

Quantique et renseignement

Autor(en): **Ventre, Daniel**

Objektyp: **Article**

Zeitschrift: **Revue Militaire Suisse**

Band (Jahr): - **(2021)**

Heft 3

PDF erstellt am: **27.09.2024**

Persistenter Link: <https://doi.org/10.5169/seals-977681>

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.

Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.

Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.



Présentation consolidée de la situation par un officier de renseignement de l'armée de Terre française.

Renseignement

Quantique et renseignement

Daniel Ventre

Docteur en science politique, chercheur au Centre de recherche sur le droit et les institutions pénales, UMR 8183 (CNRS)

Les progrès réalisés par la recherche en physique quantique ouvrent de nouveaux horizons technologiques. On rêve déjà d'ordinateurs quantiques surpassant les capacités de tous les plus gros calculateurs dont le monde dispose aujourd'hui; on rêve aussi d'un Internet quantique et de communications inviolables. Avant d'en arriver là cependant, la R&D devra encore lever de très nombreux obstacles. Les principales puissances de ce monde ont depuis plusieurs années déjà publié leurs feuilles de route en matière de technologies quantiques, associant sur les moyens et long terme les efforts des secteurs public et privé et ambitionnant de construire les fondements d'une nouvelle économie pour le XXI^e siècle. Les enjeux de sécurité et de défense sont au cœur de ces considérations et projets. Dans cet article, nous proposons une brève revue de la littérature internationale qui traite des applications du quantique dans les domaines militaire et du renseignement.

Applications du quantique dans les domaines de la sécurité et de la défense

La littérature semble s'accorder sur les grandes catégories de technologies quantiques qui entreront au service de la sécurité et de la défense. Les taxonomies proposées sont habituellement construites autour de trois ou quatre principales catégories. Le *Department of Homeland Security* (DHS) américain décline ainsi quatre catégories¹: les ordinateurs quantiques, les communications quantiques, les réseaux quantiques et les capteurs quantiques. Le Defense Science Board du Département de la Défense américain identifie quant à lui trois applications majeures dans l'espace militaire:

les capteurs quantiques (sensing), l'informatique quantique (quantum computing) et les communications quantiques.² D'autres travaux déclinent des taxonomies approchantes. Ainsi, dans *La guerre quantique*,³ Michal Krelina retient-il les domaines applicatifs suivants:

- L'informatique quantique et ses applications telles que la simulation de systèmes, l'optimisation; et les simulateurs quantiques (circuits quantiques non programmables). Certains domaines particuliers, comme la logistique, pourraient bénéficier de l'apport des capacités de calcul quantique pour la résolution de problèmes spécifiques (propres aux systèmes complexes et environnement chaotiques, et aux futurs environnements faits de systèmes autonomes et robotisés)⁴. Les principaux enjeux ici se traduisent en termes d'accélération (des calculs, des opérations, de transport des données), de temps réel, de précision, de contrôle temps réel à grande distance.⁵ Les communications quantiques et la cryptographie: réseaux quantiques, composants réseaux, distribution de clé quantique, cryptographie pos-quantique, etc.
- Les communications quantiques ont pour enjeu la sécurisation des communications à l'aide des propriétés de la mécanique quantique.
- Capteurs et métrologie quantique: magnétomètres, gravimètres, mesure du temps, imagerie quantique

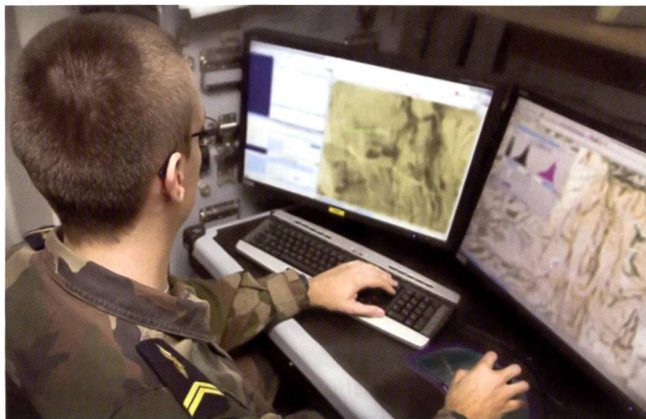
² Defense Science Board, Applications of Quantum Technologies: Executive Summary, October 2019, at <https://dsb.cto.mil/reports.html>

³ Michal Krelina, Quantum Warfare: Definitions, Overview and Challenges, Faculty of Nuclear Sciences and Physical Engineering, Czech Technical University in Prague, mars 2021, 43 pages, <https://arxiv.org/pdf/2103.12548.pdf>.

