L'Intelligence Artificielle et les Technologies Quantiques au regard de la Cybersécurité - Introduction

Artificial Intelligence and Quantum Technologies in relation to Cybersecurity - Introduction

Laurent Adatto[1], Fehmi Jaafar[2], Schallum Pierre[3]

[1] Laboratoire ISI/Lab RII, Université du Littoral, Côte d'Opale, France, lradatto@yahoo.com
[2] Département d'informatique et de mathématique, Université du Québec à Chicoutimi, Québec, Canada, fehmi.jaafar@uqac.ca
[3] Institut intelligence et données (IID), Université Laval, Québec, Canada, schallum.pierre@iid.ulaval.ca

RÉSUMÉ. Le présent texte est une introduction au numéro spécial "L'Intelligence Artificielle et les Technologies Quantiques au regard de la Cybersécurité" de la revue "Technologie et innovation". Il propose un développement des thématiques au cœur de ce numéro, une contextualisation des éléments liés, ainsi qu'une présentation de tous les articles constituant le numéro spécial.

ABSTRACT. This paper is an introduction to the special issue "Artificial Intelligence and Quantum Technologies in relation to Cybersecurity" from the journal "Technology and Innovation". It proposes a development of the themes at the heart of this issue, a contextualization of the related elements, as well as a rundown of all the articles constituting the special issue.

MOTS-CLÉS. Intelligence artificielle, Technologies quantiques, Cybersécurité, Technologies de l'information et de la communication, Numérique, Innovation.

KEYWORDS. Artificial Intelligence, Quantum Technologies, Cybersecurity, Information and Communication Technologies, Digital, Innovation.

Le numéro présent de la revue « Technologie et innovation » a pour thèmes l'Intelligence Artificielle et les Technologies Quantiques au regard de la Cybersécurité, et par extension les éléments concourants relatifs à la révolution numérique en cours.

Le concept de cybersécurité se réfère à la confidentialité, l'intégrité et la disponibilité des données ou services informatiques, ainsi qu'à l'infrastructure qui les supporte [KRE 19]. L'un des enjeux d'envergure en cybersécurité pour les organisations réside pour la communauté des chercheurs dans les avancées majeures relatives à l'IA et aux technologies quantiques.

En effet, l'IA, en tant qu'ensemble de techniques et de méthodes de développement de systèmes informatiques, vise à reproduire des activités qui ressemblent à l'intelligence humaine parmi lesquelles le raisonnement logique, la reconnaissance des formes, l'apprentissage [DEG 17]. Durant les dernières années, l'IA a été appliquée à une multitude de domaines dont l'informatique ubiquitaire [ANT 19], l'imagerie médicale [BRU 19] et la cybersécurité [HER 19]. De plus en plus d'équipes de recherche mettent en œuvre des approches de cybersécurité utilisant l'IA [VEN 20]. De même, les pirates informatiques peuvent tirer profit de l'IA pour perfectionner leurs attaques et développer des *malwares* plus efficaces [BER 15]. En ce sens, l'apprentissage automatique et les réseaux de neurones sont mis à contribution pour amplifier les cyberattaques [LI 20].

Outre l'impact de l'IA sur la protection des données, il est reconnu que l'arrivée des ordinateurs quantiques menace tous les systèmes de cybersécurité actuels [NAT 19]. Néanmoins, les systèmes quantiques pourraient constituer un moyen fiable pour garantir l'intégrité des données transportées

dans les plateformes distribuées [FED 17]. Les technologies quantiques recèlent un potentiel considérable de progrès apte à façonner, et au-delà révolutionner, la société de demain. Et cela suivant de nombreux secteurs d'application et en lien à de multiples vecteurs : calculateurs quantiques, infrastructures (réseaux et câblages spécifiques) de la communication quantique, simulateurs et technologies habilitantes, dispositifs nécessaires au développement du futur ordinateur quantique universel à la puissance de calcul sans commune mesure et ouvrant la voie à la "suprématie quantique" [HAR 17]. En plus du développement des machines, un parallèle façonnement de l'expertise et des savoirs quantiques, des progrès de la recherche fondamentale à ceux de l'algorithmie et de la programmation quantique, et de la cryptographie post-quantique (capable de résister à la puissance de déchiffrement quantique) à la cryptographie purement quantique [PIR 19], reposant notamment sur la propriété d'intrication singulière du domaine quantique.

