

Technologies quantiques dans la défense et la sécurité du renseignement

BESSMA MOMANI ET MICHELE MOSCA

Bessma Momani est vice-rectrice associée, International et professeure titulaire au département de science politique de l'Université de Waterloo. Elle est également agrégée supérieure au Centre pour l'innovation dans la gouvernance internationale et boursière Fulbright. Elle assume les fonctions de gouverneure au conseil d'administration du Centre de recherches pour le développement international.

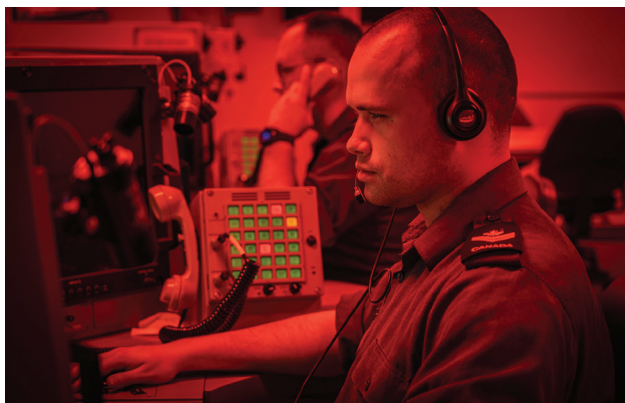
Michele Mosca est cofondateur de l'Institute for Quantum Computing de l'Université de Waterloo, professeur au département de combinatoire et d'optimisation de la Faculté de mathématiques et membre fondateur de l'Institut Périphère de physique théorique de Waterloo. Il était directeur fondateur de CryptoWorks21, un programme de formation en cryptographie à résistance quantique. Il a cofondé evolutionQ Inc. pour aider les organisations à faire évoluer leurs systèmes vulnérables aux attaques quantiques vers des systèmes à résistance quantique, et softwareQ Inc. pour fournir des outils et des services logiciels quantiques.

L'incidence de la technologie quantique sur la recherche du renseignement pour les opérations de défense et de sécurité peut devenir importante, et il est impératif d'être préparé plutôt que réactionnaire. En tant que technologie à double usage, les technologies quantiques peuvent être utilisées à bon ou à mauvais escient, à des fins civiles ou militaires. Nous adoptons une vision universelle de cette technologie, tout en soutenant que nous pourrions être à l'aube d'une percée technologique qui exposera nos vulnérabilités dans la protection des informations sensibles et accordera aux adversaires de nouvelles capacités militaires. De plus, ce concept pourrait ne pas s'appliquer seulement aux adversaires étatiques; à terme, lorsque la technologie sera plus répandue, elle pourrait également être commercialisée par des acteurs non étatiques, y compris des groupes criminels et terroristes politiques. Cette dernière menace verra le jour à long terme, car la capacité quantique est encore relativement coûteuse à acquérir et se concentre dans les institutions étatiques et certaines entités commerciales multinationales. Le calcul quantique y fait partiellement exception, car l'accès à un appareil (au lieu de devoir le posséder) suffit aux auteurs de menaces, ce qui peut considérablement réduire le laps de temps prévu. Cela dit, les décideurs doivent investir dans ce domaine critique pour faire face de manière proactive aux changements perturbateurs résultant des capacités de transformation des technologies quantiques. Le présent article explique les répercussions potentielles des technologies quantiques sur la défense et la sécurité, tout en soulignant l'impératif stratégique d'investir dans cette industrie canadienne et de la soutenir. La Stratégie quantique nationale du Canada est une étape positive, et sa mise en œuvre complète est nécessaire pour que cette stratégie se concrétise et profite à une industrie en plein essor qui pourrait avoir des retombées positives sur la richesse et la prospérité globales des Canadiennes et Canadiens.

La menace quantique qui pèse sur nos systèmes numériques est imminente et nécessite une attention urgente de la part des décideurs politiques. Bien que l'échéancier de la menace soit inconnu, l'atteinte de jalons clés se poursuit, et les décideurs doivent investir dans la recherche, le développement et le déploiement pour s'assurer que nous conservons notre avantage comparatif dans ce domaine et que nous déjouons ou atténuons les attaques d'origine quantique. Bien que de nombreuses applications des technologies quantiques aient de faibles niveaux de maturité technologique (NMT) ou niveaux de maturité de la

solution, les connaissances scientifiques et l'orientation de ces applications deviennent plus transparentes et plus diffuses, et il est impératif pour la sécurité et la prospérité nationales que le Canada demeure un acteur important dans une course mondiale à la technologie quantique toujours plus intense.

Tout au long du présent article, nous passons en revue les documents et les études de sources ouvertes sur l'application potentielle des technologies quantiques à la défense et à la sécurité nationales, en mettant l'accent sur la recherche du renseignement. Nous possédons tous deux une expertise en sciences



L'image a été modifiée numériquement pour des raisons de sécurité opérationnelle. Un marin surveille son ordinateur alors que le NCSM HARRY DEWOLF navigue dans l'océan Atlantique au cours de l'opération CARIBBE, le 14 avril 2022.

Photo des Forces armées canadiennes

quantiques, en cryptographie, en affaires internationales, en cybersécurité, en géopolitique et en études de défense et de sécurité. Dans la mesure du possible, nous intégrons des liens vers les articles universitaires et les nouvelles connexes.

Le présent article traite de l'application de l'informatique quantique, des communications et réseaux quantiques et de la détection quantique à la recherche, à l'analyse et à la diffusion du renseignement. Ces trois domaines de la science quantique sont les plus importants dans notre discussion sur l'application des technologies quantiques à la défense et à la sécurité. En termes simples, la dernière évolution des technologies quantiques, souvent appelée la deuxième révolution quantique ou Quantum 2.0, améliorera de nombreux aspects du monde numérique, rendant les processus plus rapides, les mesures plus précises et le traitement des données plus puissant que les technologies actuelles et les technologies quantiques des générations précédentes. Il est important de noter que cette deuxième vague de la révolution quantique n'apportera pas nécessairement de nouveaux types d'instruments ou d'armes, mais qu'elle améliorera considérablement ceux qui existent déjà, renforçant ainsi les capacités globales.¹

