus de 10 Md€ ⁽³⁰⁾. Par ailleurs le secteur privé et notamment certaines entreprises du numérique telles Baidu, Alibaba et Huawei Technologies consacrent des budgets considérables à la recherche et au développement des technologies quantiques ⁽³¹⁾.

Autre compétiteur, la **Russie** laisse filtrer peu d'informations sur sa stratégie dans le domaine quantique, mais nul doute que les technologies quantiques, potentiellement disruptives, intéressent le pouvoir russe. Ce dernier peut pour cela compter sur des mathématiciens et physiciens aux compétences reconnues. Le gouvernement a annoncé en décembre 2019 qu'il consacrerait 50 Md de roubles (600 millions €) à la recherche quantique sur les cinq prochaines années ⁽³²⁾ pour ainsi rester dans la course.

En **Europe**, l'Union européenne a lancé en 2018 le programme ⁽³³⁾ *Quantum Technologies flagship* doté d'un milliard d'euros sur dix ans. Organisé autour de quatre grands domaines ⁽³⁴⁾, le programme vise à financer les recherches et à fédérer les efforts des États-membres. La vision à long terme consiste au déploiement d'un *Internet* quantique qui relierait, en Europe, les capteurs, ordinateurs et simulateurs quantiques dans un large partage des ressources. Parallèlement, des plans nationaux regroupent au sein de partenariats des acteurs académiques et des sociétés telles que Microsoft, IBM et Intel. C'est le cas en Allemagne, au Royaume-Uni, aux Pays-Bas et également en France.

La **France** bénéficie d'un écosystème cohérent. Il est structuré autour de centres de recherche ⁽³⁵⁾ de grande qualité, de quelques groupes industriels ⁽³⁶⁾ volontaires et de *start-up* ⁽³⁷⁾ performantes. Grands groupes et *start-up* français commercialisent d'ores et déjà des applications quantiques avec succès. À titre d'exemple, Atos propose la seule plateforme de simulation quantique du marché ⁽³⁸⁾ et investit fortement dans

⁽²⁹⁾ VILLANY Cédric, « Les technologies quantiques introduction et enjeux », *Les notes scientifiques de l'Office* n° 13, Office parlementaire d'évaluation des choix scientifiques et technologiques, mars 2019, 7 pages (<http://questions.assemblee-nationale.fr/>).

⁽³⁰⁾ Dans son rapport annuel, *The Military Balance 2019*, l'*International Institute for Strategic Studies (IISS)* évoque le projet chinois de construction d'un centre de recherche pour les sciences quantiques de l'information à Hefei dans la province de Anhui (région au sud de Pékin et à l'ouest de Shanghai), un projet à 10 Md\$.

⁽³¹⁾ LACROIX Hélène (D^r), « Les BATX chinois dans la course à l'informatique quantique : de la recherche au capital-risque en passant par la pharmacie et la fintech », *The Red (Team) Analysis Society*, 17 juillet 2019 (www.redanalysis.org/fr/2019/07/17/chinese-batx-race-to-quantum/)

⁽³²⁾ SCHIERMEIER Quirin, « Russia joins race to make quantum dreams a reality », *Nature*, 17 décembre 2019 (www.nature.com/articles/d41586-019-03855-z).

⁽³³⁾ Cf. EUROPEAN COMMISSION, « Shaping Europe's digital future – Policy, Quantum Technologies Flagship » (<https://ec.europa.eu/digital-single-market/en/quantum-technologies>).

⁽³⁴⁾ Le calcul quantique ; la simulation des interactions quantiques à l'échelle moléculaire ; les communications quantiques ; et les capteurs quantiques.

⁽³⁵⁾ Centre national de la recherche scientifique (CNRS), Commissariat à l'énergie atomique et aux énergies alternatives (CEA), Office national d'études et de recherches aérospatiales (Onéra), Institut national de recherche en sciences et technologies du numérique (Inria), Université Paris-Saclay, etc.

⁽³⁶⁾ Thales, Atos, etc.

