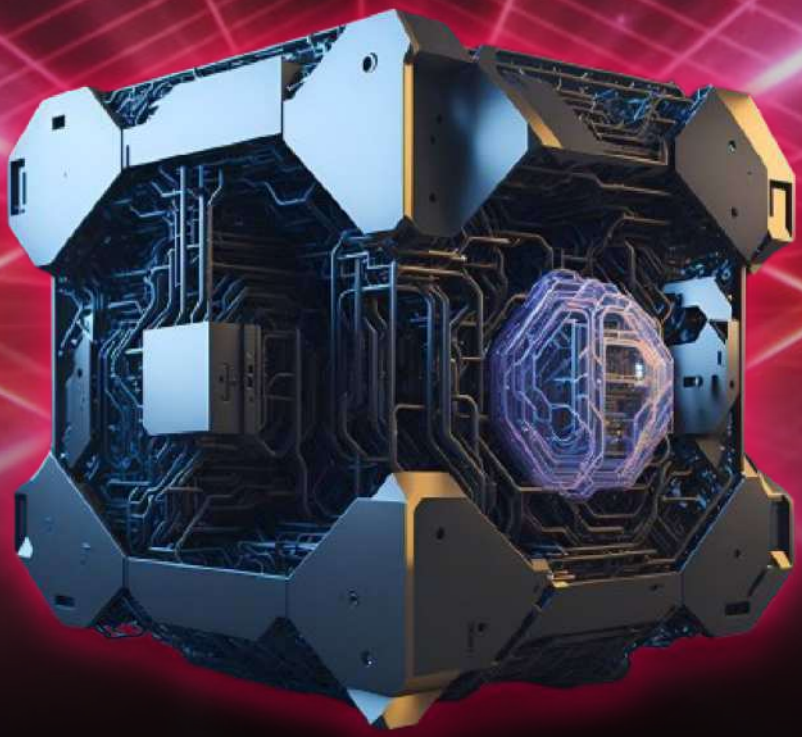
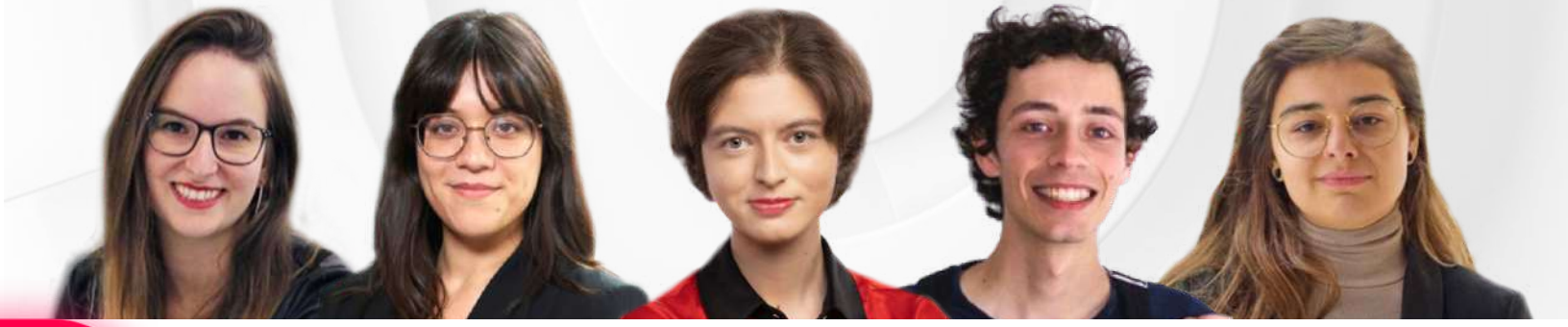
5 DÉCEMBRE 2024 | REVUE BIMENSUELLE NO. 8 | 42 PAGES

LES CONNECTEURS

Le mag québécois sans frontières pour tout savoir sur la révolution techno



COMPRENDRE LA SCIENCE QUANTIQUE : UNE RÉVOLUTION À NOS PORTES



LES CONNECTEURS

5 DÉCEMBRE 2024

Direction éditoriale et artistique, et idée originale
Chloé-Anne Touma
catouma@lesconnecteurs.ca

Édition
CScience Le Lab
contact@lesconnecteurs.ca
405 Av. Ogilvy #101, Montréal, Quebec H3N 1M3

Direction générale
Jonathan Chodjaï
chodjai@lesconnecteurs.ca

Reportages
Axel Dansereau Macias
Chloé-Anne Touma
Fanny Tan
Roxanne Lachapelle
Sacha Israël

Chroniques
Julien Teste-Harnois
Isabelle Lacroix
Michel Savard
Quentin Hibom
René-Sylvain Bédard

ON VEUT VOUS LIRE !

Comment la révolution technologique change-t-elle votre vie au quoditien?
Pour témoigner, nous proposer un sujet, nous poser une question ou publier une annonce, écrivez-nous à contact@lesconnecteurs.ca

Dossier | Cybersécurité et quantique : de nouveaux défis à relever

LES BONS CYBER RÉFLEXES DE JULIEN

SECTION DÉBAT + COURRIER DU LECTEUR

Mise à jour et réflexion collective nécessaires sur le domaine quantique

Chloé-Anne Touma
Rédactrice en chef, LES CONNECTEURS
catouma@lesconnecteurs.ca

Le Québec se positionne aujourd'hui comme un acteur incontournable de la révolution quantique. Avec des investissements massifs et une vision ambitieuse, notre province s'impose comme un leader dans ce domaine, qui promet de transformer radicalement notre société. Mais comment s'opèrera ce changement? Qu'est-ce que vraiment l'innovation quantique? Comment l'arrimer avec la recherche responsable? Quelles en seront vraiment les retombées? Qui en profitera et dans quels milieux? Et quels risques faut-il aussi entrevoir, par exemple, en matière de cybersécurité? Ce sont certaines des questions auxquelles s'attardent à répondre nos journalistes et chroniqueurs, dans ce numéro de LES CONNECTEURS destiné aux lecteurs de tous niveaux de connaissance, allant des novices aux experts. Dressant le portrait global de l'écosystème de la recherche et de l'innovation en quantique, pour vous mettre à jour, ce numéro se veut aussi contribuer à démocratiser les savoirs, démystifier la science quantique, justifier son intérêt et nourrir la réflexion collective.

COMMENT ARRIMER LA RECHERCHE ET L'INNOVATION?

L'informatique quantique, en particulier, suscite de grands espoirs. Ses capacités de calcul exponentielles laissent entrevoir des avancées majeures dans des domaines aussi variés que la pharmacologie, les transports ou encore la cybersécurité. Mais pour que cette promesse se concrétise, il incombe aux élites et institutions qui en ont le pouvoir de travailler à démocratiser l'accès aux ressources quantiques auprès d'autres entreprises et organismes, chercheurs et communautés, et d'intégrer l'ensemble de la société aux échanges visant à favoriser une innovation axée sur les vrais besoins sociétaux. La création de la zone d'innovation quantique de Sherbrooke, Distriq, témoigne de cette volonté de rapprocher le monde académique et l'industrie. Ce pôle public-privé favorisera non seulement le transfert de connaissances, mais aussi l'émergence d'un écosystème dynamique capable de transformer les découvertes scientifiques en innovations commercialisables.

« On crée des emplois dans un domaine d'avenir, les sciences quantiques ; c'est quand même extraordinaire! », a d'ailleurs soutenu le premier ministre François Legault, au micro de LES CONNECTEURS.

Certes, l'avenir quantique du Québec est prometteur, mais il repose sur notre capacité à relever collectivement ces défis. Chercheurs, entrepreneurs, décideurs politiques, médias et citoyens : nous avons tous un rôle à jouer dans cette aventure. En favorisant le dialogue, la collaboration et l'ouverture, nous pourrons pleinement exploiter le potentiel de cette technologie révolutionnaire.

La révolution quantique n'est pas seulement une question de qubits. C'est avant tout une opportunité de repenser notre approche de l'innovation, de la recherche et du progrès technologique. En embrassant cette vision holistique et collaborative, le Québec ne se contente pas de participer à la révolution quantique : il contribue à la façonner, pour le bénéfice de tous.

Alors que nous nous engageons dans cette ère quantique, gardons à l'esprit que notre plus grande force réside dans notre capacité à travailler ensemble, à partager nos connaissances et à rester ouverts aux possibilités infinies que cette technologie nous offre. C'est ainsi que nous transformerons la promesse quantique en une réalité tangible, au service du progrès et du bien-être de notre société.

Notre prochaine émission C+Clair, qu'il sera possible de visionner sur nos tribunes dès le 11 décembre, portera justement sur la thématique « Quantique responsable : comment arrimer la recherche et l'innovation? ». C'est la question à laquelle répondront nos invités : Anne-Marie-Soleil Bernard, Alexandre Blais, Jean-Pierre Perreault, Philippe Cadieux, Michel Pioro-Ladrière, Étienne Grondin, Elsa Paukovics et Martin Laforest, au cours d'un épisode inédit d'une heure. Trois axes y seront abordés : 1) l'importance du dialogue, à renforcer entre acteurs, disciplines et milieux de la société, 2) la démocratisation des ressources et infrastructures, et 3) la responsabilité sociale. Vous en aurez un avant-goût en consultant, dans ce numéro, le voxpop de notre journaliste Axel Dansereau Macias, qui prend le pouls des connaissances de la population quant à la science quantique, la chronique de la professeure Isabelle Lacroix sur la notion de dialogue en recherche, le reportage de notre journaliste Sacha Israël, qui fait un tour d'horizon des acquis du Québec en matière de quantique, et beaucoup d'autres contenus inédits.

Aperçu de l'émission C+Clair portant sur la thématique « Quantique responsable : comment arrimer la recherche et l'innovation? », produite par LES CONNECTEURS, en partenariat avec l'Université de Sherbrooke.

VOIR TOUS LES NUMÉROS

Que savent les Québécois de la science quantique ?

Axel Dansereau Macias
Journaliste, LES CONNECTEURS

Est-ce que le dialogue passe bien entre les scientifiques et les Québécois? Est-ce qu'ils comprennent ce que font les chercheurs? Et, surtout, est-ce qu'ils comprennent les nuances entre physique quantique et ordinateur quantique? Ce que ça mange en hiver? Notre journaliste Axel Dansereau Macias est allé à la rencontre de Québécois pour connaître leur perception. Découvrez son voxpop en primeur dans ce numéro de LES CONNECTEURS! Vous pourrez voir le milieu de la recherche quantique y réagir sur le plateau de notre émission C+Clair, en visionnant l'épisode du 11 décembre prochain, bientôt en ligne sur la plateforme lesconnecteurs.ca.

« X-Men en parle, c'est le film Marvel (...) Il peut se rapetisser à l'infiniment petit! »

« Le problème majeur, si je me souviens bien, c'est la portabilité. »

« Non, la physique quantique ne me fait pas peur. Je pense qu'elle va ouvrir des portes à l'innovation et la création de nouvelles technologies importantes dans notre société. »

« Comme c'est flou pour moi, ça me fait un peu peur! »

« « Moi, ça me fait pas peur, comparé à l'IA. » »

« C'est un truc qui calcule super vite, et dans ma tête, c'est énorme, mais je ne sais pas si c'est vrai... »

« La physique quantique, ça me fait penser aux ordinateurs quantiques, à la mécanique quantique découverte par Albert Einstein. »

L'ordinateur quantique pour les nuls : 4 notions pour tout comprendre

Chloé-Anne Touma
Rédactrice en chef, LES CONNECTEURS
catouma@lesconnecteurs.ca

L'ordinateur quantique est le gage d'avancées majeures pour le milieu de la recherche et du développement dans tous les secteurs. Sa puissance de calcul et ses propriétés font rêver. Que faut-il en comprendre et qu'est-ce qui le distingue d'un ordinateur classique?

1. SON ASPECT

Si vous vous demandez à quoi ressemble un ordinateur quantique, imaginez-vous un curieux lustre sorti tout droit d'un film de science fiction.

