Capgemini invent

SÉCURITÉ NUMÉRIQUE ET INFORMATIQUE QUANTIQUE : UNE RELATION ESSENTIELLEMENT PARADOXALE

L'ensemble de nos actions en ligne est régi par un ensemble de règles cryptographiques permettant les échanges sécurisés entre les différentes parties. Alors que nous attendons impatiemment l'émergence de l'application des technologies quantiques, porteuses de progrès technologiques majeurs, Internet se prépare pour le jour où les ordinateurs quantiques seront capables de décrypter nos communications sécurisées, appelé par certains le Q-Day ; une nouvelle menace se profile certainement sur nos données.
Et alors que le hardware quantique n'est pas encore suffisamment mature pour décrypter les algorithmes utilisés, nos données sont déjà à risque des hackers qui accumulent des données cryptées afin de les décrypter dans le futur. Comment alors se préparer à cette éventualité et comment cette menace a, dès aujourd'hui, changé la façon dont nous réfléchissons cette relation entre cybersécurité et informatique quantique ?

L'informatique quantique est une évolution technologique scientifique. A l'inverse, la sécurité numérique est un concept : par essence, elle peut être interprétée différemment en fonction de ses usages, parfois concurrents (B. Buzan, D. Batistella). Explorer la relation entre l'informatique quantique et la sécurité numérique peut donc générer des discours paradoxaux.

LE PARADOXE DU PROGRÈS QUANTIQUE : MENACE OU OPPORTUNITÉ POUR LA SÉCURITÉ ?

Le marché des technologies quantiques foisonne et **les publications de brevets connaissent une croissance exponentielle depuis les 10 dernières années**. L'émergence de nombreux Venture Capitals dans l'écosystème, démontre également l'intérêt du marché pour ces technologies qui amèneront de nombreux cas d'usage en proposant des ordinateurs dotés de puissance de calcul exceptionnelle mais qui offriront **aussi des outils aux cybercriminels pour déconstruire les dispositifs de sécurité** déjà déployés.

Par exemple, via l'implémentation quantique des algorithmes de Shor, il sera possible **de casser les moyens de protections cryptographiques** actuels reposant en majeure partie sur la difficulté actuelle à factoriser des grands nombres premiers dans un temps raisonnable. Ainsi, l'arrivée de l'ordinateur quantique et son utilisation par des réseaux de cybercriminels entraînera un risque fort pour les entreprises. Les données nécessitant un stockage long terme (biométrie, plan de bâtiment stratégiques, PI stratégique, …) pourront alors être facilement accessibles par des entités malveillantes.

Ces menaces remettent alors en question la création d'un espace numérique dit « de confiance ». Le risque est donc trop grand pour rester immobile face à cette révolution quantique, et le lancement d'initiatives au plus tôt est nécessaire pour identifier les risques associés aux différentes activités de l'entreprise et rassurer à grande échelle.

Dans le même temps, de nouvelles technologies promettant une sécurité quantique font leur apparition. Premièrement de nouvelles cryptographies basées sur les mathématiques sont en cours de développement et restent "incassables" même pour les ordinateurs quantiques.

> D'après le point de vue publié par l'ANSSI le 4 janvier 2022, le National Institute of Standards and Technology (NIST) analyse depuis 2016 des algorithmes de « cryptographie post-quantique » (PQC) permettant de décupler les forces de défense du monde virtuel. Cette recommandation de standardisation devrait être publiée d'ici 2024.

Deuxièmement, la cryptographie basée sur la physique, appelée distribution de clés quantiques (QKD), apparaît comme une alternative pour des communications ultra-sécurisées. Alors que la cryptographie post-quantique repose sur le principe qu'aucun algorithme (quantique) efficace n'a été trouvé pour la « casser », la technologie QKD repose sur des principes physiques permettant de détecter l'interception de clé sécurisée. En cas d'interception, ces clés peuvent être régénérées jusqu'à ce que les partis aient la certitude qu'elles soient sécurisées.