⁴ Dr. Keith Aliberti and Thomas L. Bruen, Quantum Computation and Communication, Army Logistician, Vol. 8, n°5, septembre 2006, https://alu.army.mil/alog/issues/SepOct06/quantum_comp.html.

⁵ *Ibid.* 4.

¹ DHS, Final Report: Emerging Technologies Subcommittee Quantum Information Science, Homeland Security Advisory Council, Emerging Technology Subcommittee, novembre 2020, 31 pages, États-Unis, https://www.dhs.gov/sites/default/files/publications/final_emerging_technologies_quantom_report_1.pdf.



La planification des opérations nécessite l'accès à des quantités toujours plus importantes de données. Le traitement de celles-ci, leur compression, leur stockage sûr et leur transmission sont des défis qui appellent des solutions et des technologies nouvelles.

(radars, etc.). La métrologie quantique exploite les particularités du quantique pour développer des outils de mesure de très grande précision, avec de potentielles applications dans de nouvelles caméras, radars et systèmes capables par exemple de détecter des avions furtifs ou des sous-marins (imagerie fantôme quantique, gravimétrie quantique). À court terme, les développements intéressants les armées pourraient proposer des outils de navigation de plus grande précision, indispensables aux missions militaires.⁶

Les technologies quantiques sont également vouées à l'hybridation⁷ avec d'autres domaines, tels que l'intelligence artificielle ou le machine learning. Il est déjà question d'IA quantique (Quantum Artificial Intelligence).

Le pouvoir transformatif des technologies quantiques

La combinaison de toutes ces capacités serait de nature à radicalement transformer la conduite de la guerre. Michal Krelina propose une définition de la guerre quantique (Quantum Warfare), qui serait « une guerre utilisant les technologies quantiques pour des applications militaires qui touchent au renseignement, à la sécurité, et aux capacités de défense, de tous les domaines de la guerre ».⁸ La transformation résulterait d'un accroissement de la précision, de la vitesse, de la sécurisation des communications et d'une connaissance accrue de l'environnement. Le quantique est qualifié d'innovation de rupture (en anglais « Disruptive Innovation ») dans les guerres hybrides modernes.⁹

6 John Harper, Pentagon Trying to Manage Quantum Science Hype, *National Defense Magazine*, 2020, <https://www.nationaldefensemagazine.org/articles/2020/12/10/pentagon-trying-to-manage-quantum-science-hype>.

7 International Institute for Strategic Studies, Quantum Computing and Defence, Chapitre I, Partie 3, dans *The Military Balance 2019*, pages 8-20, février 2019, <https://www.iiss.org/publications/the-military-balance/the-military-balance-2019/quantum-computing-and-defence>.

8 *Ibid.* 3.

9 Ralph Thiele, Quantum sciences – a disruptive innovation in hybrid

Au-delà de ces discours annonçant une nouvelle révolution dans les affaires militaires, il paraît à ce stade très difficile d'anticiper les effets du quantique sur la reconfiguration des rapports de force interétatiques, ou entre États et acteurs non étatiques.¹⁰ Quelques questions peuvent cependant être soulevées :

- La suprématie quantique assurera-t-elle celui qui en disposera d'une supériorité stratégique réelle et durable?¹¹
- L'introduction du quantique révolutionnera-t-elle l'art de la guerre à tous les niveaux (tactique, opérationnel et stratégique)?
- Si l'accent est bien mis dans la littérature de défense sur l'effet « multiplicateur de force »¹² de l'introduction du quantique dans les affaires militaires, on perçoit aussi un discours plus alarmiste : le quantique est également une menace. Car le quantique, partagé par les adversaires, introduit naturellement de nouvelles vulnérabilités : nos avions jusqu'alors furtifs vont-ils perdre leur suprématie, les sous-marins nucléaires vont-ils perdre leur invisibilité ? Rendre les océans transparents aurait bien sûr des conséquences stratégiques majeures.¹³
- Qui sera le maître du domaine quantique ? En matière de recherche ces dernières décennies le secteur privé a investi des champs jusqu'alors réservés aux États (pensons à la conquête spatiale) ou a développé des domaines technologiques mettant au défi les pouvoirs de l'État (cyberespace). Aujourd'hui, dans le domaine quantique, l'entreprise privée joue de nouveau un rôle central, en Occident du moins. C'est alors peut-être elle qui détiendra la première les capacités convoitées par le renseignement : capacités de calcul, capteurs, cryptanalyse, réseaux sécurisés, etc.