Il est composé d'une structure enveloppante en or pur, qui abrite son processeur, une puce, sans mémoire, sans disque, qui requiert un environnement HPC (calcul haute performance) pour se connecter aux machines.

2. LE QUBIT POUR UNITÉ DE MESURE

Dans l'informatique traditionnelle, qui repose sur un système binaire, on parlera de bits, qui correspondent à la plus petite unité d'information manipulable par une machine numérique. La lecture d'un bit donne 1 ou 0. On dit donc qu'elle est « déterministe ».

En quantique, le premier élément de base d'un ordinateur est le qubit, capable d'être simultanément dans les valeurs 0 et 1, et dans toutes les valeurs intermédiaires du spectre entre les deux. On passe donc du déterminisme au « probabilisme ».

À titre d'exemple, le modèle System Quantum One, exploité au Québec, peut supporter jusqu'à 127 qubits.

3. DES CALCULS TRÈS COMPLEXES ET LA RÉSOLUTION DE PROBLÈMES

Il serait possible, avec un ordinateur quantique, de stocker jusqu'à deux ou trois fois le nom de toutes les planètes qui existent dans l'univers, ce qu'un ordinateur classique d'aujourd'hui ne pourrait faire, mais aussi de résoudre des problèmes complexes.

Avec un instrument aussi puissant, on envisage notamment de faire de grandes découvertes par la modélisation moléculaire.

En médecine, on a l'ambition de modéliser, grâce aux ordinateurs quantiques, de nouvelles molécules pour trouver des remèdes efficaces contre des maladies aujourd'hui incurables. On pourra, par exemple, simuler le corps humain, chercher à voir ce qui se passe lorsqu'on manipule un traitement qui existe déjà pour le cancer du cerveau, et qu'on le modifie pour obtenir une variante afin de traiter un autre type de cancer, tel que celui de la prostate.

4. SES LIMITES

Pourtant, l'ordinateur quantique trouve aussi ses limites dans certains types de calculs. Pourquoi ? Parce que les qubits sont en fait des atomes, que l'on doit organiser d'une certaine manière pour réaliser des calculs complexes. Les atomes étant instables, il faut pas moins de sept réfrigérateurs pour les ralentir et maintenir le système à une température de -272 °C.

Ainsi, le taux d'erreur est actuellement couramment supérieur de plus de 1 % par opération de calcul, soit beaucoup plus important que dans les bits classiques. S'additionnant après chaque opération, ces erreurs faussent les calculs, et en rendent les résultats inexploitables.

Pour remédier à ce problème, on répète la même opération plusieurs fois avec l'ordinateur quantique, et on retient la réponse la plus récurrente (celle qui a la probabilité la plus élevée) comme étant la meilleure.

Physique quantique, informatique quantique et informatique classique : les nuances

Roxanne Lachapelle
Journaliste, LES CONNECTEURS

« Je pense pouvoir affirmer avec certitude que personne ne comprend la mécanique quantique. » Difficile de mieux résumer cette théorie que le faisait le physicien nobélisé Richard Feynman au cours des années 1960. Alors que les ordinateurs quantiques et la révolution qu'ils semblent annoncer sont sur toutes les lèvres, ces technologies en pleine ascension demeurent particulièrement difficiles à comprendre.

DISTINGUER LA PHYSIQUE QUANTIQUE DE L'INFORMATIQUE QUI EN DÉCOULE

D'abord, une nuance entre physique quantique et informatique quantique s'impose. Bien qu'elles soient étroitement liées, elles demeurent distinctes, en ce que la physique quantique est une branche fondamentale de la physique qui étudie le comportement de la matière et de l'énergie à l'échelle subatomique, révélant des principes uniques tels que la superposition et l'intrication. L'intrication quantique permet de corréler l'état quantique de plusieurs particules subatomiques, comme des électrons ou des photons, ce qui permet d'encoder et de manipuler simultanément de multiples informations.

Comprendre et délimiter les frontières qui séparent l'information quantique du quantique en soit (c'est-à-dire de la théorique qui explique comment notre monde fonctionne à échelle microscopique) n'est pas chose simple. Mais, déjà, l'information quantique peut être considérée comme une « branche du domaine quantique, qui prend avantage du fait que l'information quantique est tout simplement un autre paradigme que l'information classique », simplifie M. Thibault.

L'informatique quantique reprend donc des principes et des propriétés du domaine du quantique, dont la superposition et l'intrication de systèmes quantiques, mis au service de concepts plus propres au domaine de l'informatique.

« Tracer la frontière entre les deux (informatique et quantique) est toujours débattable, mais il existe tout de même une barrière. »

« Tracer la frontière entre les deux (informatique et quantique) est toujours débattable, mais il existe tout de même une barrière », souligne M. Thibault. Il explique que du côté de l'informatique, on cherche notamment à déterminer comment encadrer l'information dans un système, ou comment se servir de l'information pour faire un calcul. En quantique, on s'intéresse plus à ce qui concerne le produit physique, donc au système physique.

> **« (...) la physique quantique, ça ressemble davantage à faire le système, donc faire la couche du bas de l'ordinateur. Et l'informatique quantique ressemble davantage à la couche du haut, qui est le code, l'algorithme et la manière d'utiliser un système pour faire un calcul qui va être utile (...) »**

Karl Thibault. (Photo : Institut quantique de l'Université de Sherbrooke)

De nombreux produits fonctionnent grâce à la compréhension de la physique quantique, sans que cela soit perceptible. C'est notamment le cas des lasers, de l'IRM (imagerie à résonance magnétique), ainsi que des cellulaires et des ordinateurs. Les avancées en quantique ont permis de réduire massivement la taille des transistors, rendant la portabilité de ces appareils électroniques possible.

« De façon très simplifiée, je dirais que la physique quantique, ça ressemble davantage à faire le système, donc faire la couche du bas de l'ordinateur. Et l'informatique quantique ressemble davantage à la couche du haut, qui est le code, l'algorithme et la manière d'utiliser un système pour faire un calcul qui va être utile. Mais c'est certain qu'à tous les niveaux, il y a un peu de chacun », conclut M. Thibault.

DISTINGUER L'INFORMATIQUE QUANTIQUE DE CELLE CLASSIQUE

L'informatique quantique, quant à elle, est un domaine appliqué, qui exploite ces phénomènes quantiques pour effectuer des calculs.
En informatique classique, un transistor agit tel un interrupteur qui permet de faire passer, ou non, le courant. « En quantique, c'est très différent, puisqu'on peut créer un système qui est dans une superposition d'états, puis c'est là que vient la superposition quantique. On peut créer un système où le courant passe et ne passe pas à la fois », explique M. Thibault.

Autrement dit, l'informatique quantique tire parti du fait que les données ne sont pas que binaires. En informatique classique, les bits (binary digits) peuvent être soit 0, soit 1; ces deux états dépendent de la fermeture ou de l'ouverture du transistor. En revanche, en informatique quantique, les qubits (quantum bits) peuvent être 0, 1, ou encore une combinaison linéaire ou une superposition de ces deux nombres.

L'informatique quantique permet ainsi de faire des calculs de façon différente, en plus de pouvoir solutionner des problèmes impossibles à résoudre avec les schémas actuels d'informatique classique. Pour l'instant, différentes contraintes techniques limitent le potentiel des ordinateurs quantiques, qui laissent présager la venue de percées majeures en cryptographie et en sciences de la santé, entre autres.

M. Thibault précise que les ordinateurs quantiques ne sont pas en voie de remplacer nos ordinateurs actuels, mais qu'on peut envisager l'éventualité d'une informatique quantique pouvant optimiser certains résultats algorithmiques. « Aujourd'hui, on se sert de l'IA (intelligence artificielle) sans s'en rendre compte (à travers des moteurs de recherche ou des cartes interactives, notamment). Je pense que le quantique va devenir une partie de ce flux de travail informatique. L'utilisateur moyen d'Internet ou des technologies de l'information ne va pas nécessairement se rendre compte du fait qu'un calcul quantique a été fait à un certain moment. »

L'ère quantique arrive-t-elle enfin?

Michel Savard
Chroniqueur, LES CONNECTEURS
Chef de pratique, Science des données, CRIM

La province du Québec a fait les manchettes il y a exactement un an avec l'annonce d'investissements importants dans la nouvelle zone « quantique » à Sherbrooke. Est-ce que les adopteurs précoces sont sur le point de recevoir leur premier ordinateur quantique dans leur salon? Voyons cela de plus près!

Au-delà des démonstrations que l'on peut observer à ce jour, la vraie promesse de l'ordinateur quantique est de pouvoir résoudre des problèmes mathématiques trop complexes pour les grappes de calcul les plus grandes de la planète. Si on réussit à calquer une situation d'affaires, un enjeu scientifique ou une problématique d'ingénierie sur un tel problème mathématique, et qu'on laisse l'ordinateur quantique identifier une solution grâce aux propriétés physiques des qubits qui le composent, alors on bénéficie du prophétique « avantage quantique ». Ces types de problèmes complexes sont rencontrés notamment en santé, dans la science des nouveaux matériaux et dans l'optimisation d'enjeux de logistique. Les bénéfices du quantique dans nos vies risquent donc d'arriver, indirectement, à la suite d'avancées majeures dans ces domaines scientifiques respectifs.

Au cœur d'un ordinateur quantique, on trouve un circuit de qubits. Le qubit, ou « bit » quantique, est l'équivalent du transistor qui se trouve par milliards dans les puces électroniques d'un processeur classique. Notez qu'on peine encore à ce jour à placer plus de 1000 qubits sur une puce. Chaque qubit est malheureusement très à risque d'interagir avec son environnement, et ainsi de perdre ses propriétés quantiques, redevenant une particule classique. Lorsqu'on veut faire un calcul qui implique de nombreux qubits, il suffit que l'un d'entre eux perde son état quantique pour qu'une erreur se produise. C'est un énorme défi d'ingénierie que de préparer des états quantiques sur une puce électronique sans que des fluctuations thermiques, ou même des rayons cosmiques, ne détruisent le calcul en cours. On se bat alors ici contre les lois de la physique, et celles-là, on peine à les enfreindre.

« (...) on reste encore à ce jour à des systèmes de quelques dizaines de qubits, ouffrant de stabilité réduite et demandant une expertise de pointe (...) »

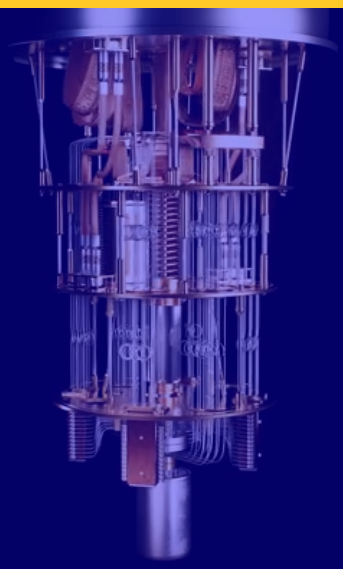
L'annonce d'avancées surprenantes a été publiée cet automne dans la revue Nature, où des chercheurs de DeepMind, le même groupe récipiendaire du Nobel de chimie 2024, ont imaginé une stratégie pour augmenter la taille des processeurs quantiques sans que le taux d'erreur ne soit prohibitif. Bien que des prestataires de service de renom comme les Amazon et IBM s'empressent de proposer d'effectuer des calculs sur de vrais ordinateurs quantiques, on reste encore à ce jour à des systèmes de quelques dizaines de qubits,

souffrant d'une réduction de stabilité et demandant une expertise de pointe afin de concevoir la bonne séquence d'opérations à appliquer aux quelques qubits pour résoudre des problèmes bien précis. Ces limitations sont sérieuses. On donne même un nom à cette étape de maturité : l'ère NISQ (« Noisy Intermediate-Scale Quantum » en anglais).