Ici même, les villes de Vancouver, Calgary, Sherbrooke et Toronto et la région de Waterloo accueillent une masse critique de la puissance intellectuelle du Canada et des entreprises en démarrage qui sous-tendent la technologie quantique.² Pourtant, nous perdons du terrain face aux concurrents des pays comme la Chine et les États-Unis, qui surpassent le Canada sur le plan des dépenses, des investissements et de l'ingéniosité, et le devançant dans la recherche, l'application et la commercialisation des technologies quantiques.³ Cet article passe en revue le paysage technologique et son application à la défense et à la sécurité, en mettant l'accent sur la recherche et l'analyse du renseignement. Cependant, on ne saurait trop insister sur le rythme rapide des changements technologiques. La Stratégie quantique nationale visant à aider le Canada à être concurrentiel offre une initiative

prometteuse pour faire progresser les capacités quantiques du pays, mais sa mise en œuvre complète nécessite des investissements considérablement plus élevés dans la recherche, le développement des compétences et la commercialisation de l'industrie afin d'accroître la capacité du Canada à soutenir la concurrence mondiale dans ce secteur essentiel.⁴

Dans la dernière section du présent article, nous visons à formuler des recommandations stratégiques, plutôt que des recommandations techniques, sur la façon dont le Canada peut mieux gérer et relever les défis des technologies quantiques émergentes et en saisir les occasions. Il est encore temps de maintenir notre place importante dans ce domaine, en particulier dans les domaines où le Canada est un chef de file mondial depuis un certain temps, comme les algorithmes et les applications des ordinateurs quantiques, la cybersécurité à résistance quantique et certains types de détection quantique.⁵

1. Que signifie « quantique »?

La présente section commence par un examen fondamental de ce que signifie le terme « quantique » avant d'approfondir son application à la recherche, à l'analyse et à la diffusion du renseignement et d'étudier ses risques et ses avantages. Nous présentons d'abord un aperçu de l'effet de la théorie quantique sur trois domaines principaux de la technologie. Dans la section suivante, nous en détaillons les répercussions sur la défense et la sécurité. Pour commencer, la mécanique quantique est une théorie fondamentale qui a permis aux physiciens de résoudre des problèmes et des paradoxes difficiles pour comprendre divers phénomènes physiques. Les technologies quantiques sont la réalisation d'applications qui dépendent des effets quantiques. Fondée sur la mécanique quantique, la théorie de l'information quantique jette les bases de l'informatique quantique et d'autres technologies de traitement de l'information quantique. L'une des caractéristiques clés de ce cadre est la capacité de décrire l'état d'un système physique comme occupant « simultanément » deux configurations distinguables ou plus, ce que l'on appelle également superposition. Par exemple, un seul électron peut occuper plusieurs niveaux d'énergie d'un atome à la fois, et un seul photon peut traverser simultanément plusieurs trajectoires.

Les règles quantiques sont une théorie fondamentale de la physique qui influe sur ce qui est possible. Par exemple, les règles quantiques déterminent si les codes sont déchiffrables et avec quelle précision nous pouvons mesurer un objet.

L'une des implications de la théorie quantique concerne le calcul. Les ordinateurs stockent l'information en bits physiques qui ont deux états distincts : 0 et 1. Selon la physique quantique, la description complète d'un seul bit d'information nécessite deux nombres complexes pour représenter les amplitudes des états 0 et 1, tandis que la description de n qubits nécessite 2^n nombres complexes représentant les amplitudes de toutes les 2^n configurations possibles. La seule méthode connue pour un

ordinateur classique de simuler n bits quantiques est de suivre ces 2^n amplitudes. Même pour quelques centaines de qubits, les besoins en stockage dépasseraient toute la matière dans l'univers connu. Cette observation met en évidence le potentiel des ordinateurs quantiques de résoudre des problèmes qui nécessiteraient une quantité exponentiellement plus importante de ressources classiques.

Une autre implication de la théorie quantique concerne la détection. Selon le cadre quantique, un résultat détectable avec une probabilité p existe avec une amplitude de probabilité quantique proportionnelle à $\sqrt{p}$, qui est supérieure à p si p est inférieur à un (lorsque $0 = 0\%$ et $1 = 100\%$). Les capteurs quantiques manipulent les objets au niveau quantique, ce qui permet la détection avec un échantillon de taille N plutôt que de taille N^2 , ou avec N signaux de sonde au lieu de N^2 signaux de sonde. De plus, certains instruments avancés mis au point pour les technologies quantiques peuvent également améliorer les applications classiques de détection et de mesure.

La troisième famille d'applications touchées par la théorie quantique est la communication. La technologie quantique transforme les réseaux de communication et le paysage de la sécurité numérique. Par exemple, la complexité supplémentaire intrinsèque aux bits quantiques fait que toute écoute clandestine, c'est-à-dire toute extraction d'informations sur les bits quantiques, conduit à une perturbation mesurable proportionnelle à la quantité d'informations extraites. Cette propriété quantique fondamentale ouvre la porte à de nouveaux outils de protection de l'information, y compris la distribution de clés quantiques (que nous détaillons plus loin).

Les réseaux de communication quantique peuvent faciliter les calculs quantiques distribués, effectués parfois avec une communication considérablement réduite entre les différents ordinateurs du réseau. La liaison quantique entre ordinateurs quantiques permet d'améliorer la puissance de calcul quantique. Ces réseaux de communication permettent également une détection quantique à corrélation quantique, combinant des informations provenant de différents capteurs à différents endroits pour reconstruire des images potentiellement meilleures. Les capteurs quantiques à corrélation quantique, utilisant un réseau quantique, peuvent également offrir une capacité de détection ou de mesure au-delà de ce qui est possible avec les seuls réseaux de communication classiques reliant les capteurs.

Le moment et l'effet du potentiel des technologies quantiques dépendent de plusieurs facteurs. Ces facteurs comprennent, par exemple, la réalisation d'avancées technologiques qui permettent de réaliser des opérations fondamentales moins brouillées par le bruit et plus rapides, comme la conversion de l'information quantique entre les photons, qui sont efficaces pour déplacer l'information, et d'autres qubits, qui sont plus efficaces pour les opérations ou le stockage à qubits multiples, et la mise au point de méthodes améliorées pour tirer parti d'opérations quantiques imparfaites. Enfin, le moment et l'effet dépendront également

du degré d'effort et d'attention consacré aux différents défis et possibilités.

2. Applications quantiques

Nous avons relevé trois domaines d'application de la technologie quantique qui sont susceptibles d'intéresser la communauté de la défense et de la sécurité : les communications et les réseaux quantiques, l'informatique quantique et la détection quantique. Dans cette section, nous discutons également des répercussions de la technologie quantique sur le travail des décideurs et des praticiens dans le domaine de la défense et de la sécurité, et du personnel militaire.

a. Communication et réseaux quantiques

Les réseaux de communication modernes sont essentiels à la société mondiale. La technologie quantique améliorera et révolutionnera les voies et les réseaux de communication qui sous-tendent nos appareils interconnectés. Les appareils sont de plus en plus numériques et interconnectés, ce qui les rend très dépendants de formes de communication sûres et sécurisées.