Les technologies quantiques auront deux versants : défensif et offensif. Elles devraient par exemple permettre de développer des systèmes de communication inviolables, dont les flux ne pourraient être ni interceptés ni déchiffrés. Cette capacité défensive assurerait un avantage considérable.

warfare, Hybrid CoE Working Paper n°7, mars 2020, 12 pages, https://www.hybridcoe.fi/wp-content/uploads/2020/07/Working-Paper-7_2020.pdf.

¹⁰ *Ibid.* 7.

¹¹ *Ibid.* 6.

¹² « La technologie quantique n'apporte pas de technologies ou armes fondamentalement nouvelles, mais augmente considérablement les capacités de mesure, la précision, la puissance et l'efficacité de calcul ». Michal Krelina, *Quantum Warfare: Definitions, Overview and Challenges*, Faculty of Nuclear Sciences and Physical Engineering, Czech Technical University in Prague, mars 2021, 43 pages, <https://arxiv.org/pdf/2103.12548.pdf>.

¹³ Katarzyna Kubiak, Quantum Technology and Submarine Near-Involvement, *Global Security Policy Brief*, décembre 2020, 18 pages, Londres, <https://www.europeanleadershipnetwork.org/wp-content/uploads/2020/12/Quantum-report.pdf>.

L'ordinateur quantique quant à lui devrait offrir, à long terme,¹⁴ des capacités de calcul considérables, permettant de déchiffrer dans des délais désormais raisonnables, des informations classifiées, sensibles ou non classifiées.¹⁵ Cette puissance de cryptanalyse exercée contre des systèmes insuffisamment protégées face aux attaques quantiques, est une arme offensive puissante. La cryptographie post-quantique tentera d'offrir une résistance suffisante aux attaques quantiques.¹⁶

Pour les acteurs du renseignement, les technologies quantiques offrent ainsi des perspectives contradictoires : d'un côté des pans entiers de l'univers des données et des communications seraient rendus inaccessibles (internet

quantique, communications quantiques); de l'autre au contraire la cryptanalyse et les capteurs quantiques ouvriraient les portes vers de nouveaux univers de données jusqu'alors inaccessibles.

Conclusion

Le renseignement et l'art de la guerre seront-ils radicalement transformés par l'arrivée du quantique? La question est somme toute conventionnelle, mais peut paraître encore prématurée au regard de l'état d'avancement de la technologie. Au cours des siècles passés, nombreuses ont été les technologies dites « de rupture » et qui ont impacté tous les niveaux (tactique, opérationnel, stratégique). Mais la réponse ne peut être donnée à l'avance, car les « transformations » ou autres « révolutions » ne sont jamais uniquement suspendues à l'évolution technologique.

D. V.

¹⁴How a quantum computer could break 2048-bit RSA encryption in 8 hours, MIT Technology Review, 30 mai 2019, <https://www.technologyreview.com/2019/05/30/65724/how-a-quantumcomputer-could-break-2048-bit-rsa-encryption-in-8-hours>.

¹⁵Government Accountability Office, National Security: Long-Range Emerging Threats Facing the United States as Identified by Federal Agencies, décembre 2018, at <https://www.gao.gov/assets/700/695981.pdf>.

¹⁶Jon R. Lindsay, Surviving the quantum cryptocalypse, Strategic Studies Quarterly, Summer 2020, pp. 49-73, https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-14_Issue-2/Lindsay.pdf.

La nouvelle app swisstopo
Gardez la vue d'ensemble

- planification et suivis faciles de vos tours
- fonction pratique de guide de parcours
- découvrir le paysage en mode panorama

swisstopo

Photo: Martin Schilliger, Uzwil



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Office fédéral de topographie swisstopo

Téléchargez maintenant gratuitement
www.swisstopo.ch/app



Conçu pour protéger. Performance éprouvée.