Les scientifiques et ingénieurs des meilleurs centres de recherche ont encore de gros obstacles à surmonter avant que les qubits, au cœur des ordinateurs quantiques, puissent être manipulés avec confiance et aise. Les projets pilotes en quantique sont prometteurs, mais ne rivalisent pas encore avec les centres de calcul classiques. Nous n'avons toujours pas l'avantage quantique. On conclut donc que l'investissement vise plutôt le soutien à une recherche fondamentale, à une formation de la relève hautement qualifiée et à la préparation à un futur où l'on prévoit sortir de l'ère NISQ. On ne doit pas retenir notre souffle pour que le calcul quantique résolve nos problématiques d'affaires!

Le premier ministre du Québec, François Legault, rencontré par notre rédaction lors de l'inauguration de l'Espace Quantique 1 de Distriq, Zone d'innovation quantique de Sherbrooke, en novembre 2023. (Photo : Chloé-Anne Touma)

Le Québec passe à la vitesse quantique



Sacha Israël
Journaliste, LES CONNECTEURS

Alors que les nombreux projets émergent et que les entreprises étrangères viennent poser bagages, le Québec est plus que déterminé à poser ses marques comme leader mondial d'informatique quantique. Comment la province parvient-elle à se placer comme pôle d'innovation dans le domaine?

QU'ENTEND-ON PAR INFORMATIQUE QUANTIQUE?

Si l'informatique quantique est une notion encore floue pour le public, elle représente pourtant un facteur clé en vue d'une économie du futur pour les experts dans le domaine.

e quantique, souvent associé à la mécanique ou à la physique, parvient avec difficulté à résonner dans les oreilles de la population comme sphère informatique aux ambitions révolutionnaires.

Il reste difficile de définir précisément une technologie qui bouleversera de nombreux domaines. Retenons surtout que l'informatique quantique permettra de résoudre de multiples problèmes complexes, en exploitant une puissance de calcul bien supérieure à celle des ordinateurs traditionnels.

« L'informatique quantique est un domaine émergent de l'informatique de pointe, qui exploite les qualités uniques de la mécanique quantum pour résoudre des problèmes qui dépassent les capacités des ordinateurs classiques les plus puissants. », explique IBM (International Business Machine Corporation).

LE QUÉBEC À L'AVANT-GARDE

Mais alors, qu'est-ce qui place le Québec comme pôle d'innovation en la matière?

La province rayonnait déjà l'an dernier avec l'arrivée du superordinateur opéré par IBM dévoilé à Bromont et exploité par la plateforme d'innovation numérique et quantique du Québec (PINQ2). Une annonce qui a mobilisé de nombreux acteurs de l'écosystème puisque le Canada est la quatrième nation après les États-Unis, l'Allemagne et le Japon à avoir un superordinateur opéré par IBM à travers le monde.

Le superordinateur quantique que le Québec exploite à Bromont est le 4ème de ce type opérationnel dans le monde

Ce superordinateur, sous les feux des projecteurs lors de son inauguration, met également de l'avant les nombreuses infrastructures québécoises à la pointe de la technologie, réunissant l'ensemble de l'écosystème quantique.

Le premier ministre François Legault, s'apprêtant à couper le ruban inaugural, le 24 novembre 2023. (Crédit photo : Chloé-Anne Touma, LES CONNECTEURS

On appelle « Distriq » la zone d'innovation quantique du Québec, située au cœur de la ville de Sherbrooke. Décrite comme une organisation qui catalyse l'expertise et les infrastructures, elle connecte et intègre les initiatives collaboratives en augmentant la synergie entre les différents acteurs de l'écosystème quantique d'ici.

L'année dernière, l'Espace Quantique 1 (EQ1) avait d'ailleurs rassemblé une foule d'acteurs de l'écosystème ainsi que quelques représentants ministériels pour inaugurer cet espace muni de nombreux locaux et matériels. Cette infrastructure mise à disposition des start-up, entreprises et organismes impliqués, offre également le DevteQ, un laboratoire de Développement des Technologies Quantiques d'une surface de 20 000 pieds carrés qui promet d'offrir un avantage compétitif sur le marché.

La priorité dans la mise en place de ces infrastructures est bel et bien de permettre aux entreprises de démarrer ou de prendre de l'accélération comme le suggère le directeur général de DistriQ, Martin Enault.

Cet avantage compétitif s'associe également à la volonté d'attirer des joueurs internationaux afin que des entreprises étrangères viennent s'implanter dans la zone d'innovation.

« Avec cet investissement majeur dans la zone d'innovation Distriq, on contribue à la création et à l'implantation de nouvelles entreprises dans un secteur stratégique d'avenir. Les retombées de ce projet assureront que les talents et l'expertise sont au rendez-vous. », soutenait Pierre Fitzgibbon, ancien ministre de l'Économie, de l'Innovation et de l'Énergie. « C'est grâce à des initiatives comme celle-ci qu'on va hisser le Québec comme leader à l'échelle mondiale dans les sciences quantiques », avait-il ajouté.

Ces investissements proviennent en partie du gouvernement québécois ayant octroyé un budget à hauteur de 65,3M$ lors de l'inauguration de l'EQ1 en 2023. Les fonds investis ont ainsi pu permettre à cinq grands projets de voir le jour, permettant d'enrichir l'écosystème quantique et de créer de l'emploi.

Des financements qui ont surtout pour vocation d'intégrer différentes start-up étrangères, notamment l'entreprise française PASQAL, qui a bénéficié d'un prêt de 15 M$ pour s'implanter dans la zone d'innovation, afin de fabriquer des ordinateurs quantiques destinés au marché nord-américain.

Cette attractivité pour les entreprises étrangères a d'ailleurs récemment incité la start-up française Quandela à s'ajouter dans les rangs en annonçant l'ouverture d'une filiale canadienne à Montréal, en septembre dernier.

MONARQ, UNE INITIATIVE QUÉBÉCOISE POUR DU QUANTIQUE QUÉBÉCOIS

MonarQ, une des dernières actualités quantiques, vient signer une nouvelle ambition quantique québécoise avec l'annonce du premier superorodinateur conçu au Québec.

Lancé par l'équipe de Calcul Québec, cet ordinateur dont le nom fait référence au papillon « monarque » comme symbole de transformation, selon la directrice générale de Calcul Québec, Suzanne Talon, constitue un pas de plus pour offrir à la communauté de la recherche et de l'innovation « une occasion unique de développer et tester de nouveaux algorithmes quantiques et hybrides ».

Annoncé en septembre dernier et décrit comme un supraconducteur de 24 qubits, il promet d'être adapté aux besoins actuels de la recherche et de résoudre des problèmes selon de nouvelles approches, tout en garantissant que l'ensemble de la propriété intellectuelle générée demeure au Québec.

Entouré d'autres superodinateurs et accessible dès janvier 2025, il se trouve actuellement dans un local de l'École de technologie supérieure (ÉTS) à Montréal, renforçant encore ce lien entre le monde quantique et le monde universitaire.

« L'arrivée de MonarQ permettra à la communauté universitaire, scientifique et aux entreprises d'avoir accès aux technologies quantiques nécessaires pour des recherches dans des domaines aussi variés que l'énergie, le transport, la pharmaceutique ou les matériaux. En soutenant l'innovation de cette manière, nous nous assurons de bien positionner les PME et les organisations du Québec, et de renforcer notre leadership mondial dans ce domaine », amène Soraya Martinez Ferrada, ministre responsable de

MonarQ. (Crédit photo : Calcul Québec)

Inauguration de l'ordinateur quantique MonarQ, le 25 septembre 2024. (Crédit photo : LES CONNECTEURS)

l'Agence de développement économique du Canada pour les régions du Québec.

FORMER UNE MAIN-D'OEUVRE EN QUANTIQUE DANS LE MILIEU ACADÉMIQUE

L'Institut quantique de Sherbrooke vient compléter la zone Distriq, avec l'ouverture du premier programme d'informatique quantique au monde.

« Distriq s'assure de créer des ponts entre cette recherche et les entreprises utilisatrices de solutions quantiques. »

Cet institut de recherche de l'Université de Sherbrooke se concentre ainsi sur la science et les technologies quantiques, en réunissant des scientifiques spécialistes en matériaux quantiques, en information quantique et en ingénierie quantique dans le but d'effectuer des travaux de recherche fondamentale et de développer les technologies quantiques du futur. Tout cela en familiarisant les étudiants à ses fonctions et ses aspirations pour l'avenir. Une autre occasion de créer un pont entre le monde académique et la recherche, dans un domaine encore complexe à démystifier pour l'opinion publique.

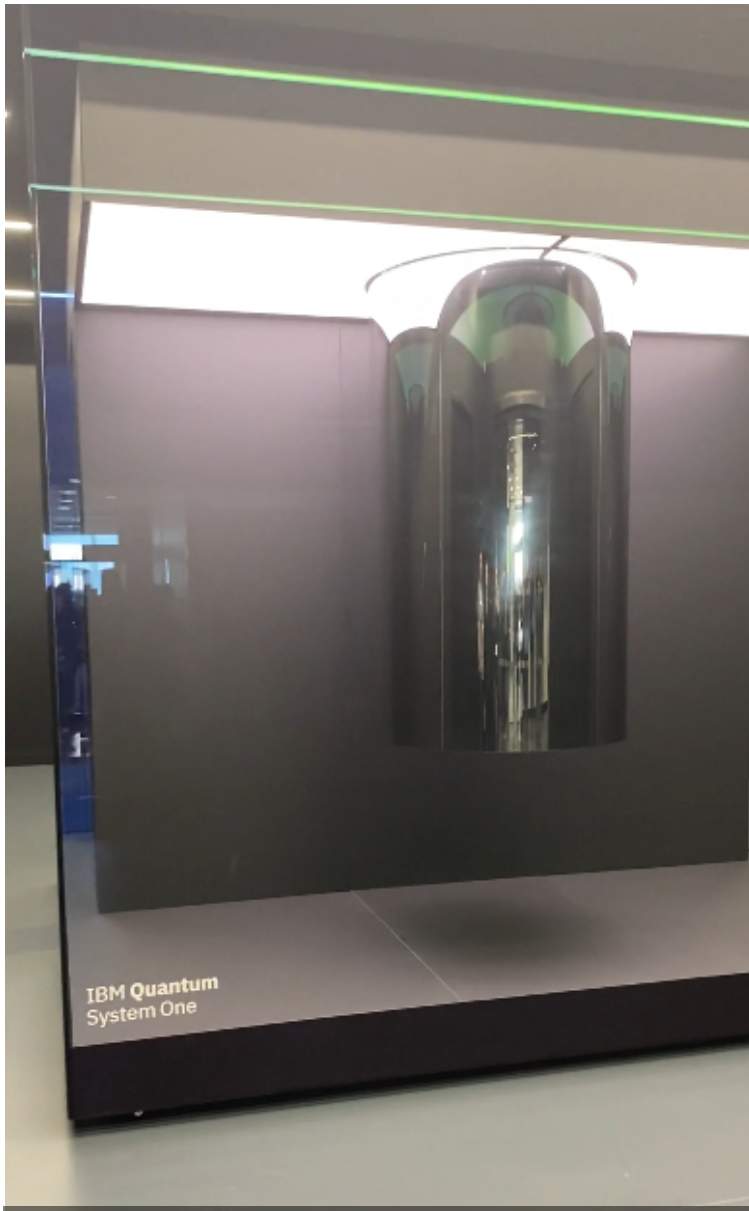
« Le financement de la recherche est la base pour le développement des technologiques quantiques, et Distriq s'assure de créer des ponts entre cette recherche et les entreprises utilisatrices de solutions quantiques. Ainsi, le développement est encadré de façon éthique pour des innovations socialement responsables », affirme Richard St-Pierre, directeur général de Distriq, faisant référence au programme de financement STIMuleS du Fonds de Recherche du Québec.