⁽³⁷⁾ Muquans, Quandela, Pasqal, VeryQloud, Aurea Technology, etc.

⁽³⁸⁾ ATOS Quantum Learning Machine.

le développement d'algorithmes quantiques, véritable système d'exploitation des ordinateurs quantiques. Atos s'est également lancé dans la fabrication d'un accélérateur quantique de type *Noisy Intermediate-Scale Quantum (NISQ)* pour 2023. Pour sa part, la *start-up* Muquans a développé des horloges atomiques de très haute précision ainsi que des gravimètres quantiques pleinement opérationnels. Enfin, les algorithmes de calcul ainsi que certaines technologies habilitantes comme la cryogénie ou l'ultravide sont des domaines bien maîtrisés dans l'Hexagone. En matière de financement, un fonds de capital-risque « Quantonation » spécialisé dans les technologies quantiques a été créé en 2018 ⁽³⁹⁾. Il a vocation à lever 40 M€ pour soutenir sur quatre ans les *start-up* à leur début. Il faut également souligner l'engagement de la banque publique d'investissement Bpifrance à épauler l'entrepreneuriat français dans ce secteur.

Par ailleurs, le 9 janvier 2020, les conclusions du rapport quantique rédigé par la députée Paula Forteza ont été présentées ⁽⁴⁰⁾. Ce rapport met en lumière six recommandations stratégiques autour du calcul quantique, du développement de technologies, du développement des usages, de l'innovation, de la sécurité économique et de la gouvernance. À cette occasion, un groupe de travail composé de représentants de l'État, de chercheurs et de financiers a été mis en place. Il est chargé de produire une feuille de route avant l'été 2020. Il devrait permettre une déclinaison dans la loi pluriannuelle de programmation de la recherche et le lancement d'un véritable plan quantique français.

Pour ce qui concerne le ministère des Armées, l'Agence de l'innovation de défense (AID) est en première ligne pour stimuler la recherche et éveiller les consciences. Son directeur, Emmanuel Chiva, ne ménage pas ses efforts dans ce sens. Il rappelle que « rater la révolution quantique nous empêche de dormir » ⁽⁴¹⁾. Le ministère des Armées finance 230 nouvelles thèses sur le quantique chaque année. Selon M. Chiva, « la ministre Florence Parly a demandé à l'AID de lancer, d'ici mi-2020, un appel à projet pour développer les meilleurs capteurs quantiques possible avec l'Agence nationale de la recherche ».

L'Europe, dans son ensemble, consacre des budgets qui lui permettent de nourrir de réelles ambitions. Il est toutefois essentiel d'unir les efforts et de sélectionner les domaines de recherches à privilégier. En revanche, les Nations européennes pourront difficilement se doter des infrastructures de recherche tant les investissements requis sont considérables. Cette situation a pour conséquence regrettable le départ de chercheurs européens vers les centres de recherches américains où ils trouvent des conditions d'expérimentation optimales.

⁽³⁹⁾ Rubrique « About » du site officiel de Quantonation (www.quantonation.com/#about).

⁽⁴⁰⁾ FORTEZA Paula, HERTEMAN Jean-Paul et KERENIDIS Iordanis, *Quantique : le virage technologique que ne ratera pas la France – 37 propositions pour une stratégie nationale ambitieuse*, mission parlementaire, 2020, 64 pages (https://forteza.fr/wp-content/uploads/2020/01/A5_Rapport-quantique-public-BD.pdf).

⁽⁴¹⁾ Séminaire *Deep Tech Week* réunissant l'écosystème français du quantique au sein des locaux de Bpifrance, 11 mars 2020. Cf. POIREAULT Kévin, « Deep Tech Week : l'écosystème français du quantique veut accélérer la R&D », *Industrie & Technologie*, 11 mars 2020 (www.industrie-techno.com/).