Les technologies quantiques émergentes auront une incidence sur l'intercommunication des avions, des navires, des véhicules, du personnel et des centres de commandement en défense et en sécurité. Bien que l'amélioration de ces réseaux suscite de l'enthousiasme, le risque que les adversaires interceptent les communications et les déchiffrent à l'aide des nouvelles capacités quantiques augmente. Des communications sécurisées et fiables sont essentielles pour les opérations militaires et la communication du renseignement, et elles pourraient être compromises si elles ne sont pas à résistance quantique grâce à une nouvelle cryptographie conçue pour contrer les ordinateurs quantiques.

Le calcul quantique peut exposer le renseignement et les données actuellement cryptées sur les ordinateurs classiques et l'infrastructure numérique. Les réseaux de communication sécurisés conventionnels deviendront plus vulnérables à la technologie quantique, mais les progrès de la cryptographie et des réseaux quantiques offrent des possibilités de renforcer la sécurité et la confidentialité des réseaux de communication. Des systèmes de communication sécurisés sont essentiels à une économie robuste. La cryptographie à résistance quantique, conçue pour contrer les ordinateurs quantiques, inclut des algorithmes classiques (ce que l'on appelle cryptographie post-quantique).⁶ De plus, l'échange/la distribution quantique de clés (DQC) est un type de cryptographie qui peut protéger les communications numériques et qui n'est pas susceptible au déchiffrement de code quantique ou classique. La technologie DQC est disponible dans le commerce depuis des années et utilisée par certains gouvernements et certaines entités privées. La normalisation continue, la certification, les améliorations des performances et la mise en

place de réseaux plus étendus en faciliteront le déploiement à plus grande échelle.

Il est encore prématuré de suggérer que cette technologie de communication est le précurseur d'un Internet quantique. Néanmoins, au vu des progrès de la communication par satellite et de la communication des nœuds quantiques, qui évoluent rapidement, on a bon espoir que ces découvertes scientifiques nous rapprochent de la réalisation des diverses capacités que permettaient des réseaux distants fiables.

b. Informatique quantique

Les ordinateurs quantiques seront capables de résoudre des problèmes spécifiques avec un nombre d'étapes astronomiquement réduit et seront donc beaucoup plus rapides que les ordinateurs classiques. Par exemple, le décodage de la cryptographie à clé publique d'aujourd'hui à l'aide d'ordinateurs classiques prend exponentiellement plus de temps que lorsqu'on utilise des ordinateurs quantiques. En 2020, des chercheurs chinois ont utilisé l'ordinateur quantique Jiuzhang pour résoudre un problème mathématique en moins de 5 minutes, une tâche qui prendrait à un ordinateur classique 2,5 milliards d'années.⁷ Fait intéressant, cette expérience fait suite à la revendication de suprématie quantique de Google en 2019 à l'aide de son processeur Sycamore. Bien que les ordinateurs quantiques imparfaits de taille intermédiaire (en abrégé NISQ pour « noisy intermediate scale quantum ») ne tirent pas pleinement parti de la puissance de calcul de la mécanique quantique, ces expériences ont confirmé qu'il est impossible dans la pratique de simuler des systèmes informatiques quantiques suffisamment grands et bien contrôlés à l'aide de plateformes informatiques classiques qui utilisent les algorithmes les plus connus. Les chercheurs explorent les applications pratiques des ordinateurs NISQ en examinant les défis informatiques du monde réel sous l'angle des capacités informatiques NISQ. Le seul moyen connu de saisir toutes les capacités de calcul des ordinateurs quantiques est d'utiliser la correction des erreurs quantiques insensibles aux défaillances, qui réduit au minimum les erreurs et le bruit, de manière semblable aux codes classiques de correction d'erreurs utilisés dans les systèmes informatiques et les systèmes de communication classiques pour permettre une communication et un calcul fiables en présence d'erreurs.

La puissance de calcul des ordinateurs quantiques menace la cryptographie à clé publique actuelle, et pourrait exposer les données de renseignement cryptées si l'accès aux clés de chiffrement est protégé par la cryptographie à clé publique. Ce risque est accru pour les données communiquées aujourd'hui ou dans le passé à l'aide de la cryptographie à clé publique pour les clés de session. Il convient de souligner qu'il est possible que des acteurs malveillants aient déjà intercepté et stocké des données cryptées, lorsque les clés étaient communiquées à l'aide de la cryptographie à clé publique, dans l'attente des capacités informatiques nécessaires pour les déchiffrer.

Les modèles de menace actuels peuvent sous-estimer le risque que présentent les données cryptées à l'aide de la cryptographie à clé publique, car elles sont considérées comme inaccessibles sans l'informatique quantique ou non pertinentes jusqu'à ce que l'IA avancée révèle de nouveaux modèles. Cependant, les adversaires ont peut-être déjà mené de telles opérations de piratage offensives, et les atteintes à la sécurité pourraient ne pas être exposées à l'avenir. Il est donc crucial de permettre la résistance quantique de l'information sensible et classifiée dès maintenant, car les données protégées par la suite B ou par des algorithmes similaires peuvent avoir déjà été siphonnées pour être déverrouillées par une future cryptanalyse quantique.

La protection du renseignement recherché et des secrets d'État prendra des années à préparer, et la résistance quantique des données du renseignement est impérative pour la sécurité nationale et la défense. Le ministère de la Défense nationale devrait inventorier les données sensibles, évaluer la tolérance au risque et élaborer une stratégie pour passer à la cryptographie à résistance quantique grâce à ses processus de gestion du cycle de vie de la technologie. À l'appui de cette migration, la communication quantique permet un échange de clés qui n'est pas sensible à la cryptanalyse algorithmique (DQC). Il est possible d'intégrer la DQC dans la suite de solutions, y compris les clés pré-partagées, pour fournir une résilience contre les avancées cryptanalytiques inattendues.

En plus de décrypter plus rapidement que toute méthode classique connue, l'informatique quantique pourrait répondre plus efficacement à d'autres défis de calcul, permettant ainsi d'améliorer l'analytique prédictive grâce à l'apprentissage automatique et à l'intelligence artificielle. Cette capacité peut faciliter des actions préventives en anticipant les mouvements des adversaires en fonction des plans de champ de bataille précédents, en améliorant la précision des cibles et en limitant les dommages collatéraux.