Horizons quantiques au Québec : le maillage entre entreprises, talents et recherche

Chloé-Anne Touma
Rédactrice en chef, LES CONNECTEURS
catouma@lesconnecteurs.ca

Bien qu'encore peu familier au grand public, le domaine quantique nourrit déjà des idées de grandeur dans le milieu de la science et de l'innovation, promettant de révolutionner plusieurs secteurs d'activité, et d'y créer des emplois hautement qualifiés et valorisés pour les années à venir. Si les grandes entreprises rencontrent déjà des défis quant au recrutement de professionnels dans les domaines de l'ingénierie et de la recherche quantique, le positionnement et le leadership du Québec en la matière incitent de plus en plus d'organisations à s'implanter dans la Zone d'innovation quantique à Sherbrooke, et à se tourner vers des pourvoyeurs de talents comme Mitacs pour s'enrichir d'une relève qualifiée, soutenant leur essor. Mais comment se dessine cette révolution, et qu'elle en est la promesse d'innovation et d'emplois d'un secteur à l'autre? La rédaction de LES CONNECTEURS s'entretient avec Sylvain Giguère, vice-président du développement des affaires chez Mitacs, pour en dresser le portrait.

L'ordinateur quantique est le gage d'avancées majeures pour le milieu de la recherche et du développement dans tous les secteurs, pour son incomparable puissance de calcul et sa vitesse. Dans l'informatique traditionnelle, qui repose sur un système binaire, on parle de bits, qui correspondent à la plus petite unité d'information manipulable par une machine numérique. En quantique, le premier élément de base d'un ordinateur est le qubit, capable d'être simultanément dans les valeurs 0 et 1, et dans toutes les valeurs intermédiaires du spectre entre les deux, tel que le rappelle M. Giguère, ce qui confère « un potentiel de calcul infini ». À titre d'exemple, le modèle System Quantum One, exploité à Bromont par la Plateforme d'Innovation Numérique et Quantique du Québec (PINQ²), peut supporter jusqu'à 127 qubits. Le dernier modèle de puce développé par IBM, IBM Osprey, en soutient quant à lui plus de 400.



Superordinateur d'IBM exploité à Bromont, filmé lors de son dévoilement officiel. (Crédit vidéo : Chloé-Anne Touma, LES CONNECTEURS)

> **On parle, au Canada, de 200 000 emplois créés grâce à la quantique d'ici 2045. Au Québec, on s'attend à au moins 50 000 emplois, vu l'essor concentré du secteur dans la province.**

Selon Sylvain Giguère, « Nous sommes aux balbutiements de l'industrie quantique. On peut espérer des retombées concrètes et révolutionnaires, mais pas avant 5, 10, ou même 15 ans », de spécifier le VP du développement des affaires chez Mitacs, un organisme sans but lucratif qui, en partenariat avec les universités, le secteur privé et les gouvernements du Canada et du Québec, aide à relever les défis organisationnels grâce à des stages rémunérés, notamment dans le secteur de l'innovation en quantique.

LA PROMESSE D'UNE RÉVOLUTION MULTI SECTORIELLE

Parmi les domaines que le quantique transforme déjà, il mentionne la cryptographie, « parce que cela ouvre tout un champ de possibilités de codage, permettant de décrypter tout ce qu'il y a à décrypter jusqu'à présent, sinon crypter ce qui ne l'a pas encore été. Les communications seront également beaucoup plus rapides, grâce à un cryptage qui est bien plus imperméable aux attaques », optimisant la gestion du risque et renforçant la sécurité des systèmes dans des secteurs où l'erreur est critique, tels que la finance, « qui implique de gros volumes de données sensibles », de pointer M. Giguère.

Or, cette puissance de calcul, qui rend le cryptage traditionnel inefficace, représente aussi une menace pour les systèmes de cybersécurité actuels. Mais pour M. Giguère, ça tombe bien, puisque « L'identification de solutions qui répondent à ce problème commence justement par l'innovation quantique, ce qui en fait un sujet de valeur stratégique, d'où l'importance de se donner les moyens d'établir son propre hub de développement quantique pour relever les défis qui accompagnent l'opportunité. »

Il ne manque pas non plus de relever la santé, domaine dans lequel les experts sont nombreux à attendre la découverte de médicaments et de traitements grâce à la modélisation moléculaire. « On va ainsi pouvoir réduire le temps et le coût de développement des traitements. Pensons aussi à l'énergie et au transport, où plusieurs projets de recherche et travaux sont en cours. »

LA CRÉATION D'EMPLOIS ET L'ATTRACTION DES TALENTS DE LA RELÈVE

En plein essor dans plusieurs industries, le domaine de la quantique foisonne d'opportunités pour la création d'emplois parfois insouçonnés, « pour des mathématiciens et des ingénieurs de toutes spécialités, car c'est un domaine d'impact transversal, qui touche toutes les branches du génie, celles-là même qui auront un rôle significatif à jouer dans ce mouvement. Pensons également aux technologies numériques et à l'implication des informaticiens. On parle, au Canada, de 200 000 emplois créés grâce à la quantique d'ici 2045. Au Québec, on s'attend à au moins 50 000 emplois, vu l'essor concentré du secteur dans la province », de compléter Sylvain Giguère.

Plus qu'en nombre d'emplois, il estime que « C'est en termes de productivité que l'on va pouvoir mesurer le progrès du secteur quantique et de sa contribution à l'épanouissement de notre économie et de notre société, et à la qualité de vie des citoyens, car nous sommes en contexte de pénurie de main-d'œuvre. Le potentiel d'augmentation de la productivité, grâce à la quantique, n'est pas négligeable. »

DES INVESTISSEMENTS À LA HAUTEUR DES AMBITIONS DU QUÉBEC

Le gouvernement du Québec s'est voulu démonstratif quant à son ambition d'exploiter le plein potentiel de la richesse de talents et de recherche produite en sciences quantiques au Québec, et de continuer d'en développer l'expertise et l'application, en formant de nouveaux talents et favorisant l'adoption de technologies en collaboration avec le milieu industriel dans la province.

« Le Québec a la chance de pouvoir compter sur des infrastructures quantiques parmi les meilleures au monde. En combinant la recherche appliquée de l'ÉTS aux infrastructures nouvellement mises en place, on s'assure de créer la synergie nécessaire pour tirer un maximum de bénéfices des sciences quantiques », a d'ailleurs souligné l'ex-ministre de l'Économie, de l'Innovation et de l'Énergie, Pierre Fitzgibbon, en marge de la récente annonce d'un octroi de 5 millions de dollars à l'ÉTS pour soutenir la réalisation d'initiatives évaluées à 19,1 millions de dollars. C'est dans cet esprit que son ministère entend aussi renforcer son appui auprès de Mitacs, grâce à un investissement de 64,6 millions de dollars étendu jusqu'à 2027.

« Le défi pour faire face à l'achat de propriété intellectuelle, c'est de convaincre les entreprises des bénéfices de miser sur le Québec pour renforcer l'écosystème et mener la révolution du quantique. »

DES EXEMPLES CONCRETS

Parmi les projets notoires du Québec en quantique, on compte le banc d'essai lancé par Numana, catalyseur d'écosystèmes d'innovation technoligique, pour tester la communication quantique, auquel Mitacs a collaboré par la mise en relation entre chercheurs et entreprises et le financement de talents comme parties prenantes.

François Borelli, PDG de Numana, au lancement de Kirq - Banc d'essai de communication quantique Numana. (Crédit photo : archives)

UN TRIO GAGNANT

Ces maillages entre instituts de recherche, entreprises et organismes aussi bien de liaison que d'activisme, constituent, selon Sylvain Giguère, les ingrédients d'une recette gagnante pour l'épanouissement de l'innovation en quantique au profit de la collectivité.

Si le retard de transfert technologique, dans d'autres secteurs que le quantique, est observé de manière généralisée au Québec et au Canada, M. Giguère l'explique par un manque de recherche et développement, de brevets, mais aussi d'investissement en machinerie et équipements. « Les PME sont aux prises avec des défis de performance et de productivité. Elles ont une plus petite capacité d'absorption des technologies, et c'est d'autant plus vrai au Canada, où l'enjeu n'est pas le même qu'aux États-Unis, par exemple. » Un constat qui fait écho au témoignage de l'Innovateur en chef du Québec, Luc Sirois, qui rappelait, en entrevue avec la rédaction il y a quelques mois, que le Québec produit 10 000 fois moins de brevets qu'aux États-Unis.

« On pourrait aussi en faire davantage dans l'aéronautique et les technologies en santé. Dans le cas de l'informatique quantique, on parle d'un domaine émergent, qui se fonde sur le plus haut niveau de connaissances et d'infrastructures de pointe atteint en communication et technologies numériques, ce qui élimine un obstacle propre à d'autres secteurs », de suggérer M. Giguère.

Questionné quant à l'équilibre à trouver entre la collaboration internationale et le protectionnisme, quand on sait que plusieurs entreprises locales et talents, dans lesquels le Québec investit, finissent par rejoindre le marché américain, il soutient que « Le défi pour faire face à l'achat de propriété intellectuelle, c'est de convaincre les entreprises des bénéfices de miser sur le Québec pour renforcer l'écosystème et mener la révolution du quantique », qui semble plus accessible que le défi homologue en intelligence artificielle, ne serait-ce qu'à en juger par le nombre d'entreprises qui s'implantent à Distriq, Zone d'innovation quantique à Sherbrooke.

« Il y a l'Institut de quantique de l'Université de Sherbrooke, l'Université de Montréal et l'ÉTS, qui mènent divers projets de recherche, ainsi que des entreprises qui sont présentes sur la scène québécoise, comme IBM, dont le superordinateur quantique est mis à disposition d'entreprises d'ici afin de mener des tests, et enfin, des start-up issues d'autres provinces canadiennes et même d'Europe qui viennent s'implanter. » Cela représente un nouvel écosystème, qu'il est impératif de structurer grâce à des connecteurs, et c'est là qu'interviennent des organismes comme Québec Quantique et Mitacs, « en connectant les industries et entreprises de toutes tailles, qui ont des besoins de productivité spécifiques, aux bonnes têtes du milieu de la recherche. Cela passe notamment par le financement de tout le processus de recherche et développement, et de talents issus d'universités du Québec et d'ailleurs au Canada », de conclure le VP du développement des affaires.

Dialogue social et technologie du futur : la voie la plus porteuse, non sans écueil

Isabelle Lacroix
Chroniqueuse, LES CONNECTEURS
Professeure de politique appliquée et chercheuse associée,
Institut quantique, Université de Sherbrooke

Nous sommes le 18 octobre 2023, heure du lunch, Zone d'innovation quantique de Sherbrooke – Distriq, il y a plus d'une vingtaine de personnes autour de la grande table. Il y a des entrepreneurs quantiques, des personnes des institutions d'enseignement de la région, des représentants de la Ville, des personnes des groupes de la société civile locale, des personnes étudiantes de l'Université de Sherbrooke et, évidemment, des personnes de la communauté de la recherche. Leur mission est simple : préparer la révolution quantique à Sherbrooke pour assurer une future intégration technologique destinée au bien commun. Rien que ça!

Depuis cette date, ces rencontres ont lieu toutes les six à huit semaines. On y discute de science et de technologies quantiques, bien sûr, mais aussi d'environnement, de démocratisation et d'accessibilité, d'éthique, d'équité et de politique. Toutes ces personnes, dont l'agenda est des plus chargés, se retrouvent ainsi régulièrement pour penser ensemble le futur technologique de Sherbrooke. Pourquoi?

La première réponse, la plus importante et la plus simple, est qu'il n'y a pas d'autre voie connue si on veut une intégration technologique dont les impacts serviront véritablement le bien commun et non pas seulement les intérêts de quelques acteurs privilégiés, notamment économiques. Il importe que ce dialogue regroupe des intérêts les plus diversifiés pour qu'ils soient pris en compte en cours de développement, et non pas uniquement au moment d'assurer l'acceptabilité d'une techno que l'on cherche à imposer.