Cette standardisation des algorithmes post quantiques est une compétition organisée par le NIST afin d'analyser différents algorithmes et conserver le plus performant.

> Lors de cette compétition, 69 algorithmes candidats ont été soumis en 2017, parmi lesquels seulement 7 ont atteint le 3ème round de qualification en juillet 2020. Les algorithmes sélectionnés lors du 3ème round sont basés sur des problèmes NP-Hard (dont la résolution s'effectue dans des temps exponentiels au mieux) et qui resteront compliqués à résoudre pour des ordinateurs quantiques. Ils sont concentrés autour des problèmes à « lattices » (basé sur le calcul du plus petit vecteur dans un ensemble de points) ainsi que des algorithmes « code-based » (basé sur le décodage d'un code linéaire). Les résultats de ce premier tour furent publiés le 5 juillet 2022.

Enfin, en accélérant drastiquement la vitesse d'apprentissage des algorithmes d'intelligence artificielle et de machine learning, l'informatique quantique va aussi renforcer tous les dispositifs de sécurité qui reposent de plus en plus en plus sur ces technologies. Les Security Operations Centers (SOC) qui déploient des outils de détection de signaux faibles d'attaques et qui ont pour but de repérer rapidement les déviances comportementales des réseaux et des usages, n'en seront que plus performants. Dans tous les secteurs, que ce soit pour détecter les cas de fraude dans la banque ou les incidents industriels, l'informatique quantique augmentera l'efficacité des SOC. En conséquence, **le besoin de montée en puissance des équipes sécurité sur ces technologies déjà visible** ne fera que s'accroître dans les prochaines années.

LE PARADOXE DE LA RECHERCHE QUANTIQUE : ATTENDRE TROP LONGTEMPS OU AGIR TROP RAPIDEMENT ?

Dans toutes les organisations publiques ou privées, la montée en compétence des équipes sécurité sur les enjeux quantiques est encore embryonnaire. Dans le meilleur des cas, les premières réflexions sont orientées autour des apports métier des technologies quantiques laissant les problématiques de cybersécurité et l'analyse concrète du risque et des opportunités au second plan. Un constat renforcé par un **manque de sensibilisation autour du sujet au sein des entreprises** qui limite les initiatives de formations internes des collaborateurs et relaye le sujet à des partenaires externes experts.

Comment professionnaliser l'approche d'une technologie qui n'est pas encore démocratisée ? A quel moment la recherche devient-elle suffisamment réelle pour déclencher des programmes industrialisés ? Alors même que nous entrons dans la phase de développement d'une nouvelle génération d'ordinateur quantique plus puissant, le besoin d'expérimentation pour les entreprises devient essentiel afin de ne pas se retrouver menacé par des réseaux de cybercriminalité qui ont constamment une longueur d'avance sur les lignes de défense et une plus grande agilité sur l'absorption des nouvelles technologies et leur détournement.

La présence des leaders du Cloud (Google, Amazon, Microsoft, IBM, …) sur ce marché, permet une démocratisation et un accès relativement facile à ces technologies. La mise à disposition de ressources quantiques via les plateformes déjà implémentées chez leurs clients permet de créer un terreau très fertile d'expérimentations variées. Mais comment sécuriser les informations sensibles de ces projets lors de l'utilisation d'appareils externes et partagés, à la base même du modèle cloud ? Ce que l'on appelle le «blind quantum computing» garantit que même le propriétaire de l'ordinateur quantique est incapable de savoir quels calculs les utilisateurs effectuent sur les ordinateurs. Néanmoins, bien que cela puisse offrir de grandes applications en termes de protection de la vie privée, il existe, en retour, un risque de perdre tout aperçu des intentions des utilisateurs.