Parmi les prédictions les plus futuristes, mentionnons la guerre cognitive alimentée par l'informatique quantique à mesure que la société étend son empreinte numérique et saisit un nombre croissant d'informations sur ses processus de pensée et de prise de décision sur des appareils numériques. Les progrès de l'informatique quantique peuvent faciliter la manipulation des dirigeants et des sociétés en dégageant des habitudes de comportement grâce à l'apprentissage automatique avancé et à l'intelligence artificielle. En fait, les médias sociaux font partie intégrante de cette collection massive d'empreintes numériques sociétales, et nous constatons déjà un intérêt commercial important pour la compréhension du comportement humain. Ceci ne fera que s'accélérer avec les progrès de l'informatique quantique. En outre, les attentes croissantes du public de notre société ouverte et occidentale à l'égard de la transparence gouvernementale contribuent à une meilleure compréhension de notre société par nos adversaires. On ne peut pas en dire autant d'eux,

car leurs tendances autoritaires dans les questions numériques se sont traduites par une contribution moindre à l'espace public virtuel. De plus, la polarisation au sein des démocraties occidentales révèle des faiblesses internes qui offrent aux adversaires la possibilité de trouver des failles afin de perturber la guerre cognitive.⁸ Les appels à une meilleure sensibilisation aux risques de la guerre cognitive doivent être entendus.⁹

c. Détection quantique

La détection et la métrologie quantiques transformeront également la recherche et l'analyse du renseignement. La détection quantique peut améliorer notre capacité à mesurer la température, l'accélération, le temps et la gravité. Elle pourrait améliorer les instruments utilisés pour détecter et mesurer les objets et le mouvement, ce qui pourrait permettre de réaliser des cartes précises et d'obtenir une connaissance de la situation en matière de positionnement et de navigation. On peut utiliser des capteurs quantiques pour améliorer la recherche du renseignement et la surveillance des mouvements des personnes, des véhicules camouflés et des objets derrière les murs et dans les coins. Ils peuvent également détecter le mouvement dans les bunkers, les tunnels ou les grottes sous la surface de la Terre. Cependant, certaines applications potentielles sont spéculatives et font encore face à des défis, notamment des problèmes de sensibilité élevée et de traitement des données dans les environnements peu clairs.

De plus, les capteurs quantiques feront considérablement progresser l'application de la métrologie quantique aux situations de faible luminosité ou de nuit, améliorant ainsi les capacités militaires de renseignement, surveillance, acquisition d'objectifs et reconnaissance (ISTAR) sur un champ de bataille multi-domaine. Les progrès de la détection quantique sont déjà utilisés et disponibles dans le commerce dans les horloges atomiques et les gravimètres. Cependant, certains défis demeurent et nécessitent des recherches approfondies à l'échelle mondiale pour surmonter ces limites.¹⁰

Les capteurs quantiques utilisés pour le positionnement, la navigation et la synchronisation (PNS) peuvent compléter ou remplacer le GPS, en particulier lorsque les transmissions et la réception échouent. Par exemple, le potentiel de la détection quantique utilisée dans les profondeurs océaniques comme odomètre suscite un intérêt considérable. Les progrès de la détection quantique pourraient exposer des sous-marins et des torpilles auparavant indétectables à des profondeurs spécifiques, perturbant potentiellement l'équilibre des puissances et compliquant la détection.¹¹ De plus, les nouvelles revendications territoriales pourraient s'accélérer avec l'application des capteurs quantiques et avoir une incidence sur la course aux revendications des territoires récemment découverts. Les pôles Sud et Nord sont des zones à surveiller en ce qui concerne les nouvelles revendications territoriales attribuables en partie à de multiples progrès scientifiques tels que la détection quantique.



A CAF member monitors the progress of firefighters during a fire exercise aboard HMCS HALIFAX during Operation REASSURANCE on January 14, 2021.

Photo: Sailor First Class Bryan Underwood, Canadian Armed Forces photo

On peut observer une augmentation de la guerre sous-marine à la suite de l'utilisation accrue des capteurs quantiques. Les magnétomètres quantiques, comme ceux qui sont basés sur un dispositif supraconducteur à interférence quantique (SQUID), pourraient révolutionner la détection des matériaux et des champs magnétiques. La dépendance actuelle à l'égard du sonar pour détecter les sous-marins pourrait céder la place à une utilisation accrue de la technologie à SQUID. Les scientifiques ont utilisé un dispositif aéroporté composé de plusieurs SQUID pour repérer des billes métalliques enterrées.¹² Les scientifiques ont également mentionné la possibilité d'utiliser le dispositif pour détecter des sous-marins à plusieurs kilomètres de distance, mais cela reste une réalisation spéculative et potentiellement lointaine de la technologie. L'analyse des données de l'étude est en cours, et il y a probablement de nombreuses difficultés associées à l'application de ce dispositif sur le terrain, sans parler d'un contexte militarisé. Les instruments nécessitent un refroidissement et une miniaturisation considérables pour être utiles dans la plupart des plateformes mobiles, par exemple, pendant une mission de reconnaissance par véhicule sans équipage. La courte durée de vie de la batterie de ces drones continue d'être un défi important pour les rendre utilisables. Les difficultés susmentionnées ont réduit les attentes quant à l'utilisation des magnétomètres à SQUID dans la guerre anti-sous-marine.¹³ Les gradiomètres à gravité présentent des défis similaires.

Les capteurs quantiques peuvent détecter les émissions électromagnétiques, renforcer les capacités militaires à localiser les forces de l'adversaire et améliorer la guerre électronique. Parallèlement, la détection militaire des émissions électromagnétiques à l'aide de capteurs quantiques pourrait aider à contrecarrer la guerre électronique. Les antennes quantiques rehausseront également la capacité des systèmes de guerre électronique d'intercepter les signaux à basse fréquence. Dans les domaines comme le renseignement d'origine électromagnétique et sur les communications et le l'antibrouillage radar, la

technologie quantique peut améliorer la recherche du renseignement, l'interception et l'identification des objets. De plus, les réseaux quantiques peuvent mieux détecter l'écoute clandestine potentielle, en particulier dans les plages de basses fréquences et les bandes passantes à commutation dynamique. Comme le note Krelina, « À l'avenir, les antennes quantiques pourraient ressembler à un réseau (matriciel) de cellules d'atomes de Rydberg. Différentes cellules peuvent mesurer différents signaux, et dans la mesure conjointe de deux cellules ou plus, l'angle d'arrivée du signal pourrait être déterminé. »[TCO]¹⁴ Cependant, le même auteur note que le refroidissement de ces atomes pose des défis. Par conséquent, le *Defense Science Board* des États-Unis a exprimé son scepticisme quant au potentiel des radars quantiques d'améliorer considérablement les capacités radar du Pentagone dans un avenir rapproché.¹⁵ En particulier, les oscillateurs à quartz à enceinte à température régulée, qui maintiennent la température et se synchronisent avec le GPS, sont déjà incroyablement précis, petits et peu coûteux, améliorant la précision des applications de localisation.