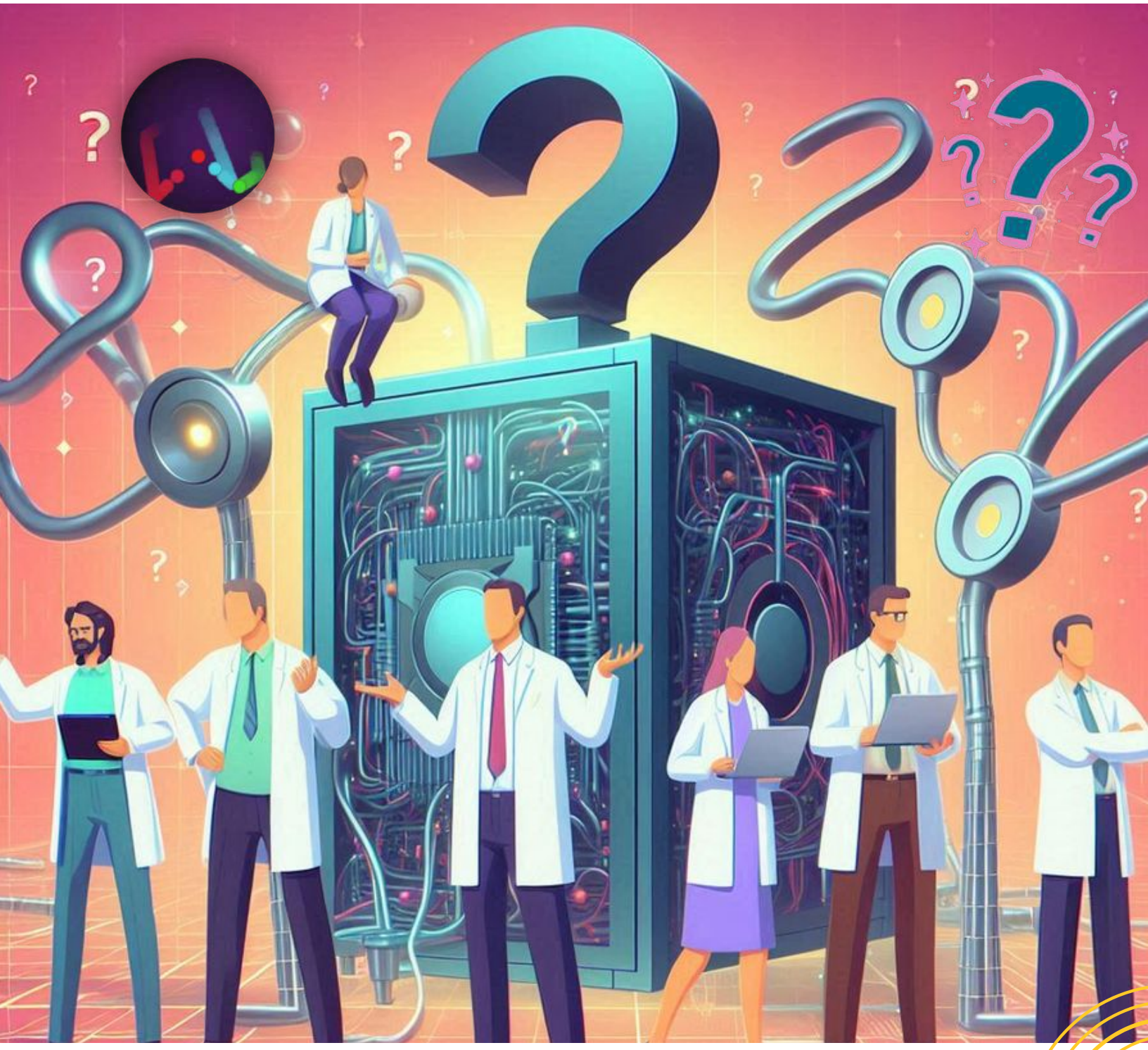
Cela n'est pourtant pas sans défi, assurément. D'abord, le défi de l'anticipation. Réfléchir les impacts d'une technologie encore inexistante, c'est accepter le risque que rien ne se passe comme prévu, tout en demeurant attentif aux promesses, amplifiées ou minimisées selon les intérêts en présence, qui peuvent faire dérailler le dialogue, à tout moment.

« L'engagement des groupes de la société civile est en ce sens aussi fragile que nécessaire. »

Ensuite, il y a le défi de la pérennisation de ce dialogue. Maintenir l'intérêt et l'engagement des personnes indirectement concernées, alors que la pression des dossiers plus urgents et plus concrets est une réalité incontournable pour tous, mais encore plus pour ces personnes qui ne sont pas aux premières loges de ce développement technologique. L'engagement des groupes de la société civile est en ce sens aussi fragile que nécessaire.
Finalement, le défi de la compréhension. Entre les personnes

expertes des technologies quantiques qui se disent incompétentes pour traiter des impacts sociétaux, et les personnes représentantes de la société civile qui affirment ne rien connaître (voire comprendre) à la science quantique, il est délicat de trouver ce point d'équilibre qui justifie la contribution de tous et toutes. Il est, en théorie, aisé de prétendre que toutes les voix sont essentielles, mais il est très compliqué de les faire cohabiter pour en arriver à une compréhension commune. Cela prend du temps, ce dont tout le monde manque cruellement.

Ainsi, est-ce une mission impossible? Puisque cela est devenu une réalité concrète à Sherbrooke, depuis plus d'une année, il faut constater que cela est possible, tout en reconnaissant que cela n'est pas facile. Faut-il croire, comme disait l'autre, que c'est parce que nous ne savions pas que c'était impossible que nous l'avons fait? Peut-être, mais, maintenant, nous savons. Le retour en arrière est impossible si nous voulons un véritable développement (recherche et innovation) responsable, de l'idéation à l'intégration en société.



Informatique quantique et cybersécurité : une arme à double tranchant

Quentin Hibon
Chroniqueur, LES CONNECTEURS
Directeur du développement des affaires, Mitacs

Au-delà des données économiques, il est encore difficile de concevoir l'impact que l'informatique quantique aura sur nos vies. Quels enjeux amène l'informatique quantique pour la cybersécurité, et quelles solutions innovantes apporte-t-elle?

Avec le dévoilement de sa stratégie quantique nationale et les importants investissements réalisés depuis des décennies, le Canada a clairement démontré son intention de rester l'un des pionniers dans les sciences quantiques. C'est tout un écosystème de centres d'expertise quantiques qui se développe, appuyé par les initiatives provinciales telles que celle de Québec, qui a investi 435 millions de dollars l'année dernière pour faire de Sherbrooke la capitale canadienne des sciences quantiques.

Cet écosystème ne cesse de grandir, et compte également sur l'appui du secteur privé. En effet, Ericsson a annoncé le lancement de son centre de recherche quantique à Montréal. Celui-ci a pour but de développer des algorithmes quantiques afin d'accélérer le traitement dans les réseaux de télécommunications et l'informatique quantique distribuée. Ce centre de recherche bénéficiera notamment de l'appui de chercheurs universitaires grâce à Mitacs, qui a reçu 40 millions de dollars de la part d'ISDE (Innovation, Sciences et Développement économique Canada). Cette collaboration vise particulièrement à soutenir l'attraction, la formation, la rétention et le déploiement de personnel hautement qualifié dans les sciences et technologies quantiques sur le plan national.

Selon le Conseil national de recherches du Canada (CNRC), le secteur quantique deviendra une industrie de 139 milliards de dollars au Canada, avec plus de 200 000 emplois et des retombées de 42 milliards de dollars d'ici 2045. On comprend donc aisément, l'importance de ce secteur pour le Canada.

Au-delà des données économiques, il est encore difficile de concevoir l'impact que l'informatique quantique aura sur nos vies. Quelles en seront les retombées positives et les enjeux s'y rapportent en matière de cybersécurité ?

Le CNRC prévoit que le secteur quantique aura des retombées de 42 G$ d'ici 20245.

L'INFORMATIQUE QUANTIQUE COMME MENACE POTENTIELLE POUR LA CYBERSÉCURITÉ

L'informatique quantique est différente de l'informatique que l'on connait actuellement car elle utilise des bits quantiques (qubits) au lieu des bits classiques. Contrairement aux bits qui ne peuvent être uniquement qu'en deux états 0 ou 1, les qubits peuvent exister dans une multitude d'états en même temps : on parle de « superposition ».

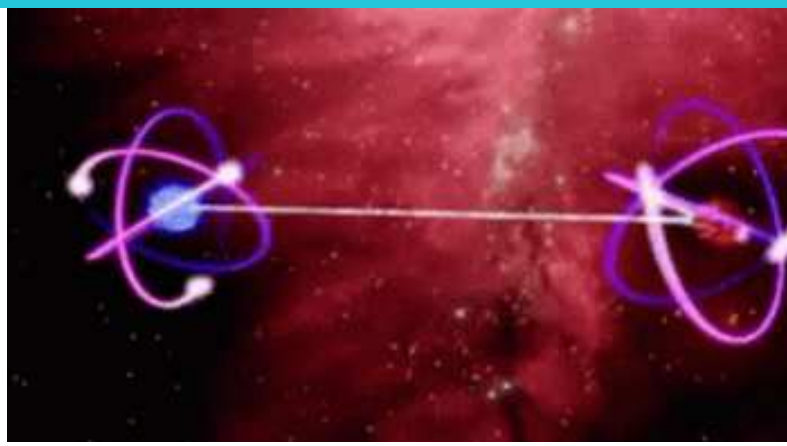
Cette particularité leur permet de réaliser un certain nombre de calculs beaucoup plus rapidement que les ordinateurs classiques, notamment de rompre les protocoles cryptographiques. Par exemple, l'algorithme Shor, un algorithme quantique, peut factoriser de grands nombres beaucoup plus rapidement que n'importe quel algorithme classique dont nous disposons actuellement. Cela signifie que de nombreux protocoles cryptographiques à clé publique que nous utilisons pourraient être vulnérables aux attaques des ordinateurs quantiques.

RENFORCER LA CYBERSÉCURITÉ GRÂCE À L'INFORMATIQUE QUANTIQUE

La construction d'un ordinateur quantique à grande échelle avec correction d'erreurs est un énorme défi technologique et nous avons encore du chemin à parcourir avant d'en arriver là. La démocratisation de l'informatique quantique n'est donc pas encore d'actualité. De plus, si l'ordinateur quantique permet de déjouer les méthodes classiques de cryptage, il permet également de développer la cryptographie quantique : les données sont donc transmises à l'aide de qubits qui ne peuvent pas être copiés ou interceptés sans être détectés. Ainsi, cela rend pratiquement impossible pour les pirates d'accéder et de voler des données sensibles.

De plus, comme dans beaucoup d'industries, pousser les systèmes dans leurs retranchements permet d'en identifier les failles afin de les renforcer. L'utilisation d'ordinateurs quantiques permet de déjouer facilement certains types de cryptage, comme l'algorithme RSA, communément utilisé pour protéger les données dans les communications et les transactions.

Cet exercice permet d'identifier les faiblesses du système et de le renforcer, par la suite, en développant d'autres méthodes de cryptage qui seront résistantes aux cyberattaques provenant d'ordinateurs quantiques. Plusieurs méthodes de cryptage sont d'ores et déjà développées, comme le QKD (Quantum Key Distribution), qui utilise les principes de la mécanique quantique pour échanger des clés cryptographiques entre deux parties.



L'idée de base derrière la QKD est que deux parties – appelons-les Pierre et Marie – utilisent les propriétés de la mécanique quantique pour générer une clé secrète partagée, qui peut être utilisée pour chiffrer et déchiffrer des messages. La QKD repose sur le fait que toute tentative de mesurer l'état d'un système quantique perturbera nécessairement ce système. En d'autres termes, si Marie envoie une série d'états quantiques à Pierre, tout éventuel pirate qui essaie d'intercepter le message introduira nécessairement des erreurs dans les résultats de mesure, alertant ainsi Pierre et Marie de la présence d'un pirate.