Les technologies quantiques mettent en œuvre les propriétés de la physique quantique, opérantes à l'échelle de l'infiniment petit. Ainsi, le domaine quantique est caractérisé par des modifications d'états par sauts et suivant un *quantum*, ou quantité indivisible, *a contrario* de la progressivité des changements d'états de la physique classique. De plus, et toujours de façon inédite par rapport à la théorie classique, un objet quantique peut revêtir plusieurs états simultanés suivant des probabilités différenciées (superposition quantique) et un système quantique formé de deux objets physiquement séparés peut être corrélé par les mêmes états quantiques (intrication quantique). Ainsi, de sa découverte fondamentale au début du XXe siècle jusqu'à ses progrès théoriques et applicatifs, le domaine quantique constitue une matrice d'innovations radicales.

Pour prendre la mesure de ce large champ d'innovations, de nombreux États, à la suite de plans stratégiques en IA, mettent en œuvre des programmes d'investissements de haut niveau concernant les technologies quantiques. À titre d'exemple, le Plan Quantique français présenté en janvier 2021 dont l'enveloppe atteint les 1,8 milliard d'euros sur cinq ans. Ainsi, la France rejoint les États investissant les plus massivement dans ces technologies, comme les États-Unis, la Chine, l'Allemagne et le Canada. À cela viennent aussi s'ajouter les développements et investissements de R&D des *startups* construites sur des projets quantiques innovants et des firmes numériques les plus puissantes, dont IBM et Google.

Dans le but d'étendre l'exploration de ces thématiques, ce numéro de la revue « Technologie et innovation » comprend les articles dont voici les présentations.

L'article « Les risques liés à l'innovation : le cas de l'intelligence artificielle » de Arvind Ashta et Vipin Mogha propose une analyse des risques induits par les innovations portées par l'IA en termes économiques, incluant les perspectives de marché, de compétitivité et concernant le secteur du travail, tandis que d'autres peuvent être simplement des craintes de changements sociaux. En particulier en lien à leur étude sur l'avènement de l'IA, les auteurs mettent en exergue plusieurs écueils liés à ce domaine d'innovation en relation aux domaines sociétaux. En outre, ils proposent une discussion sur la balance bénéfices risques de cette révolution numérique portée par toujours plus d'IA.

L'article « Les hackers dans la science-fiction, entre résistance héroïque et criminalité » de Thomas Michaud développe une analyse de la notion de hackers et des imaginaires liés. En ce dessein, l'auteur propose une historiographie de l'évolution du concept depuis son apparition dans les années 1960. Les grandes œuvres ayant contribué à bâtir et faire évoluer la notion de hacker sont convoquées et analysées. Est montré comment les éléments rattachés aux hackers ont créé des imaginaires populaires et de très nombreuses vocations dans le domaine de l'ingénierie informatique et des réseaux numériques. L'auteur montre en outre au travers son travail de recherche comment tout le secteur de la cybersécurité a été façonné au plus profond par le concept, les schémas de pensées et les réalisations des hackers.

L'article « Quand les crypto-monnaies rivalisent avec la monnaie souveraine » d'Abdellah Belmadani analyse les implications de l'apparition des crypto-monnaies et de leur progression continue. L'auteur montre comment ce type de monnaie innovante prend place au côté des monnaies historiques et fiduciaires. Il met en lumière que les crypto-monnaies par essence décentralisées peuvent échapper aux réglementations et comment cette innovation interroge les autorités monétaires internationales sur la pérennité du rôle des banques centrales et l'impact sur la stabilité financière. L'article analyse les prospectives de développements des crypto-monnaies liées à des innovations technologiques qui ne feront que s'améliorer et prendre de l'ampleur. L'auteur met en exergue le défi ainsi lancé aux autorités de régulation par ces crypto-monnaies fonctionnant suivant des processus cryptographiques novateurs.