En ce qui concerne une technique de radar quantique appelée illumination quantique, nous pourrions voir une détection plus avancée de la lumière qui pourrait conduire à déchiffrer des détails plus délicats d'un objet identifié et pourrait améliorer le ciblage sur le champ de bataille. Les radars quantiques pourraient améliorer la détection et la précision dans les conditions rigoureuses telles que l'espace, le brouillard, la fumée, les nuages, la faible luminosité, la nuit et les températures élevées comme dans les feux de forêt.¹⁶ Les radars conventionnels sont également plus sensibles aux tempêtes géomagnétiques et aux éruptions solaires, ce qui revêt une importance particulière pour les opérations canadiennes dans l'Arctique. Les radars quantiques pourraient améliorer les missions et les opérations de recherche et de sauvetage dans les environnements difficiles en émettant beaucoup moins d'énergie et en offrant une « détection furtive », selon laquelle une cible est beaucoup moins susceptible de savoir qu'elle est détectée. Cela dit, cette utilisation de la technique du radar quantique est encore sous-développée. Elle présente de nombreux défis en ce qui concerne « l'obstruction, les calculs d'annulation et l'examen factuel de l'espace inutilisé ».[TCO]¹⁷ La surface équivalente radar quantique bistatique présente souvent un effet quantique de lobe secondaire, posant un défi persistant dans le domaine de la diffusion.¹⁸ Il s'agit d'un développement naissant. D'aucuns préconisent une vision futuriste des applications potentielles des radars quantiques qui nécessite encore des recherches importantes pour trouver des buts pratiques.¹⁹

Par conséquent, les radars quantiques en sont aux tout premiers stades de l'application, principalement dans les laboratoires ayant les plus faibles NMT. L'utilisation du radar quantique et son application sur le champ de bataille²⁰ ont donné lieu à des revendications faisant débat²¹ et exagérées. En 2019, des chercheurs autrichiens ont brièvement revendiqué la « suprématie quantique » dans une démonstration en laboratoire du radar

quantique, mais la revendication a été rapidement retirée du serveur de pré-impression d'arXiv à la suite d'importantes critiques. Les ingénieurs ont réfuté²² les revendications selon lesquelles les radars quantiques peuvent détecter les avions furtifs.²³ De plus, d'autres chercheurs ont avancé que les radars quantiques ne peuvent surpasser les radars conventionnels qu'en présence de faibles signaux ou d'un fort bruit de fond, ce qui limite donc leur application sur le champ de bataille pour le moment.²⁴

Néanmoins, le développement de radars quantiques pour la détection d'avions furtifs et les applications de faible probabilité d'interception, ce qui pourrait révolutionner la dynamique du champ de bataille, suscitent un intérêt considérable. Les grandes puissances et l'industrie militaire sont dans une course mondiale pour produire cette capacité. Il est certain que la modernisation du Commandement de la défense aérospatiale de l'Amérique du Nord (NORAD) et la mise à jour du système radar du Canada sont des problèmes d'approvisionnement urgents. Pour l'instant, la capacité opérationnelle de cette technologie radar quantique dans toute mise à jour du système du NORAD est probablement limitée par les considérations techniques.

3. Tendances mondiales émergentes

Cette section examine les développements récents dans les capacités quantiques à l'échelle mondiale, et porte plus particulièrement sur la concurrence entre les acteurs mondiaux de la course quantique, tels que les États-Unis, la Chine, le Royaume-Uni, le Canada et l'Europe.²⁵ Bon nombre de ces acteurs mondiaux ont défini une stratégie nationale sur la technologie quantique pour se concentrer sur la recherche et le développement, la construction d'écosystèmes commerciaux, le perfectionnement des compétences de la main d'œuvre et l'indépendance technologique.²⁶ Comme nous l'avons mentionné précédemment, les investissements dirigés par l'État dans la recherche et le développement et dans le secteur militaro-industriel ont ouvert la voie, sauf au Canada où l'investissement du secteur privé dans la technologie quantique dépasse l'investissement du gouvernement.²⁷

La Chine a fait des investissements importants et a donc probablement une longueur d'avance dans la communication quantique. Selon un article publié par le *Center for a New American Security*, le lancement du satellite Micius a marqué une étape importante, conduisant à de nombreux « mégaprojets » dans les communications quantiques.²⁸ En utilisant sa stratégie nationale d'intégration civilo-militaire avec une grande détermination pour devenir une superpuissance scientifique et technologique, la Chine a investi massivement dans ses scientifiques et chercheurs, réduisant ainsi sa dépendance à l'égard des transferts de technologie étrangers, un changement en partie motivé par les révélations de Snowden sur l'espionnage américain des systèmes chinois. L'État chinois a investi dans la communication et l'informatique quantiques, espérant que

ces avancées le protégeraient contre l'espionnage étranger et l'exploration de données sur ses systèmes.²⁹ En outre, le « Plan des mille talents » de 2008 de la Chine vise à rapatrier les scientifiques d'origine chinoise travaillant à l'étranger; près de 60 000 professionnels ont été recrutés jusqu'à présent, souvent en appuyant les efforts de commercialisation des scientifiques, comme indiqué dans un rapport du Sénat des États-Unis.³⁰

Compte tenu de la course internationale à la suprématie quantique et, par conséquent, de l'ingérence étrangère potentielle dans la capacité des chercheurs canadiens de faire progresser la recherche et le développement quantiques, on peut comprendre les préoccupations du gouvernement canadien au pouvoir concernant l'avancement de la recherche et du développement dans le domaine quantique. En effet, le financement de la recherche par le gouvernement dans ce domaine fait maintenant l'objet d'une surveillance importante sur le plan de la sécurité nationale, y compris un examen plus approfondi des demandes de financement. Toutefois, des contrôles de sécurité nationale excessifs pourraient décourager la collaboration internationale, en particulier avec les principaux chercheurs chinois, ce qui pourrait nuire aux progrès du Canada dans le domaine de la technologie quantique. La Chine est déterminée à acquérir des talents étrangers et une propriété intellectuelle étrangère, y compris auprès du Canada, à l'aide de subventions partielles payées par les contribuables, ce qui soulève inévitablement des préoccupations liées à la sécurité nationale.