Les systèmes QKD utilisent généralement soit la polarisation des photons, soit la phase quantique pour encoder les informations. Dans le premier cas, Marie envoie à Pierre une série de photons avec des polarisations choisies aléatoirement. Pierre mesure ensuite la polarisation de chaque photon et enregistre les résultats. Alice et Pierre comparent ensuite les sous-ensembles de leurs résultats pour vérifier les erreurs et établir une clé secrète partagée.

Dans le cas d'une QKD basée sur la phase quantique, Marie envoie une série de photons avec différentes phases à Pierre. Pierre mesure ensuite la phase de chaque photon et enregistre les résultats. Marie et Pierre utilisent ensuite les mesures de phases pour établir une clé secrète partagée.

La QKD est donc considérée comme une méthode de distribution de clés efficace et sécurisée car toute tentative d'interception ou d'écoute clandestine de la communication introduira nécessairement des erreurs qui peuvent être détectées par les parties qui communiquent.

DEUX SECTEURS À RISQUE EN MATIÈRE DE CYBERSÉCURITÉ

Ces deux secteurs d'activité nécessitant de réaliser des calculs complexes en grandes quantités et plus rapidement que les ordinateurs classiques. L'adoption de l'informatique quantique devrait donc s'opérer rapidement. Étant donné la nature des données traitées, on comprend aisément que les enjeux de cybersécurité soient cruciaux dans ce secteur.

Le milieu de la finance

La finance est l'un des secteurs qui utilisent le plus de données dans le monde. Il repose sur des modèles mathématiques complexes, qui permettent de prendre des décisions d'investissement. Cela sous-entend deux choses : d'une part, l'implication d'une énorme puissance de calcul, et d'autre part, l'importance cruciale de la vitesse à laquelle ces calculs sont réalisés.

En effet, dans le « trading à haute fréquence », chaque milliseconde compte pour maximiser ses gains. Selon l'estimation de Thierry Lebreton, enseignant chercheur à l'École Centrale d'électronique de Paris, les plateformes boursières réalisent des transactions en moins de trois millisecondes dans 60 % des cas.

Évidemment, les enjeux en cybersécurité dans cette industrie sont énormes, et pourraient engendrer des milliards de dollars de perte financière. Le secteur financier est donc l'un des premiers à s'intéresser à l'informatique quantique et à développer de nouvelles méthodes de cryptage pour pallier les enjeux de cybersécurité.

Les instances gouvernementales

Les gouvernements nécessitent eux aussi une puissance de calcul colossale pour gérer d'importantes quantités de données sensibles, comme des données économiques, de défense, de renseignements...

Au même titre que pour la finance, on peut imaginer que les gouvernements utilisent l'informatique quantique pour réaliser plus rapidement les calculs portant sur de gros volumes de données.

Ils pourront également améliorer la cybersécurité de leurs systèmes en développant des méthodes de cryptage résistantes aux attaques quantiques. Évidemment, les cyberattaques réalisées par d'autres pays grâce à l'informatique quantique sont une réelle préoccupation.

Enfin, grâce aux possibilités de calcul de l'informatique, on peut envisager la simulation de systèmes complexes, afin de gérer au mieux des situations telles que les pandémies, les crises économiques, les catastrophes naturelles et les guerres.

EN GROS...

L'informatique quantique est ce que l'on appelle une technologie disruptive, car elle a le potentiel de révolutionner de nombreux domaines de l'informatique et de la science en général.

Bien qu'il soit difficile de prévoir l'ensemble des conséquences d'une telle technologie sur nos vies, une chose est sûre, la vitesse de calcul que permet l'informatique quantique aura un impact significatif sur de nombreux domaines, tels que la cryptographie, la recherche pharmaceutique, la conception de matériaux et l'IA. Elle pourra également permettre de résoudre des problèmes actuellement considérés comme insolubles ou très difficiles.

Telle une boite de pandore, un certain nombre de menaces notamment en termes de cybersécurité pourront apparaitre en chemin. Toutefois, la recherche réalisée au Canada depuis de nombreuses années grâce aux moyens mis en œuvre par le gouvernement et le secteur privé devrait nous permettre de les anticiper, de les surmonter et de tirer parti de cette nouvelle technologie à son plein potentiel. Ainsi, le Canada pourra se positionner comme l'un des pionniers dans le domaine des sciences quantiques.

Pour du contenu vidéo, regardez nos capsules de la série LES CONNECTEURS 3 Q/R, offertes en rediffusion sur notre plateforme lesconnecteurs.ca.

800 hôpitaux victimes de piratage en 2 ans ; une majorité d'incidents en cybersécurité attribuables à l'erreur humaine ; une faillite presque assurée pour les PME victimes de cyberattaques... Avec l'experte Valérie Doye, rencontrée à MTL connecte, notre rédactrice en chef, Chloé-Anne Touma, aborde les grands enjeux de cybersécurité et les possibilités entrevues en IA et quantique, dans cette capsule de LES CONNECTEURS 3Q/R, offerte comme toutes les capsules de la série sur la plateforme lesconnecteurs.ca, ainsi que sur notre chaîne YouTube (@LESCONNECTEURS).

Les défis de la cryptographie à l'ère post-quantique

Fanny Tan
Journaliste, LES CONNECTEURS

À l'aube de l'ère post-quantique, les experts s'interrogent sur les enjeux de sécurité liés à la montée des technologies quantiques. Alors que des acteurs étatiques et privés s'affairent à comprendre et à anticiper les risques associés, le Canada se positionne en tant que leader grâce à sa Stratégie quantique. Face à des investissements colossaux de puissances comme les États-Unis et la Chine, la protection des informations sensibles apparaît comme incontournable.

Contrairement à l'informatique classique, qui repose sur l'encodage de l'information à l'aide de bits (0 et 1), l'ordinateur quantique exploite les qubits, capables de représenter simultanément les deux valeurs. Cette superposition d'états au sein des qubits confère à ces derniers une nature probabiliste, permettant ainsi aux ordinateurs quantiques d'effectuer des calculs dits « parallèles », où les deux valeurs peuvent être traitées en même temps. « Les ordinateurs quantiques peuvent produire des calculs plus rapidement, car les qubits stockent plus d'information que les bits », explique Marc Frappier, directeur du pôle d'expertises en cybersécurité Intact et titulaire de la Chaire de recherche en cybersécurité post-quantique de l'Université de Sherbrooke.

La puissance des machines quantiques offre la possibilité d'effectuer des calculs à une vitesse inégalée, permettant ainsi de résoudre rapidement certains problèmes mathématiques critiques, y compris ceux utilisés pour protéger les communications sensibles. Par exemple, l'algorithme de Shor, développé en 1995, permet de résoudre le problème du logarithme discret, sur lequel se base une grande partie de la cryptographie moderne.

L'essor fulgurant des machines quantiques, capables d'effectuer des calculs à une vitesse sans précédent, pose ainsi un défi considérable pour la sécurité de l'information. « Alors qu'un ordinateur classique prendrait des centaines de milliers, voire de millions d'années, pour briser un algorithme de cryptographie, un ordinateur quantique pourrait briser le même algorithme en-deçà d'une journée », explique Marc Frappier.

« Alors qu'un ordinateur classique prendrait des centaines de milliers, voire de millions d'années, pour briser un algorithme de cryptographie, un ordinateur quantique pourrait briser le même algorithme en-deçà d'une journée. »

COMBATTRE LE FEU PAR LE FEU

Bien que l'ère des ordinateurs quantiques ne soit pas imminente, il est toutefois estimé que nous pourrions pleinement entrer dans l'ère quantique dans les 20 à 50 ans à venir. Résister à la puissance des machines quantiques est donc un défi essentiel à relever le plus tôt possible pour assurer l'avenir de la sécurité de l'information. « On devra modifier énormément d'applications pour qu'elles utilisent les nouveaux algorithmes résistants à la puissance quantique, soit les algorithmes post-quantiques », prévient Marc Frappier.

Les algorithmes post-quantiques reposent sur des principes classiques plutôt que sur des propriétés quantiques, souligne Didier Guignard, responsable du développement des affaires et de la recherche en Amérique du Nord chez VeriQloud, une entreprise spécialisée dans les protocoles de sécurité résistants aux menaces quantiques. Adaptés aux appareils traditionnels tels que les ordinateurs, les téléphones mobiles et les objets connectés d'aujourd'hui, ces algorithmes sont développés avec une résistance mathématiquement prouvée aux calculs quantiques. En 2014, le National Institute of Standards and Technology (NIST), l'agence américaine chargée de définir les normes en informatique, a d'ailleurs lancé un concours visant à développer de tels algorithmes.

Une solution prometteuse, mais pas infaillible, prévient Marc Frappier : « Il est impossible d'être totalement certain que ces algorithmes ne pourront être déjoués par une machine, qu'elle soit quantique ou classique. Il suffit qu'une personne ait une idée brillante pour résoudre un problème mathématique afin de les briser! » En outre, parmi la soixantaine d'algorithmes complexes proposés pour remplacer ceux actuels, seuls quatre ont été sélectionnés et recommandés pour la standardisation par le NIST, soulignant ainsi la difficulté de cette démarche.

UN ENJEU NÉGLIGÉ?

Bien que les experts en informatique quantique soulignent l'importance de se préparer à l'ère post-quantique, peu de spécialistes en sécurité de l'information traditionnelle semblent réellement s'en soucier. « Déjà, il y a beaucoup d'incertitudes sur la création d'ordinateurs quantiques suffisamment puissants », explique Marc Frappier. Pour l'heure, les machines quantiques ne contiennent qu'un nombre limité de qubits, « environ un millier », précise-t-il. « Pour décrypter les communications, on s'attend à ce que ça en prenne à peu près 10 000. » La nature des qubits, toujours instable aujourd'hui, freine elle aussi le développement de ces machines aux capacités de calcul hyper puissantes.

Toutefois, « on ne peut pas attendre la résolution de ces problèmes techniques avant de faire des changements », prévient Marc Frappier, qui rappelle que les investissements en quantique autour du globe sont considérables. Si le Canada est un joueur important dans le domaine, des puissances mondiales comme les États-Unis et la Chine dépensent des sommes faramineuses pour prendre l'avantage dans cette course au quantique. Certains États adoptent déjà des stratégies de surveillance dites « Harvest now, decrypt later », qui consistent à accumuler d'importantes quantités de données chiffrées en vue de les déchiffrer ultérieurement. Une telle menace compromet les secrets d'État dans des secteurs cruciaux, tels que la défense et la santé, comme l'explique Didier Guignard. « Il est essentiel de commencer dès maintenant à se protéger, car quiconque stocke des informations échangées actuellement pourra y accéder lorsqu'il y aura des ordinateurs suffisamment puissants », conclut Marc Frappier.

Des acteurs, notamment étatiques, s'emploient à souligner l'importance de prêter attention à la menace que représente l'ère post-quantique, explique Didier Guignard. Il poursuit : « Le Canada a établi la Stratégie quantique, qui vise à accompagner les acteurs des secteurs industriels et institutionnels dans leur compréhension des enjeux quantiques et des risques associés. » Au-delà de la mise en place de directives et d'actions concrètes, il souligne également l'importance de transmettre le message, de le vulgariser, pour susciter une prise de conscience face à un enjeu de sécurité complexe.

2024 : l'année où l'IA et le quantique ont changé les règles

René-Sylvain Bédard
Chroniqueur, LES CONNECTEURS
Fondateur et PDG d'Indominus Sécurité Gérée

En me fondant sur ma propre expérience, je vais tenter pour vous d'analyser les plus récents développements en quantique, IA et autres technologies, afin de mieux vous préparer à ce qui nous attend, dans un futur proche.

Je tiens à préciser qu'il ne s'agit pas ici de prédictions, mais bien d'une analyse fondée sur des faits, qui crée ce que je m'amuse à appeler « un futur possible ».