Des ruptures pour la défense

Considérant le potentiel des technologies quantiques et l'engouement des États pour s'en doter, nul doute que la seconde révolution quantique est en cours. Ces technologies, de nature disruptive ⁽⁴²⁾, conféreront un avantage stratégique à ceux qui les maîtriseront, ce qui induit d'indéniables enjeux d'autonomie, de souveraineté et de croissance économique. Dans le domaine de la sécurité et de la défense, elles sont de nature à générer des ruptures, c'est-à-dire qu'elles autoriseront de nouveaux modes d'actions, ou bien elles amélioreront des modes d'actions existants. Dans les deux cas, elles conféreront une avance significative et un avantage opérationnel décisif. Les applications quantiques recèlent le potentiel pour donner une supériorité opérationnelle décisive à une force militaire. L'utilisation des propriétés quantiques provoquera un bouleversement des méthodes et des capacités militaires dans des domaines aussi variés que les communications, le renseignement, la détection, la navigation autonome ainsi que l'intelligence artificielle (IA).

Vers des communications ultra-sécurisées

La sécurité des systèmes d'information et des données est un élément essentiel dans la protection et la défense d'une Nation. Les technologies quantiques portent la promesse de communications ultra-sécurisées. La maturité des applications de distribution de clés de chiffrement laisse entrevoir, à moyen terme, des solutions pour les échanges à courtes distances, de l'ordre de plusieurs kilomètres. Pour les communications à longues distances, même si des expérimentations impliquant des liaisons satellitaires ont été conduites, un usage à grande échelle n'est pas envisageable avant au moins une décennie. Ces nouvelles technologies conduiront à repenser la façon de communiquer et de relier des systèmes entre eux, et ce de manière autonome. En utilisant la téléportation quantique ⁽⁴³⁾, il sera possible de relier en permanence différentes parties d'un même système ainsi que plusieurs systèmes entre eux. Ces nouveaux moyens de communiquer remettront en question les architectures de communication en vigueur actuellement. Elles apporteront, en outre, des solutions encore plus sûres pour les communications sensibles telles que celles liées à la dissuasion nucléaire et, plus particulièrement, à l'acheminement de l'ordre présidentiel de tir.

Un saut quantique pour le renseignement

Les capteurs quantiques capables de révéler d'infimes variations des spectres lumineux et électromagnétiques ouvriront le chemin à des applications qui décupleront certaines capacités de renseignement. Des images lointaines prises dans des conditions météorologiques défavorables ainsi que des interceptions électromagnétiques

⁽⁴²⁾ « Although economical applications and widespread use are still years away, there is little doubt that they [quantum technologies] will have disruptive effect when they are employed at scale », IISS, *The Military Balance 2019*, chapter one, part III « *Quantum Computing and Defence* », février 2019.

⁽⁴³⁾ Protocole de communications consistant à transférer l'état quantique d'un système vers un autre système similaire et séparé spatialement du premier en mettant à profit l'intrication quantique, Wikipédia.

seront possibles pour tout système doté de tels capteurs. Compte tenu de l'importance du renseignement au niveau tactique comme stratégique, celui qui maîtrisera ces technologies aura un avantage considérable. De même, le calcul quantique augmentera la puissance de calcul au service du traitement de masse de données collectées toujours plus nombreuses.

L'apport du quantique à la détection dans les airs, sous la terre et les océans

De la même manière, l'emploi de capteurs quantiques fera qu'il sera plus complexe de se dissimuler dans les airs, sur et sous la terre mais aussi dans les océans. Des usages civils de gravimètres quantiques, permettent déjà l'exploration souterraine et la détection de cavités enfermant des hydrocarbures ⁽⁴⁴⁾. Une miniaturisation de ces technologies permettrait de détecter des installations souterraines ennemies. Dans les domaines de la surveillance aérienne et sous-marine, de nombreux obstacles techniques restent encore à lever avant d'aboutir à un usage généralisé du radar quantique. En revanche, des capteurs quantiques encore immatures peuvent constituer des briques technologiques intégrées aux systèmes de détection classiques afin d'en améliorer les performances et de poursuivre leur développement. Un radar quantique ou un *LIDAR* génère moins d'émissions qu'un radar classique pour obtenir le même résultat ; on obtient ainsi une meilleure précision aux mêmes niveaux de puissance. Ce radar peut également fonctionner avec un très faible niveau de puissance le rendant plus discret et donc plus difficile à contrer par un adversaire. Ce principe est de nature à révolutionner la guerre sous-marine.