Un groupe de réflexion australien a suivi les universités chinoises engagées dans la recherche militaire visant à aider les universités internationales à trouver des institutions partenaires qui pourraient faciliter des fuites potentielles de technologie et de recherche vers l'État chinois.³¹ Ce projet a suscité un malaise considérable dans de nombreuses universités et au sein du gouvernement canadien, qui craignent que la filière de compétences et de connaissances scientifiques ne se retrouve à la merci de la Chine. Cela dit, les communautés universitaires sont très inquiètes de l'attention excessive accordée par la sécurité nationale aux universités et à la recherche alors que de nombreux scientifiques publient leurs résultats de recherche pour le plus grand bénéfice de la communauté scientifique quantique. L'organisme de financement des trois organismes du Canada et certaines provinces sont devenus plus conscients de ces fuites potentielles, rendant obligatoire un examen de sécurité des demandes de subvention. Ironiquement, les chercheurs craignent que ces examens de sécurité des trois organismes les poussent à chercher davantage de financement auprès de l'industrie, ce qui pourrait entraîner d'autres fuites vers des pays comme les États-Unis et certaines parties de l'Europe. De plus, les chercheurs de RAND ont noté que, comme le NMT de l'informatique quantique et des communications reste faible, les contrôles à l'exportation pourraient ralentir encore la recherche scientifique et les progrès technologiques.³²

Les États-Unis et le Royaume-Uni étaient considérés comme des chefs de file de la détection quantique. L'investissement important de la *Defense Advanced Research Projects Agency* (DARPA) dans la technologie quantique stimule le progrès scientifique aux États-Unis. La recherche universitaire américaine s'est développée grâce à d'importants investissements gouvernementaux, principalement par le biais du projet *National Quantum Initiative*, qui a dépensé 710 millions de dollars en recherche et développement en 2021 seulement, affichant une augmentation de 20 % par an ces dernières années. Selon les chercheurs de RAND, les États-Unis se concentrent sur l'informatique et la détection quantiques, tandis que la Chine donne la priorité à la communication quantique, suivie de près par l'informatique quantique.³³ L'accord AUKUS entre l'Australie, le Royaume-Uni et les États-Unis pour faire progresser les technologies militaires a suscité des spéculations selon lesquelles les États-Unis équiperont les sous-marins australiens de technologies de détection quantique et font progresser l'innovation dans ce domaine technologique qui pourrait exclure le Canada.³⁴

4. Recommandations stratégiques

Nous décrivons les mesures recommandées pour nous préparer aux défis et aux possibilités découlant des technologies quantiques émergentes et y répondre, tout en notant que Recherche et Développement pour la défense Canada (RDDC) a élaboré une stratégie quantique pour le MDN et les FAC.³⁵ Innovation, Sciences et Développement économique Canada a entrepris un processus de consultation pour formuler une Stratégie quantique nationale (SQN) intégrée.³⁶ La recherche quantique évolue rapidement, et le MDN et les FAC doivent continuer de faire participer le secteur universitaire pour surmonter les multiples défis scientifiques, dont bon nombre sont des considérations techniques qui transformeront la recherche en une réalité déployable.³⁷ L'allocation budgétaire 2021 de 360 millions de dollars sur sept ans pour une SQN est insuffisante pour maintenir la domination quantique existante et rattraper nos concurrents homologues.

La collaboration internationale avec les alliés de l'Organisation du Traité de l'Atlantique Nord (OTAN) dans les domaines de la commercialisation, de la recherche et du développement est essentielle au succès collectif et à l'interopérabilité. Cela dit, la Chine attire et finance avec succès des chercheurs du monde entier. La nature à double usage de la technologie quantique mènera naturellement à des progrès commerciaux dans la technologie quantique que le MDN et les FAC pourront utiliser. L'investissement continu du MDN et des FAC dans la recherche sur la détection et les radars quantiques, en particulier pour la détection des sous-marins et des aéronefs furtifs, est impératif pour notre défense nationale et la surveillance de l'Arctique.

Il est essentiel de tirer parti des forces du milieu universitaire et des petites et moyennes entreprises (PME) du Canada pour relever les défis scientifiques. Compte tenu du bassin de talents

concurrentiel, cette approche intégrée dans tous les secteurs est nécessaire pour maximiser les développements technologiques quantiques au Canada. Par conséquent, nous devons élaborer un programme cohérent qui explore la détection, l'informatique et les communications et le réseautage quantiques pour la défense nationale et le renseignement. Cela pourrait signifier s'inspirer d'un modèle de type DARPA/*Intelligence Advanced Research Projects Activity* (IARPA) dans lequel la mission ultime est de prévenir les surprises stratégiques, et où la propriété intellectuelle (PI) continue d'appartenir aux chercheurs pour favoriser l'activité commerciale et soutenir l'écosystème quantique canadien, y compris les projets dont le NMT varie. Une partie du programme pourrait prévoir la formation et l'éducation du personnel du MDN et des FAC au moyen de détachements dans les universités et dans l'industrie. Cela soutiendrait également les PME, qui dominent cet écosystème.

Nous devons nous rappeler que l'impact de la technologie quantique est plus susceptible d'être exponentiel que linéaire; il y a donc un besoin urgent d'investissement. Le Canada ne peut pas se permettre d'adopter une approche attentiste, particulièrement pour ce qui est de sécuriser le renseignement national. L'impact de cette technologie peut passer d'« aucun impact connu » à « impact transformateur », comme on l'a vu avec la cryptographie à clé publique entre 1993 et 1994. Les ordinateurs quantiques n'existaient même pas à l'époque. Une fois que les ordinateurs quantiques feront leur apparition, il n'y aura pas de possibilité de « temps mort » pour se préparer aux implications sur le plan de la sécurité. Une fois que la PI, sous forme de connaissance et de produits, se retrouvera entre les mains des adversaires, nous n'aurons pas un parcours facile pour accéder aux capacités quantiques transformatrices. Nous devons prendre l'initiative de réunir les responsables des problèmes difficiles et des experts de calibre mondial du milieu universitaire et de l'industrie du Canada afin de découvrir et de développer les domaines d'application potentiels de la technologie quantique.