Ces quelques événements, survenus au cours des 18 derniers mois, ont un impact aujourd'hui :

- Février 2023 - le lancement d'Azure Quantum Element ;
- Mars 2023 - le lancement de Chat GPT-4 ;
- Juin 2023 - des avancées en chimie et science des matériaux ;
- Décembre 2023 - le lancement de Gemini par Google Deepmind ;
- Septembre 2024 - l'inauguration de MonarQ au Québec ;
- Octobre 2024 - des développements en quantique en France ;
- Novembre 2024 - une série d'annonces en lien avec d'importantes avancées pour Microsoft Ignite.

Des événements qui témoignent de l'accélération du rythme de l'innovation...

PREMIÈREMENT, QUELQUES DÉFINITIONS...

Microsoft Azure Éléments, c'est quoi?

Azure Éléments est un environnement que Microsoft a créé pour accélérer la recherche. Cet environnement n'est ouvert qu'à des groupes de recherche très précis, soit en génétique, recherche de matériaux et chimie. Il s'agit d'une classe d'ordinateurs qui allie quantique HPC (high performance computing) et IA, le but étant d'accélérer la recherche pour régler les grands problèmes de la planète.

Selon les premiers essais, cette plateforme était en mesure de réduire une année de calcul en 4 minutes, soit 50,000:1, puisqu'elle serait 50 000 fois plus rapide que les méthodes de calcul traditionnelles pour certaines tâches spécifiques.

« Le but est d'accélérer la recherche pour régler les grands problèmes de la planète. »

En collaboration avec le Pacific Northwest National Laboratory, Microsoft a utilisé Azure Quantum Éléments pour modéliser et analyser 32 millions de nouveaux matériaux candidats, aboutissant à la découverte de matériaux potentiellement capables de remplacer les batteries lithium-ion.

Démystifier ce que sont Copilot, Gemini, Llama, Bard, Claude et ChatGPT

En gros, il s'agit de différents produits, des modèles IA, qui proviennent de différentes compagnies. C'est la course aux

armements, version IA.

Non que je veuille offenser les grands fans des modèles de génération de contenu, mais à mon sens, il s'agit d'une mise en bouche. Nous n'en sommes qu'au balbutiement.

Tout ces modèles sont encore en mode d'apprentissage et sont une préparation, une mise en place de l'acceptation sociale pour ce qui s'en vient.

Et c'est sans compter le fait qu'ils sont énormément énergivores... Pourquoi? Parce qu'à chaque requête, le modèle recherche et fait référence à des milliards d'entrées pour répondre à votre question. Ces données et ces processeurs doivent exécuter ces recherches sur des ordinateurs dédiés et, vous l'aurez deviné, ne sont pas en mode « économie d'énergie ».

La seule nuance que je souhaite apporter relativement à ces modèles se rapporte à Copilot. La version pour entreprises du modèle de Microsoft a cette exception d'être conçue pour que les données demeurent dans votre environnement, ce qui, à mon avis, est une proposition unique et extrêmement intéressante pour les entreprises qui souhaitent infuser de l'IA à leurs processus d'affaires.

« Imaginez un instant que nos meilleurs modèles IA, d'ici 3 ans, aient soudainement accès à un ordinateur quantique de 100 qubits. »

L'ÉLECTION AMÉRICAINE

L'ordre exécutif présidentiel

Le 30 octobre 2023, le président Joe Biden a émis un ordre exécutif concernant les futurs développements en IA. Cet ordre mettait en place les fondements d'un cadre contraignant pour les sociétés américaines, et un premier pas pour encadrer le futur de l'IA. L'ordre était composé de 4 grands vecteurs : 1) Standards en sécurité et en prévention, 2) Protection de la vie privée, 3) Intégration des Droits civiques et équité, et 4) Collaboration avec les partenaires internationaux.

L'initiative a reçu un accueil mitigé, mais fut saluée comme une première pierre dans la fondation de la création d'une intelligence artificielle de confiance, sûre et surtout juste et équitable.

Le président élu, Donald Trump, a promis, durant sa campagne qu'il annulerait l'ordre exécutif, laissant place au libre marché.

Le premier ami

Nous avons droit, pratiquement en direct, à une scène historique, impliquant la création d'un nouveau rôle au sein du gouvernement : le premier ami.

Le défi est que cet ami n'est nul autre qu'Elon Musk, l'homme le plus riche de la planète, également dirigeant de SpaceX, Tesla, et plus récemment Twitter/X.

Ce que peu de gens savent, c'est que Musk a participé à la création d'OpenAI, en tant que société sans but lucratif. Il a d'ailleurs participé à la première ronde de financement de l'OBNL. Il a également collaboré à la mise ne place de règles de gouvernance très strictes qui ont guidé OpenAI.

En 2018, il quitte le conseil d'administration, suite à des divergences d'opinion, surtout autour du changement de modèle d'affaires, pour aller vers un modèle à profit limité.

Pourquoi est-ce que je mentionne ceci? D'abord parce que Musk a, depuis 2016, une société qui vise à lier l'esprit humain à l'ordinateur, Neural Link, et qu'il a également lancé sa propre société d'IA en 2023 (xAI), ayant pour mission de comprendre la vraie nature de l'univers. Son propre modèle d'IA, Grok, se nourrit entre autres des données disponibles dans X.

Donc, quand nous combinons ces derniers points, nous pouvons comprendre qu'il y aura, si l'on se fie aux événements à venir, un fort risque de dérapage.

LES ANNONCES DE MICROSOFT IGNITE

Hollow core Fiber : le véhicule pour l'ère de l'IA

Microsoft a investi fortement, depuis quelques années, dans une nouvelle technologie de transport d'information, la fibre à cœur creux nommée « Hollow Fiber ».

En décembre 2022, il a acquis l'un des leaders dans ce segment de marché, la firme Lumenisity.

La logique derrière ce nouveau modèle : l'air a moins de friction que le verre. Donc, il est possible d'émettre des signaux lumineux, à travers un tuyau vide, ce qui permet de déplacer plus de données, plus rapidement. Combien en plus? Environ 47 % plus vite, avec 4 fois plus de données.

Donc, à l'ère de l'IA, pouvoir transporter plus de données, plus rapidement, représente un avantage significatif pour la qualité du traitement.

Des partenariats pour élargir l'empreinte quantique dans Azure

Il est important de noter que Microsoft et son partenaire Continuum avaient annoncé, il n'y a que quelques mois, un record de 12 qubits logiques. Et en quelques mois, le record fut brisé de nouveau. 24 qubits logiques avec la société Atom Computing. Ce qui, apparemment, est un record. La barrière pour un avantage scientifique quantique serait de 100.

C'est alors que Satya Nadella annonce une collaboration étroite avec Atom Computing et Microsoft, visant à co-créer un nouvel ordinateur quantique commercial, mais pas n'importe lequel : le plus grand ordinateur commercial, intégrant des technologies d'auto-correction et, surtout, un modèle de processeur qui offrira le plus grand nombre de qubits qui soient stables et sans erreur.

Les chercheurs peuvent passer d'un modèle de prédiction statique à dynamique

La mise en place d'Azure Quantum Elements permet désormais à de grandes sociétés de recherche de faire des prédictions dynamiques. Elles sont donc en mesure de valider une structure de protéine dynamiquement, au fur et à mesure que les facteurs externes changent. Il n'y a pas si longtemps, cela aurait pris des années d'essais et erreurs...

Je suis en pleine lecture de ce superbe ouvrage de Yuval Noah Harari. Une merveilleuse suite à « Sapiens », que j'ai dévoré précédemment. Je les recommande fortement.

Si nous considérons que nos émotions sont le résultat de signaux dans le cerveau, et que ces derniers peuvent êtres interprétés et traduits en mathématiques, alors pourquoi est-ce qu'une IA ne pourrait pas l'interpréter, voire même la reproduire? C'est là tout le principe qui soutient sa réflexion. Il jette ainsi un peu une douche froide sur le concept qui veut que l'IA ne peut avoir de sentiment et de conscience, chose que je trouve importante à réaliser, surtout durant cette course vers l'intelligence artificielle générale.

Et il va même plus loin, en soumettant que certains rôles de la société, impliquant justement la lecture de ces sentiments, pourraient être mieux « performés » par une machine, qui n'aurait pas de biais cognitif ou d'historique.

QUANTUM + IA, ÇA SERT À QUOI ?

Imaginez un instant que nos meilleurs modèles IA, d'ici 3 ans, aient soudainement accès à un ordinateur quantique de 100 qubits.

Qu'est-ce que cela impliquerait? Le modèle IA pourrait calculer toutes les possibilités et résultats d'une solution en quelques secondes.

Un peu comme Doctor Strange dans le film « Avengers Infinity War », lorsqu'il examine les millions de futurs possibles.

Donc, le modèle prédictif sera immense... mais encore? Pensons simplement au traitement de l'information, à l'analyse et l'évaluation de risques, aux sentiments, ou même à la créativité. Car si l'IA venait tout d'un coup à être munie de la quantique, qu'est-ce qui l'empêcherait de créer? De faire preuve de créativité?

Attention, je ne parle pas ici de répliquer ce qu'elle a appris sur l'analyse de tous les textes existants de Shakespeare, mais bien de créer à partir de rien. La limite que même notre cerveau rencontre relèverait alors de l'histoire ancienne...

Maintenant, imaginez une équipe de scientifiques, qui souhaiteraient résoudre le problème du réchauffement climatique, avec un ordinateur quantique, des données météorologiques et relatives à la pollution des 100 dernières années, et une IA de pointe. Alors, nous avons une chance de régler ce problème. C'est ce que permet ce genre d'avancée : régler des problèmes qui sont trop grands pour nos capacités actuelles.

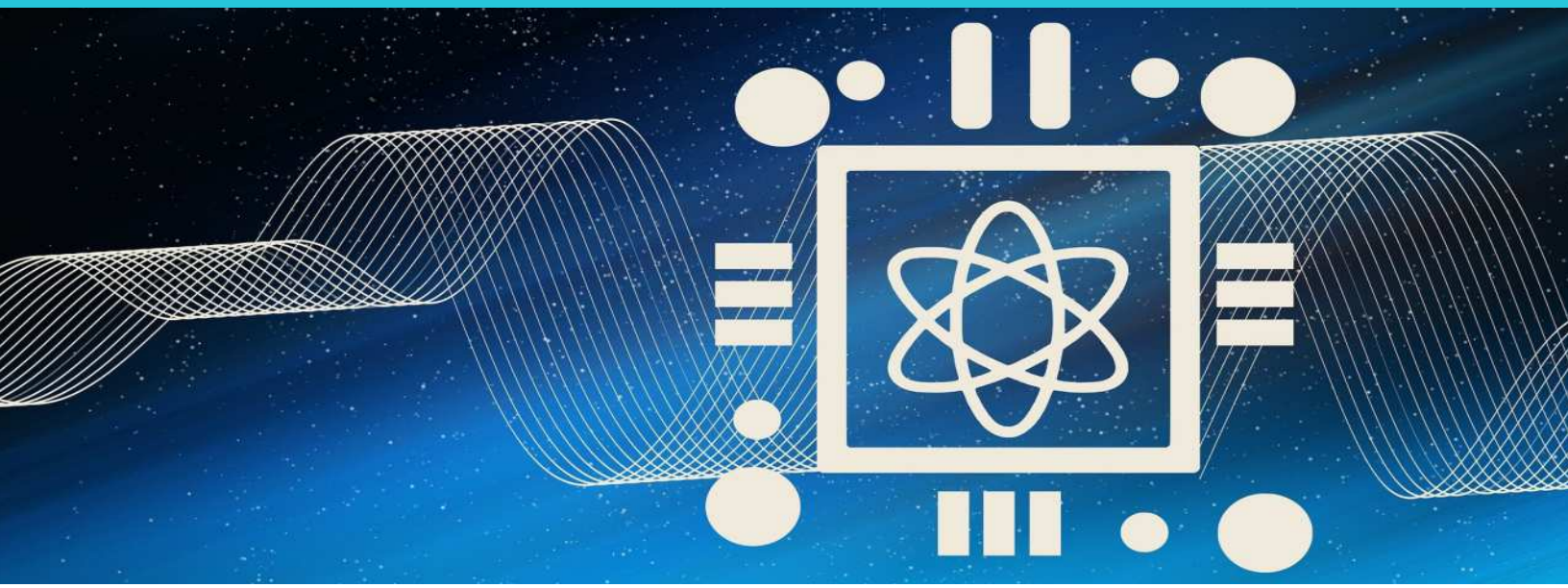
QUEL IMPACT SUR LA CYBERSÉCURITÉ ?