La détection quantique doit, par conséquent, conduire à revisiter le concept de furtivité des vecteurs aériens ou celui de la dilution des sous-marins dans leur milieu respectif. Furtivité contre quels systèmes de détection ? Il sera nécessaire de penser la furtivité davantage en termes de leurrage et de camouflage plutôt que d'indétectabilité. Pour cela, des technologies quantiques permettant la maîtrise des interactions lumière-matière seront très utiles. Au bilan, des besoins et des cas d'usage doivent être définis afin de guider la recherche et le développement d'applications.

La navigation quantique autonome

Les capteurs gravitationnels quantiques peuvent également être utilisés comme gyroscopes, jetant les bases de systèmes de navigation inertielle très précis qui s'affranchissent de signaux comme ceux du *GPS* ou de *Galileo*, sensibles au brouillage. Même s'il existe des moyens efficaces de navigation classique, l'utilisation de systèmes quantiques les rend encore plus précis et ce, dans un éventail d'emploi élargi. Ils offrent la redondance indispensable à l'efficacité opérationnelle. Ils apporteront également un plus grand niveau de sécurité et de sûreté aux systèmes autonomes pour les intégrer dans des espaces communs.

⁽⁴⁴⁾ Muqans, « Absolute Quantum Gravimeter. Applications—Exploration and management of underground resources: Hydrocarbon and mineral exploration » (www.muqans.com/product/absolute-quantum-gravimeter).

Le traitement massif de données

De nombreuses incertitudes demeurent quant à la capacité de développer un ordinateur quantique d'emploi courant. Son développement relève parfois davantage du battage médiatique que de la réalité. On peut toutefois se souvenir de la taille et de la puissance des premiers ordinateurs et les comparer avec celles d'un *smartphone* que beaucoup possèdent désormais au fond de leur poche. Il semble donc raisonnable de penser qu'à l'horizon de vingt ans, le calcul quantique fournira une puissance de calcul encore jamais atteinte. En attendant l'avènement de l'ordinateur quantique, des capacités de calcul quantique intermédiaires seront progressivement disponibles et offriront de nouvelles possibilités de modéliser, d'optimiser et de simuler des systèmes complexes. Les simulateurs quantiques permettent d'ores et déjà d'accélérer les calculs de supercalculateurs classiques tout en poursuivant le développement de l'ordinateur quantique. Leur aptitude à résoudre des problèmes complexes permettra notamment de développer des applications d'aide à la décision. Il sera possible, par exemple, d'optimiser des flux logistiques sur un théâtre d'opérations ou bien de simuler des plans d'opérations. À terme, le calcul quantique permettra le traitement massif de données, dans un temps extrêmement court, rendant ainsi l'IA et les systèmes autonomes pleinement fonctionnels. L'ordinateur quantique constitue le levier indispensable au développement futur de ces nouvelles technologies. En matière de sécurité des communications, le risque que fait peser l'ordinateur quantique universel sur la cryptographie classique doit conduire à anticiper une parade sans tarder.

Enfin, les perspectives offertes par le calcul quantique ne sont pas toutes définies. Des applications ou cas d'usage inattendus ne manqueront pas de surgir, chacun de nature transformationnelle. Pour reprendre l'analogie avec l'informatique classique, rare sont ceux qui avaient anticipé l'invention du *smartphone* et ces applications. Il a pourtant fondamentalement changé, à l'échelle planétaire, la manière de communiquer.

Même si la pleine promesse des technologies quantiques en matière de sécurité et de défense reste inconnue, son pouvoir disruptif est indéniable et exige de rester dans la course à défaut de la mener.