Avec l'article « Repérez le piratage : Systèmes de détection d'intrusion pour réseaux avioniques en utilisant l'apprentissage automatique », Fehmi Jaafar propose avec une équipe de recherche affiliée au Centre de Recherche Informatique de Montréal et à l'Université de Québec, les résultats d'un projet qui était fait dans le cadre du programme « Innovation pour la défense, l'excellence et la sécurité du ministère de la Défense nationale et les Forces armées canadiennes » (MDN/FAC). L'article décrit une méthode à base de réseaux de neurones pour inférer des modèles approximant la norme militaire de bus MIL-STD-1553 qui est utilisé couramment dans des aéronefs et d'autres équipement d'utilisation critique pour échanger des renseignements avioniques, comme l'altitude, la position et la vitesse. Après l'étude de différentes options architecturales, est utilisé LogBERT pour la détection d'anomalies sur un bus MIL-STD-1553 simulé. LogBERT a montré des performances prometteuses sur les traces d'exécutions qui lui ont été fournies. Cela permettra la création de Systèmes de Détection d'Intrusions (SDI) efficaces pour les réseaux avioniques et les technologies de bus utilisés dans l'industrie spatiale et aérospatiale.

L'article « Le principe de nécessité ou de minimisation des données comme condition à l'innovation responsable : données de qualité, vie privée, cybersécurité et environnement » de Schallum Pierre montre comment dans le cadre de l'utilisation des données numériques, nécessité et minimisation d'usage et d'accès à ces données forment une nouvelle éthique de pratique. Celle-ci est promue par des organismes veillant au respect des droits numériques dont la CNIL (Commission nationale informatique et libertés) en France et son homologue au Québec, la CAI (Commission d'accès à l'information), dont les éléments impartis sont étudiés dans cet article. Les implications du principe de nécessité ou de minimisation des données sont analysées. Les impacts sont mis en lumière. Enfin, la portée du principe est décrite et étendue aux secteurs de la cybersécurité, de la vie privée, de l'environnement et de l'innovation.

Avec l'article « Invisible Force, une science-fiction institutionnelle sur la guerre de l'information du futur », Thomas Michaud propose une prospective des manières dont les opinions publiques peuvent être manipulées par les réseaux numériques, sociaux et les *fake news*, situations déjà très avancées aujourd'hui, mais qui plus est demain amplifiées par une intelligence artificielle encore plus développée. Ainsi cette IA sera en mesure d'avoir un poids des plus prépondérants dans cette guerre de l'information numérique de tous les instants. Dans cette perspective, l'auteur analyse en profondeur l'œuvre référence anticipatrice de bande-dessinée américaine « Invisible Force », modèle de science-fiction de qualité sur ce sujet. De plus, l'auteur agrémente ses développements par la mise en exergue de rapports des plus grands experts du sujet. L'article fournit une grille de lecture prospectiviste en particulier utile pour les chercheurs, décideurs et stratèges. Dans cette voie, l'auteur montre la façon dont la science-fiction peut avoir une aptitude à influencer et façonner les esprits, de son premier public de lecteurs et spectateurs, aux opinions publiques élargies, jusqu'aux gouvernants et états majors militaires. Avec, au cœur de la matrice de cette analyse, le rôle de plus en plus prééminent de l'IA.