Mais le défi réside dans le fait que la cybercriminalité et le dark web soient désormais la seconde économie mondiale. Donc, si des compagnies comme Microsoft peuvent investir en recherche et développement (R-D) pour des technologies à grand impact, comme celles de la quantique, alors nos compétiteurs du côté obscure peuvent également le faire.

Nous pouvons donc être certains que les cybercriminels vont tout faire pour tirer avantage de ces dernières avancées, et tenterons de l'utiliser pour s'enrichir davantage.

J'ai toutefois bon espoir que les avancées faites sur ce terrain ne feront pas leur arrivée aussi rapidement.

De plus, j'ai personnellement envie de développer pour cette nouvelle plateforme. J'ai même imaginé un produit pour lequel je crois que les PME auraient beaucoup d'intérêt : une plateforme qui permettrait le déchiffrement des compagnies qui seraient victimes d'une attaque de rançongiciel. Mais je vois aussi se dessiner de nombreux autres produits, qui viendraient soutenir la lutte des cyberdéfenseurs contre les cybercriminels.



POURQUOI EST-CE QUE LA CYBERSÉCURITÉ EST UNE PIERRE ANGULAIRE POUR L'IA ?

Comme vous l'aurez deviné, l'IA est nourrie à travers sa base de données. Les modèles sont toujours en mode d'apprentissage et d'amélioration.

Donc, qu'arrive-t-il lorsque quelqu'un a accès à l'altération de votre modèle, et le nourrit de fausses informations? Eh bien tous les systèmes et processus d'affaires en sont affectés.

Si la tendance se maintient, nous aurons bientôt une invasion d'agents, tous propulsés par l'IA, pour accompagner et améliorer l'exécution de nos tâches quotidiennes, que ce soit pour préparer une réponse à un courriel, choisir un film ou même déterminer le meilleur resto à proximité.

Alors, selon vous, est-ce que vos données personnelles et vos données d'entreprise sont prêtes?

Imaginez lorsque vous en serez rendus à analyser votre plan de croissance stratégique avec un agent IA pour obtenir un point de vue externe. Ne croyez vous pas que cela demandera une bonne dose de confiance? Et si une IA corporative a accès à l'entièreté de vos données, êtes-vous sur qu'il n'y aura pas de fuite de données, vers des personnes issues d'organisations qui ne devraient pas les avoir en leur possession? Tant de choses à sécuriser avant d'activer le modèle...

LA LOI DE MOORE À L'ÈRE DE L'IA

La loi de Moore, ainsi nommée par le co-fondateur d'Intel, en 1965, impliquait que le nombre de transistors sur un microprocesseur doublait aux deux ans. Cette règle, traduite librement dans les cercles informatiques, a tenu bon pendant près de 50 ans. Elle est à la veille d'être envoyée aux oubliettes.

La comparaison que je donnais à l'un de mes collaborateurs il y a quelques jours est que le modèle T est sur le point de se faire dépasser par une Tesla.

Depuis l'arrivée de l'infonuagique, nous voyons déjà une cadence d'innovation extraordinaire, entre 600 et 1 000 nouveautés par année. Même cela est à la veille d'être considéré comme antique.

Les prévisions de l'été 2023 voulaient que durant l'été 2025, nous ayons une IA avec un quotient intellectuel de 1 500. En comparaison, Albert Einstein en avait un de 180! On parle donc d'une puissance de calcul décuplée, et d'une intelligence fortement supérieure à la nôtre. Ce monde est sur le point d'être transformé. Pour le mieux, espérons-le...

LES CONNECTEURS

Comment la révolution techno change-t-elle votre vie au quotidien? On veut vous lire!

Pour donner votre avis, témoigner, proposer un sujet, publier une annonce, écrivez-nous à contact@lesconnecteurs.ca

Quand le quantique révolutionne la détection des menaces en ligne

Julien Teste-Harnois
Chroniqueur, LES CONNECTEURS
Président, expert en cybersécurité, Resolock

Dans chaque numéro de LES CONNECTEURS, notre expert Julien Teste-Harnois vous plonge dans une situation de cybersécurité concrète. Découvrez les bonnes pratiques pour éviter les pièges du numérique et protéger vos données avec des conseils clairs et pratiques!

Dans un monde où nos interactions numériques s'intensifient, les réseaux sociaux jouent un rôle crucial, mais ils ne sont pas sans risques. Chaque jour, des plateformes comme Facebook, X ou LinkedIn sont la cible d'attaques : piratage de comptes, campagnes de désinformation, cyberharcèlement. Ces menaces évoluent si rapidement qu'il devient difficile pour les systèmes traditionnels de détection de suivre le rythme. Et si l'informatique quantique était la clé pour inverser la tendance?

L'AVÈNEMENT DE LA PUISSANCE QUANTIQUE

L'informatique quantique, avec ses qubits capables de traiter des volumes massifs de données à une vitesse inégalée, promet de transformer de nombreux secteurs, y compris celui de la cybersécurité. Contrairement aux ordinateurs classiques, qui traitent l'information de manière linéaire, les ordinateurs quantiques peuvent explorer simultanément plusieurs solutions possibles, ouvrant la voie à des modèles de détection beaucoup plus rapides et précis.

Pour les réseaux sociaux, cela pourrait signifier la capacité de scruter des milliards d'interactions en temps quasi réel, afin d'identifier des comportements suspects ou des menaces émergentes. Imaginez un système capable de repérer une campagne de désinformation avant même qu'elle ne devienne virale, ou de bloquer un accès non autorisé en une fraction de seconde.

DES ALGORITHMES DE DÉTECTION BOOSTÉS PAR LA QUANTIQUE

Les algorithmes de détection des menaces actuels reposent sur des analyses statistiques et des modèles d'apprentissage machine. Bien qu'efficaces, ils sont souvent limités par la capacité des infrastructures classiques. Avec la quantique, ces algorithmes pourraient être considérablement améliorés. Par exemple, le machine learning quantique permettrait de traiter des ensembles de données gigantesques beaucoup plus rapidement, tout en détectant des schémas subtils qui pourraient échapper aux systèmes classiques.

Prenons le cas d'un réseau social confronté à une vague de piratages coordonnés. En utilisant un ordinateur quantique, il serait possible d'analyser les connexions entre différents comptes compromis, de repérer des points communs dans les comportements des attaquants et d'intervenir avant que l'attaque ne s'étende. Une telle capacité pourrait transformer la manière dont les plateformes gèrent les menaces.

> **Le potentiel de la quantique pour transformer la détection des menaces en ligne est indéniable.**

Prenons le cas d'un réseau social confronté à une vague de piratages coordonnés. En utilisant un ordinateur quantique, il serait possible d'analyser les connexions entre différents comptes compromis, de repérer des points communs dans les comportements des attaquants et d'intervenir avant que l'attaque ne s'étende. Une telle capacité pourrait transformer la manière dont les plateformes gèrent les menaces.

UNE RÉVOLUTION AUX IMPLICATIONS ÉTHIQUES

Mais cette révolution technologique n'est pas sans soulever des questions. La détection des menaces en ligne via l'informatique quantique nécessiterait un accès massif aux données des utilisateurs. Ces données devraient être traitées avec une transparence irréprochable, mais l'historique des plateformes de réseaux sociaux en matière de respect de la vie privée reste mitigé.

Il y a également le risque de voir cette puissance technologique tomber entre de mauvaises mains. Si les entreprises peuvent utiliser la quantique pour protéger leurs systèmes, les cybercriminels pourraient l'exploiter pour contourner des protections ou mener des attaques d'une complexité sans précédent.

LES DÉFIS TECHNIQUES ET PRATIQUES

Malgré son potentiel, l'informatique quantique en est encore à ses balbutiements. Les systèmes quantiques sont coûteux et difficiles à maintenir. Leur adoption à grande échelle dans la cybersécurité prendra encore des années, voire des décennies.

Par ailleurs, pour intégrer la quantique aux réseaux sociaux, il faudra surmonter des obstacles liés à l'interopérabilité (compatibilité avec les systèmes classiques) et former des experts capables de comprendre et d'exploiter ces technologies.

UN AVENIR PROMETTEUR, MAIS ENCORE LOINTAIN

En attendant que l'informatique quantique atteigne sa maturité, les entreprises qui utilisent les réseaux sociaux doivent continuer de se protéger en appliquant de bonnes pratiques. Le double facteur d'authentification, la limitation des accès des administrateurs et l'utilisation de plateformes de gestion restent des mesures déterminantes pour la réduction des risques.

Le potentiel de la quantique pour transformer la détection des menaces en ligne est indéniable. Dans un futur pas si lointain, il pourrait devenir un allié indispensable pour protéger nos interactions numériques et garantir la sécurité des milliards d'utilisateurs connectés chaque jour.

L'informatique quantique offre ainsi de nouvelles perspectives pour la cybersécurité, mais présente également des défis éthiques, techniques et pratiques. Bien qu'elle soit encore hors de portée pour la majorité des entreprises, son potentiel est tel qu'il est déjà temps de réfléchir à la manière dont elle pourrait être utilisée pour protéger les réseaux sociaux de demain. L'avenir appartient peut-être à ces technologies qui, à défaut de tout résoudre, pourraient améliorer considérablement notre capacité à prévoir et neutraliser les menaces.

« L'IntelligentsIA démocratique »

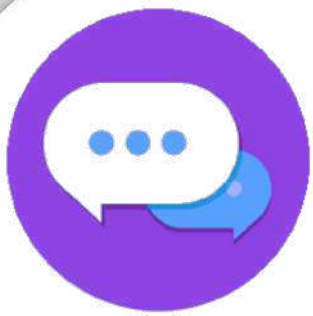
Par Gabriel Landry

L'artiste Gabriel Landry a envoyé à notre rédaction son œuvre, un tableau peint à l'huile qui expose sa perception de l'intelligence artificielle.

L'artiste Gabriel Landry a envoyé à notre rédaction son œuvre, un tableau peint à l'huile qui expose sa perception de l'intelligence artificielle.

« À l'image du cerf-volant, c'est contre le vent que les consciences s'élèvent et que l'humanité grandit. Dans un cas comme dans l'autre, ici, la main et l'œil servent de guide. L'Intelligence ARTificielle, cet outil si précieux à la disposition de l'être humain, est entre les mains et sous le regard de tous : les femmes et les personnes qui s'identifient comme femme, ainsi que les hommes et les personnes s'identifient comme homme, et ce, qu'ils ou qu'elles soient concepteur.trice.s, producteurs.trice.s ou utilisateur.trice.s de cette Intelligence ARTificielle

'L'IntelligentsIA démocratique'. Tel est le titre de ce tableau, qui a été sélectionné pour un prix par AI Impact Alliance, lors d'un appel à projets pour la conférence IA en Mission Sociale édition 2021.
Fondée en 2017, par Valentine Goddard, AI Impact Alliance est une organisation à but non lucratif qui vise à faciliter une mise en œuvre éthique et responsable de l'intelligence artificielle (IA) L'œuvre a trouvé preneur dans les mois qui ont suivi sa réalisation. »



Pour donner votre avis, témoigner, proposer un sujet, publier une annonce, écrivez-nous à contact@lesconnecteurs.ca

LE MAGAZINE ÉLECTRONIQUE

LES CONNECTEURS

POUR TOUT SAVOIR SUR LA RÉVOLUTION TECHNO

GRATUIT
ANIMÉ
INTERACTIF
ACCESSIBLE

CS Le Lab.

VOIR TOUS LES NUMÉROS