Anticiper les ruptures et rester dans la course

Alors que les Européens sont toujours en train de s'adapter à la révolution numérique, la tentation est forte de se contenter d'injonctions incantatoires au sujet d'une révolution quantique qui promet d'être tout aussi disruptive, voire davantage. Les Nations européennes, individuellement ou collectivement, ne parviendront à suivre ni le rythme imprimé, ni le niveau de moyens engagés par les États-Unis et la Chine dans le développement des technologies quantiques. Le risque de décrochage est grand et l'exemple de la 5G ou encore l'absence d'équivalents européens des Gafam ⁽⁴⁵⁾

⁽⁴⁵⁾ Google, Amazon, Facebook, Apple et Microsoft (États-Unis).

ou des BATX⁽⁴⁶⁾ n'est pas de nature à rassurer. Il semble donc indispensable de donner corps à l'initiative de l'UE (*Quantum Technologies flagship program*) en fédérant les efforts consentis par les États-membres. Pour cela, la priorisation des domaines de recherche doit être poursuivie et précisée. Outre le calcul quantique et le développement d'un *Internet* quantique à l'horizon 2035-2040, le fort potentiel des capteurs quantiques dans les années à venir doit être exploité. Ce secteur est à suivre de près, notamment pour la nature duale de ses applications, civiles et militaires.

Autre point de vigilance, celui lié aux sujets de normalisation et de standardisation. Le nombre considérable de brevets américains et chinois doit être le signal pour réagir. L'enjeu est double : il s'agit de préserver une autonomie dans des domaines stratégiques et également de maintenir l'interopérabilité avec l'allié américain. Les technologies de cryptographie quantique comme les algorithmes indispensables aux ordinateurs quantiques contribueront à établir la norme dans le domaine de la communication et du calcul. Enfin, la maîtrise des technologies habilitantes permettra également de façonner le standard des applications quantiques.

Concernant la France, et plus spécifiquement le ministère des Armées, il apparaît essentiel de se doter d'un plan d'actions « technologies quantiques » pragmatique qui doit permettre aux armées d'intégrer cette révolution technologique à l'horizon 2040. Déclinaison de la feuille de route interministérielle, ce plan d'action pourrait s'articuler autour de quatre grands thèmes : la recherche, le domaine capacitaire, les doctrines et la coopération internationale.

Sur le plan de la **recherche scientifique**, le ministère des Armées doit poursuivre et densifier ses relations avec les centres de recherche nationaux ainsi que le monde industriel. Pour ce faire, l'AID doit être le catalyseur et proposer, en lien étroit avec les armées, un catalogue de cas d'usage. Ce dernier regrouperait les besoins militaires futurs pour lesquels les technologies quantiques apporteraient une solution et un niveau de performance susceptibles de donner l'avantage sur le terrain.

Dans le **domaine capacitaire**, les futurs programmes d'équipement devront intégrer un volet en lien avec les technologies quantiques. Il s'agit de définir quelle part prendront ces technologies dans les futurs programmes tels que le *SCAF*⁽⁴⁷⁾, le *MGCS*⁽⁴⁸⁾, le porte-avions nouvelle génération et le Sous-marin nucléaire lanceur d'engins (SNLE) de 3^e génération. Ces nouvelles capacités, intégreront-elles nativement des systèmes quantiques pour communiquer, détecter et naviguer ? Ou bien le choix, portera-t-il sur une intégration après la mise en service, à mi-vie, ou sur l'exclusion des technologies quantiques ? Autant de sujets qui méritent d'être étudiés sans délai pour des systèmes qui équiperont les forces armées à l'horizon 2040.

De même, l'apport prévisible des technologies quantiques doit conduire à une profonde **réflexion doctrinale et conceptuelle**. Les efforts déployés par la Chine et la

⁽⁴⁶⁾ Baidu, Alibaba, Tencent et Xiaomi (Chine).

⁽⁴⁷⁾ *Système aérien de combat du futur*, projet franco-allemand d'un ensemble de systèmes d'arme aérien connectés entre eux, rejoint par l'Espagne.

⁽⁴⁸⁾ *Main Ground Combat System*, char de combat visant à remplacer les *Leclerc* français et les *Leopard 2* allemands.