L'article de Laurent Adatto « Enjeux et prospectives du développement des technologies quantiques » met en œuvre une étude approfondie du secteur des technologies quantiques. Tout

d'abord, les éléments matriciels de la physique quantique sont analysés pour leurs rôles liés aux développements des technologies quantiques. Ces analyses sont développées de façon didactique pour intéresser, au-delà d'un public ingénieur, tous les esprits souhaitant s'enquérir de ces éléments scientifiques au rôle primordial dans le façonnement des technologies quantiques. Ensuite, une étude de cas est entreprise concernant le Plan Quantique français lancé en 2021. Les analyses liées concernent les très nombreux éléments, technologies et acteurs publics et privés, impliqués dans ce grand plan d'investissement à haute portée modernisatrice et apte à façonner l'univers industriel et numérique de demain. En outre, les autres plans d'investissements d'envergure des acteurs internationaux relatifs aux technologies quantiques sont mis en exergue et comparés. Au-delà des États procédant à ces investissements à hauteurs de milliards, les développements quantiques des géants du numérique sont aussi étudiés, tant des firmes telles Google et IBM ont des capacités technologiques, humaines, financières, ainsi que des labos de R&D de qualité optimum, aptes à rivaliser avec ceux des États impliqués à pourtant très grande échelle dans les investissements quantiques. Ainsi une large analyse prospective est dressée quant à l'évolution des technologies quantiques et à leur prépondérance en marche dans une variété très large de domaines. En particulier celui de la cybersécurité que les technologies quantiques, au fil de leurs progrès et montées et puissance, s'apprêtent à révolutionner, comme l'essentiel des implications ayant trait au numérique du monde qui vient.

Bibliographie

[ANT 19] ANTOINE-SANTONI T., POGGI B., VITTORI E., VAN HIEU H., ARAUJO D., AIELLO A., Vers un système d'information pervasif pour un Smart Village. In *Evolution des SI: vers des SI Pervasifs ?*, Juin 2019, Université Paris 1 Panthéon-Sorbonne, Paris, 2019.

[BER 15] BERTHIER T., « Hacktivisme : vers une complexification des cyberattaques », *Revue Défense Nationale*, 9: 45-48, 2015.

[BRU 19] BRUNELLE F., BRUNELLE P., « Intelligence artificielle et imagerie médicale : Définition, état des lieux et perspectives », *Bulletin de l'Académie Nationale de Médecine*, 203, no. 8-9: 683-687, 2019.

[DEG 17] DE GANAY C., GILLOT D., Pour une intelligence artificielle maîtrisée, utile et démystifiée. *Report, Office parlementaire d'évaluation des choix scientifiques et technologiques*, 2017.

[FED 17] FEDRICI B., Solutions évolutives pour les réseaux de communication quantique. PhD diss., *Université Côte d'Azur*, 2017.

[HAR 17] HARROW A., MONTANARO A., « Quantum computational supremacy », *Nature*, 549, 203-209, 2017.

[HER 19] HERMANN G., « IA et cybersécurité : une boucle émergente de rétroactions », *Revue Défense Nationale*, 6: 131-137, 2019.

[KRE 19] KREMER S., MÉ L., RÉMY D., ROCA V., Cybersecurity: Current challenges and Inria's research directions, *Inria white book*, Inria, January 2019, no. 3, 172 p., 2019.

[LI 20] LI L., THAKUR K., ALI M.L., « Potential Development on Cyberattack and Prospect Analysis for Cybersecurity », 2020 IEEE International IOT, *Electronics and Mechatronics Conference*.

[NAT 19] NATIONAL ACADEMIES OF SCIENCES, ENGINEERING, AND MEDICINE, *Quantum computing: progress and prospects*. National Academies Press, 2019.

[PIR 19] PIRANDOLA S., ANDERSEN U.L., BANCHI L., BERTA M., BUNANDAR D., COLBECK R., ENGLUND D., GEHRING T., LUPO C., OTTAVIANI C., PEREIRA J., RAZAVI M., SHAARI J.S., TOMAMICHEL M., USENKO V.C., VALLONE G., VILLORESI P., WALLDEN P., Advances in Quantum Cryptography. *Quantum Physics and Information Technology*, 2019.

[VEN 20] VENTRE D., *Intelligence artificielle, cybersécurité et cyberdéfense, Vol. 2*. Série Cybersécurité, ISTE Éditions, 2020.