Une vision partagée. Une mission commune. Un partenariat idéal offrant une solution éprouvée pour aider la Suisse dans la défense de sa souveraineté, et renforcer son industrie. Avec le système Patriot,[®] la Suisse rejoindra sept nations européennes bénéficiant des avantages d'une défense aérienne moderne et performante.



Image: Poste de commande Patriot Suisse



rtxdefense.co/suissepatriot



Le lanceur n'est qu'une composante d'un système complexe, fonctionnant en réseau.

Défense aérienne

Raytheon Technologies système sol-air *Patriot*® - La défense aérienne dans une classe à part et une valeur ajoutée pour l'économie suisse

Raytheon

Publireportage

Les candidats pour un système de défense aérienne sol-air à longue portée (BODLUV GR) ont soumis leur deuxième offre à armasuisse le 18 novembre 2020. L'agence pour l'armement a désormais commencé à travailler sur les rapports d'évaluation, qui doivent être achevés au premier trimestre 2021. [1]

Les offres contiennent entre autres les éléments suivants :

- Prix des systèmes de défense aérienne au sol à longue portée pour couvrir une zone d'au moins 15'000 km², y compris la logistique et l'armement définis comme point de départ contraignant pour des négociations détaillées avec le candidat sélectionné, après la décision sur le type ;
- Offres de coopération entre les forces armées et les autorités d'acquisition en Suisse et celles du pays fournisseur ;
- Projets de compensation prévus ou déjà lancés. [1]

Les gouvernements et constructeurs des pays suivants ont participé à l'évaluation d'un nouveau système de défense aérienne au sol: la France (Eurosam avec le système SAMP/T) et les Etats-Unis d'Amérique (Raytheon Technologies avec le système *Patriot*).

Raytheon Technologies *Patriot*

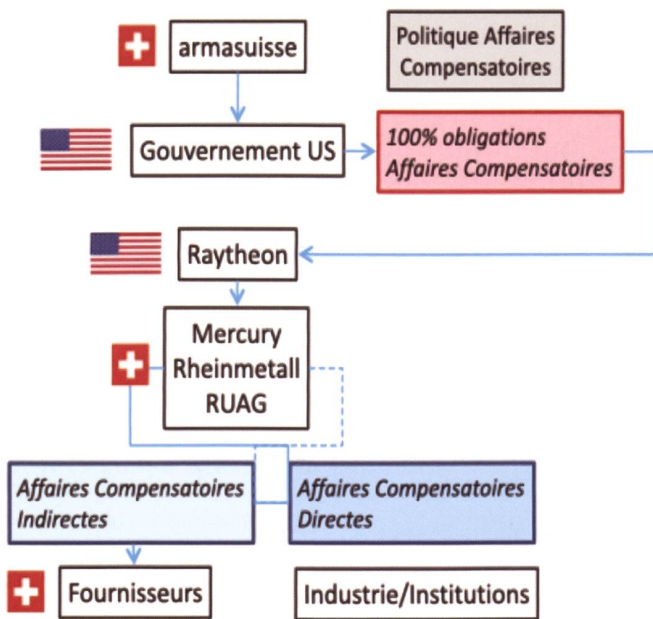
Actuellement, 17 utilisateurs utilisent le système *Patriot* à travers le monde, dont sept en Europe.

Patriot peut être mis en oeuvre rapidement et garantir la protection de zones importantes tous azimuts, contre les menaces de la 3^e dimension. Avec son puissant radar de contrôle de tir et ses missiles guidés GEM-T très rapides, les menaces sont enregistrées avec précision, suivies et combattues rapidement. Etant donné que la cible est suivie à la fois par le radar de contrôle de tir et par le radar de poursuite logé dans la pointe de l'engin guidé, un haut niveau de sécurité contre les contre-mesures électroniques

est garanti. En plus de son efficacité dans le combat défensif contre un large éventail de menaces aériennes, le système *Patriot* impressionne par sa rentabilité. La communauté d'utilisateurs de *Patriot System* s'assure soigneusement que le système est régulièrement mis à jour. A cet effet, un *pool* de financement commun a été créé dans lequel chaque pays utilisateur participe proportionnellement au nombre d'unités de feu en service. La Suisse bénéficierait également de cette communauté d'utilisateurs. Si à l'avenir notre armée exploitait des unités de tir *Patriot*, elle n'aurait par conséquent à contribuer qu'à une très faible part des coûts de développement et de maintenance ultérieurs. De cette manière, la Suisse peut bénéficier des mêmes mises à jour que les utilisateurs qui possèdent une part plus élevée du financement.

