e-Revues en libre accès
Online Journals in Open Access

Technologie et innovation

Technology and Innovation

iSTE OpenScience
27-37 St George's Road
London SW19 4EU — United Kingdom
+44 208 879 4580 – www.openscience.fr

Appel à articles

Technologie et Innovation
https://www.openscience.fr/Technologie-et-innovation

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

Co-directeurs du numéro spécial (par ordre alphabétique) :
ADATTO Laurent, JAAFAR Fehmi, PIERRE Schallum

La revue *Technologie et Innovation* lance un appel à contributions à toute partie prenante de la recherche, de la science et de l'entreprise concernée par l'analyse des enjeux connexes à l'Intelligence Artificielle (IA) et aux Technologies Quantiques sous l'angle de la Cybersécurité. Les articles, qui feront l'objet d'une évaluation par des pairs, devront comporter de 6000 à 8000 mots et être rédigés en français.

Dans le cadre de cette publication, 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 (Kremer *et al.*, 2019). 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 (De Ganay et Gillot, 2017). Durant les dernières années, l'IA a été appliquée à une multitude de domaines dont l'informatique ubiquitaire (Antoine-Santoni *et al.*, 2019), l'imagerie médicale (Brunelle et Brunelle, 2019) et la cybersécurité (Hermann, 2019). De plus en plus d'équipes de recherche mettent en œuvre des approches de cybersécurité utilisant l'IA (Ventre, 2020). De même, les pirates informatiques peuvent tirer profit de l'IA pour perfectionner leurs attaques et développer des *malwares* plus efficaces (Berthier, 2015). En ce sens, l'apprentissage automatique et les réseaux de neurones sont mis à contribution pour amplifier les cyberattaques (Li *et al.*, 2020).

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 (*National Academies of Sciences, Engineering, and Medicine*, 2019). Néanmoins, les systèmes quantiques pourraient constituer un moyen fiable pour garantir l'intégrité des données transportées dans les plateformes distribuées (Fedrici, 2017). 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" (Harrow et Montanaro, 2017). En plus du développement

e-Revues en libre accès
Online Journals in Open Access
Technologie et innovation
Technology and Innovation
27-37 St George's Road
London SW19 4EU — United Kingdom
+44 208 879 4580 – www.openscience.fr

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 (Pirandola *et al.*, 2019), 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.

Ce numéro spécial entend réunir autant les travaux relevant de la recherche fondamentale qu'appliquée. La publication pourra ainsi accueillir des contributions liées aux différents domaines concernés selon les prismes (et sans les limiter) de l'ingénierie, de la programmation, de l'algorithmie, de l'économie, de la gestion de l'innovation, des stratégies de R&D des entreprises, de l'analyse des programmes d'investissements régionaux, du passage de la recherche fondamentale à la valorisation industrielle et commerciale des applications, de l'impact environnemental et des questions éthiques en lien à ces progrès technologiques.

Date limite de soumission : 15 février 2022

Adresse de soumission : techin.ia.quantique.cybersecurite@gmail.com

Consignes aux auteurs : https://www.openscience.fr/Auteurs

e-Revues en libre accès
Online Journals in Open Access
Technologie et innovation
Technology and Innovation
27-37 St George's Road
London SW19 4EU — United Kingdom
+44 208 879 4580 – www.openscience.fr

Références :

Antoine-Santoni, T., Poggi, B., Vittori, E., Van Hieu, H., Araujo, D., & Aiello, A. (2019) 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.

Berthier, T. (2015) Hacktivisme: vers une complexification des cyberattaques. *Revue Défense Nationale*, 9: 45-48.

Brunelle, F., & Brunelle, P. (2019) Intelligence artificielle et imagerie médicale: Définition, état des lieux et perspectives. *Bulletin de l'Académie Nationale de Médecine*, 203, no. 8-9: 683-687.

De Ganay, C., & Gillot., D. (2017) Pour une intelligence artificielle maîtrisée, utile et démystifiée. *Report, Office parlementaire d'évaluation des choix scientifiques et technologiques*.

Fedrici, B. (2017) Solutions évolutives pour les réseaux de communication quantique. PhD diss., *Université Côte d'Azur*.

Harrow, A., & Montanaro, A. (2017) Quantum computational supremacy. *Nature*, 549, 203-209.

Hermann, G. (2019) IA et cybersécurité: une boucle émergente de rétroactions. *Revue Défense Nationale*, 6: 131-137.

Kremer, S., Mé, L., Rémy, D., & Roca., V. (2019) Cybersecurity: Current challenges and Inria's research directions. *Inria white book*, Inria, January 2019, no. 3, 172 p.

Li, L., Thakur, K., & Ali, M.L. (2020) Potential Development on Cyberattack and Prospect Analysis for Cybersecurity, 2020 IEEE International IOT, *Electronics and Mechatronics Conference*.

National Academies of Sciences, Engineering, and Medicine. (2019) *Quantum computing: progress and prospects*. National Academies Press.

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. (2019) Advances in Quantum Cryptography. *Quantum Physics and Information Technology*.

Ventre, D. (2020) *Intelligence artificielle, cybersécurité et cyberdéfense, Vol. 2*. ISTE Group.