Dans de nombreux cas, ils concluront qu'il n'y a pas d'avantage quantique connu. Ce n'est pas un échec; cela fait plutôt partie du processus de découverte scientifique. Il nous éloigne des applications moins prometteuses et nous oriente vers celles qui le sont plus, tout en faisant progresser l'expertise nécessaire. Les réussites peuvent se transformer ensuite en projets à NMT plus élevé.

Nous devons également améliorer la capacité de la communauté de la défense nationale et du renseignement à faire progresser sa compréhension des menaces et des possibilités quantiques potentielles grâce à la formation continue et à l'éducation offertes par le milieu universitaire et l'industrie. La base de connaissances de cette technologie est plutôt mince et relativement jeune. Pour assurer un bassin de talents continu, le Canada doit former les jeunes professionnels qui travaillent dans ce domaine et fournir au pays un écosystème dynamique qui permet de créer de la valeur pour le Canada. Le financement des

étudiants des cycles supérieurs et des boursiers de recherches postdoctorales fait défaut au Canada, et bon nombre d'entre eux choisissent de partir étudier ailleurs. En plus de salaires concurrentiels, les chercheurs ont besoin d'occasions de travailler sur des projets avant-gardistes percutants. De plus, à l'extérieur de leurs laboratoires et de leur milieu universitaire, les étudiants des cycles supérieurs, les boursiers de recherches postdoctorales et les chercheurs en début de carrière bénéficieraient également d'occasions de réseauter, d'échanger de l'information et de collaborer avec la communauté des politiques de défense et de sécurité pour résoudre certains des défis urgents en matière de défense nationale abordés dans le présent article.

Conclusion

La science de l'information et la technologie quantiques sont un vaste domaine composé de différents éléments à différents stades de maturité et de nombreux groupes d'expertise dans le monde entier. Les acteurs mondiaux de la course quantique, principalement les États-Unis, la Chine, le Royaume-Uni, le Canada et l'Allemagne, ont défini une stratégie quantique nationale axée sur la recherche et le développement, la construction d'écosystèmes commerciaux, l'avancement des compétences de la main d'œuvre et l'indépendance technologique. Dans l'ensemble, l'opinion largement répandue est que l'Amérique du Nord est le chef de file mondial de la technologie de l'informatique quantique (suivie de la Chine, puis de l'Europe), la Chine est le chef de file global des communications quantiques (y compris son satellite Micius), et il existe une forte concentration de leadership dans la détection quantique (qui est un domaine beaucoup plus large) au Royaume-Uni et en Amérique du Nord.

Les tensions géopolitiques et les préoccupations concernant les fuites scientifiques potentielles vers la Chine augmentent la pression pour les contrôles à l'exportation et autres contrôles autour des technologies quantiques. Ces contrôles sont d'autant plus pertinents que les investissements dirigés par l'État dans la recherche et le développement et le secteur militaro-industriel ont ouvert la voie. En protégeant nos connaissances scientifiques et nos capacités technologiques, la technologie quantique pose des défis uniques. Il est difficile de contrôler une technologie encore en cours de développement dont les implications sont encore en cours de découverte, de développement et d'évaluation. Des tentatives de contrôle prématurées ou mal dirigées ralentiront les développements et pourraient les miner. Pourtant, les conséquences d'un manque de contrôles adéquats peuvent être inattendues et potentiellement exponentielles. La navigation dans ces eaux incertaines exige beaucoup d'attention, de financement et d'engagement de la part des décideurs.