Valeur ajoutée pour l'économie suisse grâce à des opérations de compensation

Sur la base des principes du Conseil fédéral pour la politique d'armement du DDPS et de la stratégie d'armement, armasuisse a défini dans la politique de compensation la mise en œuvre et l'évaluation des *offsets* pour l'acquisition de matériel de guerre à l'étranger. Afin de protéger ses intérêts essentiels en matière de sécurité, la Suisse dépend d'une technologie et d'une base industrielle efficaces en matière de sécurité (STIB). Afin de renforcer la STIB, les compensations devraient lui donner accès aux technologies, au savoir-faire et aux marchés étrangers. [2] Les compensations directes sont principalement entendues comme des transactions qui sont directement liées à l'achat d'armements. Des compensations directes sont effectuées lorsque des capacités ou des compétences et des connaissances sont créées, qui contribuent à la plus grande autonomie de maintenance possible, au maintien et à l'augmentation de la valeur d'un système, de même qu'à l'augmentation des capacités de l'armée et des capacités de base de l'industrie d'armement et de matériels de sécurité.



Organisation des offsets.

Les compensations indirectes ne concernent pas spécifiquement l'achat d'armements. Ce type de participation industrielle concerne principalement les commandes industrielles, les activités de financement liées à la compensation, les transferts de connaissances et de technologies, les développements communs, le support marketing/commercial, etc. Pour mettre en œuvre ces compensation obligatoires, Raytheon Technologies a décidé de conclure un partenariat avec la société zurichoise Rheinmetall Air Defence AG. Rheinmetall continue de fabriquer des systèmes de défense aérienne au sol à courte portée à ce jour. Une collaboration entre Raytheon Technologies et Mercury Systems, basée dans le canton de Genève, existe depuis longtemps. De quel genre d'emplois s'agit-il exactement? En plus d'autres entreprises, Rheinmetall Air Defence et Mercury Systems de Raytheon Technologies fabriqueraient certains composants du système *Patriot*. Le nombre de composants à livrer dépasse la demande suisse, ce qui génère des commandes supplémentaires et une valeur ajoutée à long terme. De telles transactions comptent comme une compensation directe. L'entreprise nationale d'armement RUAG, basée à Berne, est également chargée des travaux de maintenance et de réparation. Les innombrables fournisseurs basés en Suisse bénéficient également indirectement de Rheinmetall Air Defence et Mercury Systems. Les entreprises -y compris de nombreuses PME- de toutes les régions du pays et des régions linguistiques bénéficient des accords de compensations directs.

Pourquoi de telles opérations de compensation sont-elles si importantes pour l'industrie suisse? Elles signifient que l'industrie suisse peut bénéficier du transfert de nouvelles technologies, ce qui lui permet de rester compétitive



sur le marché international. Un pays neutre comme la Suisse en dépend, car il n'est pas autorisé à conclure des partenariats militaires avec d'autres nations.

Grâce aux accords de compensation en cas d'achat du système *Patriot*, Rheinmetall Air Defence et Mercury Systems pourront continuer à développer et à fabriquer des technologies de pointe sur les sites de Zurich et de Genève. Les différents instituts de recherche et universités suisses bénéficient également du transfert de connaissances et de technologies.

Suite du programme Air2030

Avec les informations de la deuxième offre et les résultats des différentes évaluations, l'avantage global de chaque système est déterminé. Les résultats sont accompagnés d'une analyse complète des risques dans des rapports d'évaluation indépendants, où les avantages globaux respectifs du nouveau système de défense aérienne au sol à longue portée sont comparés aux coûts d'acquisition et d'exploitation sur une durée de 30 ans. Les rapports d'évaluation devraient être achevés au premier trimestre 2021. Le choix du système par Conseil fédéral est prévu pour le deuxième trimestre 2021. [1]

Sources :

[1] Communiqué de presse du DDPS du 18 novembre 2020 <https://www.vbs.admin.ch/content/vbs-internet/de/dieschweizer-armee/sicherheit-im-luftraum.detail.nsb.html> / 81207. Html

[2] Offset - Office fédéral de l'armement armasuisse <https://www.ar.admin.ch/de/beschendung/ruestungspolitik-des-bundesrates/offset.html>