Russie laissent entrevoir la fin de la suprématie occidentale. Les interventions se feront dans des milieux de plus en plus contestés. L'enjeu consiste à préserver un avantage stratégique pour ne pas subir le tempo opérationnel d'un adversaire qui maîtriserait des technologies de rupture. Il s'agit donc de repenser la manière de combattre à l'aune du quantique car, comme le souligne le général Lecointre ⁽⁴⁹⁾, c'est l'accélération du tempo décisionnel qui assurera la supériorité opérationnelle. Aussi, les architectures de communication, de commandement et de contrôle seront à réinventer. Comment relier les systèmes de force entre eux ? Quelle sera la place de l'autonomie lorsque la puissance de calcul permettra la gestion massive de données dans un laps de temps très court ? Comment sera présentée la situation d'ensemble aux décideurs politiques et militaires et quels seront les outils d'aide à décision ? Autant de questions qui nécessitent des études approfondies suivant différents scénarios de montée en puissance des technologies quantiques. Également, dans des domaines tels que le cyberspace ou l'espace exo-atmosphérique ⁽⁵⁰⁾, pour lesquels les armées se dotent de plans ambitieux, l'apport potentiel du quantique reste une question ouverte qui inquiète certaines autorités ⁽⁵¹⁾. Les technologies quantiques contribueront très probablement à la montée en gamme des opérations dans ces deux domaines. Elles permettront même de donner corps aux opérations multidomaines. Enfin, la dissuasion nucléaire devra passer au filtre quantique : quels progrès sont susceptibles d'apporter les technologies quantiques dans le domaine de la sécurisation des communications ? Quelles menaces fait peser la détection quantique sur les vecteurs de la dissuasion ?

L'ensemble de ces sujets liés à la recherche, au développement capacitaire et à la doctrine ne peut se concevoir de manière isolée. Il doit largement alimenter la **coopération internationale** et particulièrement européenne. Aussi, le thème de l'interopérabilité doit-il être au cœur des préoccupations. Elle est indispensable et le fruit d'efforts constants. La standardisation et la normalisation des techniques qui seront utilisées constituent par conséquent autant d'enjeux majeurs. Le travail de l'Organisation du Traité de l'Atlantique Nord (Otan) en matière d'interopérabilité est un atout essentiel et la présence du Commandement allié de la transformation (ACT) à Norfolk sur le sol américain doit permettre de suivre ces sujets tout en renforçant le lien avec les initiatives américaines dans le domaine quantique.

⁽⁴⁹⁾ « La numérisation de l'espace de bataille est une réalité ancienne qui permet notamment d'avoir la vision la plus claire possible de la totalité du champ de bataille, des positions des alliés comme des ennemis, des niveaux de soutien logistique nécessaires à chacune des formations, et qui permet de détenir une supériorité opérationnelle au regard d'un aspect qui nous semble aujourd'hui majeur, à savoir l'accélération du tempo décisionnel. C'est cette accélération qui, dans un conflit de haute intensité, nous semble être de nature à assurer la supériorité opérationnelle. » COMMISSION DE DÉFENSE NATIONALE ET DES FORCES ARMÉES, « Audition du général François Lecointre, chef d'état-major des armées, sur le projet de loi de programmation militaire », 21 février 2018, Assemblée nationale (www.assemblee-nationale.fr/).

⁽⁵⁰⁾ « L'échiquier spatial international est en voie de bouleversement du fait des progrès quantiques des principales puissances et du rattrapage rapide des puissances spatiales de second rang. » ZAJEC Olivier, « Le paysage spatial militaire international : un bouleversement multipolaire entre ruptures technologiques et continuité de puissance », *Les Cahiers de la RDN (L'air et l'Espace enjeux de souveraineté et de liberté d'action de la France)* (www.defnat.com/).