Notes

- 1 M. Krelina, « Quantum technology for military applications », *EPJ Quantum Technology*, vol. 8, n° 24 (2021). Tiré de : <https://doi.org/10.1140/epjqt/s40507-021-00113-y>
- 2 Gouvernement du Canada, Institut canadien de recherches avancées, Conseil de recherches en sciences naturelles et en génie du Canada, *Saisir les possibilités du Canada dans le domaine quantique : rapport sur le symposium et l'atelier de Quantique Canada, les 11 et 12 avril 2017*, NR16-151/2017F-PDF, Publications du gouvernement du Canada, Publications.gc.ca, 2017. Tiré de : <https://publications.gc.ca/site/fra/9.858244/publication.html>
- 3 Jamie Gaida, *ASPI's Critical Technology Tracker*, aspi.org.au, 2023. Tiré de : <https://www.aspi.org.au/report/critical-technology-tracker>
- 4 Lori Valigra, « Canada Lays the Groundwork to Become a Powerhouse in Quantum Technology », *Science Business*, 23 juin 2022. Tiré de : <https://sciencebusiness.net/news/quantum-computing/canada-lays-groundwork-become-powerhouse-quantum-technology>
- 5 Ben Sussman, Paul Corkum, Alexandre Blais, David Cory et Andrea Damascelli, « Quantum Canada », *Quantum Science and Technology*, vol. 4, n° 2 (22 février 2019), article 020503. Tiré de : <https://doi.org/10.1088/2058-9565/ab029d>
- 6 Lily Chen, Stephen Jordan, Yi-Kai Liu, Dustin Moody, Rene Peralta, Ray Perlner et Daniel Smith-Tone, *Report on Post-Quantum Cryptography*, National Institute of Standards and Technology, avril 2016. Tiré de : <https://doi.org/10.6028/nist.ir.8105>
- 7 Han-Sen Zhong, Hui Wang, Yu-Hao Deng, Ming-Cheng Chen, Li-Chao Peng, Yi-Han Luo, Jian Qin et coll., « Quantum Computational Advantage Using Photons », *Science*, vol. 370, n° 6523 (18 décembre 2020), p. 1460-1463. Tiré de : <https://doi.org/10.1126/science.abe8770>
- 8 Kimberley Orinx et Tanguy Stuye de Swielande, « China and Cognitive Warfare: Why Is the West Losing? », *HAL open science*, vol. 8 (2022), p. 1-6. <https://hal.science/hal-03635930>
- 9 A. Bernal, C. Carter, I. Singh, K. Cao et O. Madreperla, *Cognitive Warfare: An Attack on Truth and Thought*, 2021. Tiré de : <https://innovationhub-act.org/wp-content/uploads/2023/12/Cognitive-Warfare.pdf>
- 10 Remi Geiger, Arnaud Landragin, Sébastien Merlet et Franck Pereira Dos Santos, « High-accuracy inertial measurements with cold-atom sensors », *AVS Quantum Science*, vol. 2, n° 2 (2020). Tiré de : <https://arxiv.org/pdf/2003.12516v1#page25>
- 11 Congressional Research Service, *Defense Primer: Quantum Technology*, 4 novembre 2024. Tiré de : <https://crsreports.congress.gov/product/pdf/IF/IF11836>
- 12 David Hambling, « China's Quantum Submarine Detector Could Seal South China Sea », *New Scientist*, 22 août 2017. Tiré de : <https://www.newscientist.com/article/2144721-chinas-quantum-submarine-detector-could-seal-south-china-sea/>
- 13 Katarzyna Kubiak, *Quantum Technology and Submarine Near-Invulnerability: Global Security Policy Brief*, European Leadership Network, décembre 2020. Tiré de : <https://www.europeanleadershipnetwork.org/wp-content/uploads/2020/12/Quantum-report.pdf>
- 14 Michal Krelina, « Quantum Technology for Military Applications », *EPJ Quantum Technology*, vol. 8, n° 1 (6 novembre 2021). Tiré de : <https://doi.org/10.1140/epjqt/s40507-021-00113-y>
- 15 Kelley M. Saylor, « Defense Primer: Quantum Technology », *Congressional Research Service (CRS) Reports and Issue Briefs*, 2022, mis le 24 novembre 2024. Tiré de : <https://crsreports.congress.gov/product/pdf/IF/IF11836#:~:text=Quantum%20sensors%20could%20also%20enable,electromagnetic%20emissions%20thus%20enhancing%20electronic>
- 16 Hasan Abbas Al-Moahmed, *Quantum Radar: A Brief Analytical Study*, 29 décembre 2020, p. 174-180. Tiré de : <https://doi.org/10.1109/icenco49778.2020.9357379>
- 17 Adarsh Kumar, Diego Augusto de Jesus Pacheco, Keshav Kaushik et Joel J.P.C Rodrigues, « Futuristic View of the Internet of Quantum Drones: Review, Challenges and Research Agenda », *Vehicular Communications*, vol. 36 (août 2022), article 100487. Tiré de : <https://doi.org/10.1016/j.vehcom.2022.100487>
- 18 *Ibid.*
- 19 *Ibid.*
- 20 Kyle Mizokami, « How Quantum Radar Could Completely Change Warfare », *Popular Mechanics*, 26 août 2019. Tiré de : <https://www.popularmechanics.com/military/a28818232/quantum-radar/>
- 21 Capitaine de corvette Graham Hill, *Quantum Radar Is Stealth Radar: Examining the Potential Impact on the Defence Team*, PCEMI 48, Étude militaire, 2022. Tiré de : <https://www.cfc.forces.gc.ca/259/290/24/192/Hill.pdf>
- 22 Heidi Vella, « Could Quantum Radars Expose Stealth Planes? », *Engineering and Technology*, 18 avril 2019. Tiré de : <https://eandt.theiet.org/2019/04/18/could-quantum-radars-expose-stealth-planes>
- 23 Kyle Mizokami, « China Claims It Developed "Quantum" Radar to See Stealth Planes », *Popular Mechanics*, 22 septembre 2016. Tiré de : <https://www.popularmechanics.com/military/research/a22996/china-quantum-stealth-radar/>
- 24 Nicholas Hardy, Ben Dixon, Jeff Shapiro et Scott Hamilton, *Quantum Illumination Radar Feasibility*, Lincoln Laboratory, Massachusetts Institute of Technology, 2018. Tiré de : <https://apps.dtic.mil/sti/pdfs/AD1132052.pdf>
- 25 Edward Parker, *Commercial and Military Applications and Timelines for Quantum Technology Research*, Research Report, RAND Corporation, 28 octobre 2021. Tiré de : https://www.rand.org/content/dam/rand/pubs/research_reports/RR1400/RR1482-4/RAND_RR1482-4.pdf
- 26 Armée de l'Australie, *Army Quantum Technology Roadmap*, avril 2021. Tiré de : https://researchcentre.army.gov.au/sites/default/files/RD5734_Quantum%20Roadmap%20WEB.pdf
- 27 Edward Parker, *Commercial and Military Applications and Timelines*.
- 28 Elsa B. Kania et John Costello, *Quantum Hegemony?*, Center for a New American Security, 2024. Tiré de : <https://www.cnas.org/publications/reports/quantum-hegemony>
- 29 *Ibid.*
- 30 Rob Portman et Tom Carper, *Threats to the U.S. Research Enterprise: China's Talent Recruitment Plans, Staff Report*, United States Senate, Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs, <https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/2019-11-18%20PSI%20Staff%20Report%20-%20China's%20Talent%20Recruitment%20Plans%20Updated2.pdf> (consulté le 26 novembre 2024).
- 31 *Chinese Defence Universities Tracker*, page d'accueil de 2024. Tiré de : <https://unitracker.aspi.org.au/>
- 32 Edward Parker, Daniel Gonzales, Ajay K. Kochhar, Sydney Litterer, Kathryn O'Connor, Jon Schmid, Keller Scholl, Richard Silberglitt, Joan Chang, Christopher A. Eusebi et Scott W. Harold, *An Assessment of the U.S. and Chinese Industrial Bases in Quantum Technology*, RAND Corporation, 2022. Tiré de : https://www.rand.org/pubs/research_reports/RR4869-1.html
- 33 *Ibid.*
- 34 Matthew Bondy, *AUKUS Is Not Just about Subs: It's about Advanced Technology*, Centre pour l'innovation dans la gouvernance internationale, 10 décembre 2021. Tiré de : <https://www.cigionline.org/articles/aokus-is-not-just-about-subs-its-about-advanced-technology/>
- 35 Aimee Gunther, Peter Mason et Julie Lefebvre, *Stratégie S et T quantique du MDN et des FAC : se préparer à des ruptures technologiques dans l'environnement opérationnel futur*, Recherche et développement pour la défense Canada, CAN SANS CLASSIFICATION, 2021. Tiré de : https://cradpdf.drc-rddc.gc.ca/PDFS/unc356/p812810_A1b.pdf
- 36 Innovation, Sciences et Développement économique Canada, *Consultations sur la Stratégie quantique nationale : Ce que nous avons entendu*, rapport, ISDE, https://ised-isde.canada.ca/site/national-quantum-strategy/sites/default/files/documents/2022-07/1032_06_21_nqs_wwh_report_fr_v7.pdf (consulté le 26 novembre 2024).
- 37 « Here, There and Everywhere », *The Economist*, 2019. Lien initialement trouvé à : <https://www.economist.com/news/essays/21717782-quantum-technology-beginning-come-its-own>