⁽⁵¹⁾ « Dans le champ cyber, s'il est une technologie qui fera la différence, c'est l'informatique quantique, car elle changera totalement la donne en termes de puissance de calcul et produira des effets aussi importants que l'arrivée de la poudre sur le champ de bataille. » propos du député Thomas Gassilloud. Cf. COMMISSION DE LA DÉFENSE NATIONALE ET DES FORCES ARMÉES, « Audition de M. Louis Gautier, secrétaire général de la défense et de la sécurité nationale, sur le projet de loi de programmation militaire et sur la revue stratégique de cyberdéfense », 21 février 2018, Assemblée nationale (www.assemblee-nationale.fr/).

Les enjeux de la physique quantique et les ruptures à anticiper



Les technologies utilisant les principes quantiques auront, à n'en pas douter, un impact majeur sur la défense en permettant de sécuriser certaines communications, de casser les codes d'autres, de détecter des systèmes dans l'air, sous la terre et sous les mers ainsi qu'en facilitant la prise de décision. Il est cependant impossible de prédire ni la magnitude de ces ruptures, ni le calendrier de leur mise en œuvre. Cependant, face aux enjeux que cela représente, il est primordial de rester dans la course et de contribuer, d'une façon ou d'une autre, au développement de technologies qui revêtent bien souvent un caractère dual. Pour les armées, réfléchir à des cas d'usage est une étape indispensable. Cette démarche doit permettre de guider la recherche et, surtout, de penser le format et l'organisation des armées de demain. Le contexte stratégique sera différent. Il sera marqué par la fin de la supériorité occidentale et obligera à agir dans des milieux contestés. Les technologies quantiques mais aussi l'IA ou encore les systèmes de systèmes mêlant combattants et plateformes autonomes doivent susciter une profonde réflexion sur ce que seront les armées en 2040 : quels contrats, quel format, quels concepts d'emploi et quels équipements ? Là se trouve, peut-être, la véritable révolution qu'il convient d'anticiper.

Éléments de bibliographie

BUCHHOLZ Scott, MARIANI Joe, ROUTH Adam, KEYAL Akash et KISHNANI Panjkaj, « The realist's guide to quantum technology and national security », Deloitte Insights, 2020, 19 pages (www2.deloitte.com/).

FORTEZA Paula, HERTEMAN Jean-Paul et KERENIDIS Iordanis, *Quantique : le virage technologique que ne ratera pas la France – 37 propositions pour une stratégie nationale ambitieuse*, mission parlementaire, 2020, 64 pages (https://forteza.fr/wp-content/uploads/2020/01/A5_Rapport-quantique-public-BD.pdf).

INTERNATIONAL INSTITUTE FOR STRATEGIC STUDIES (IISS), *The Military Balance 2019*, février 2019, 504 pages.

KLEIN Étienne, *Petit voyage dans le monde des quanta*, Flammarion, 2004, 190 pages.

PLUCHET Blandine, *La Physique quantique pour les nuls*, First Edition, 2018, 264 pages.

SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE (SGDSN), *Chocs futurs : Étude prospective à l'horizon 2030 : impacts des transformations et ruptures technologiques sur notre environnement stratégique et de sécurité*, 2017, 208 pages (www.sgdsn.gouv.fr/uploads/2017/04/sgdsn-document-prospectives-v5-bd.pdf).

SHRÖDINGER Erwin, *Physique quantique et représentation du monde*, Éditions du Seuil, 1992, 185 pages.

STARBUST, *Quantique, pour quoi faire ? Étude de marché*, 11 juin 2019, Innovation Défense Lab, 37 pages.

VILLANY Cédric, « Les technologies quantiques introduction et enjeux », *Les notes scientifiques de l'Office n° 13*, Office parlementaire d'évaluation des choix scientifiques et technologiques, mars 2019, 7 pages (<http://questions.assemblee-nationale.fr/>).

ZAJEC Olivier, « Le paysage spatial militaire international : un bouleversement multipolaire entre ruptures technologiques et continuité de puissance », *Les Cahiers de la RDN (L'air et l'Espace enjeux de souveraineté et de liberté d'action de la France)* (www.defnat.com/e-RDN/vue-article-cahier.php?carticle=80).