Attendre trop longtemps ou agir trop rapidement : la réponse n'est pas simple et viendra d'un mouvement collectif impulsé par la construction de larges programmes de formation en ingénierie quantique (formations certifiantes, allocation de budgets de recherche, etc.), ou encore le pairing entre organisations et start-ups.

LE PARADOXE GÉOPOLITIQUE : UN ENJEU UNIVERSEL OU UNE QUESTION DE SOUVERAINETÉ ?

Toutes les révolutions scientifiques finissent par devenir universelles d'une manière ou d'une autre. Elles impactent les structures sociétales, les moyens de production et, de facto, les citoyens. La révolution quantique ne dérogera pas à la règle.

Pourtant, force est de constater qu'elle fait l'objet d'une **confrontation géopolitique**. Au même titre que le numérique, l'informatique quantique est un terrain de compétition économique et politique entre les Etats. **Certains Etats investissent plus que d'autres**, impliquant deux phénomènes : un avantage compétitif dans le cadre de l'économie de marché autour du quantique qui se créera dans les prochaines années, et une utilisation à des fins de renseignement national.

La Chine est ainsi en passe de devenir leader des technologies quantiques, notamment dans le domaine des communications, avec un volume d'investissement estimé à 10 milliards d'euros sur cette technologie. Elle possède le plus grand réseau de communication quantique, appelé QKD, disposant de satellites et d'un réseau de fibre optique capable de communiquer sur plus de 4600 km. Il s'agit d'un projet stratégique qui vise à protéger ses communications commerciales et militaires des intrusions.

> La France ambitionne de son coté de devenir leader à l'échelle européenne, avec un plan de 1,8 milliards d'euros sur cinq ans, annoncé en janvier 2021. Avec un écosystème très dynamique de start-ups – comme Pasqal qui développe son offre (un ordinateur quantique capable de calculer à température ambiante, fournissant le meilleur ratio capacité de calcul/énergie consommée au monde) en fusionnant avec Qu&Co pour créer un leader européen, ou Alice et Bob qui lève 27 millions d'euros – et d'académiques autour du plateau de Saclay, la France investit dans des moyens de faciliter les rencontres entre les experts académique et les industriels.

Ce dynamisme donne lieu à de premières réalisations telles que la marine Française qui est en train de développer le système Girafe (gravimètres interférométriques de recherche à atomes froids embarquables), un système de navigation autonome basé sur les technologies de détection quantiques permettant de calculer son positionnement exact sans utiliser le réseau GPS, américain, prévu pour 2026/2027.

Côté Cyber, l'inauguration du Campus Cyber le 15 février 2022 est un autre exemple : elle démontre une volonté française d'organiser de la coopération intersectorielle, publique/privée, autour des grands défis de cybersécurité et des innovations à venir. C'est typiquement le lieu où pourront être discutés les enjeux de l'arrivée du quantique.

L'informatique quantique devient alors une question de souveraineté numérique : l'idée que dans un ordre mondial polarisé, il sera important pour les Etats d'affirmer une puissance quantique et une capacité d'auto-détermination sur son espace numérique. L'informatique quantique va porter des contradictions intrinsèques : le progrès scientifique universel et l'affermissement de nos capacités de lutte anti-cybercriminalité d'une part, et le renforcement d'un conflit géopolitique, économique et une menace à la confiance numérique d'autre part.

Auteurs

Jeanne Heuré
Vice-President - Head of Strategic Services on Digital Trust & Security - Capgemini Invent

Clément Brauner
Quantum Computing Lead - Capgemini Invent

Nicolas Gaudilliere
Chief Technology Officer - Capgemini Invent

A propos de Capgemini Invent

Capgemini Invent est la marque d'innovation digitale, de design et de transformation du groupe Capgemini, qui permet aux dirigeants de façonner l'avenir de leurs entreprises. Etablie dans plus de 36 bureaux et 37 studios de création dans le monde, elle comprend une équipe de plus de 10 000 collaborateurs composée d'experts en stratégie, de data scientists, de concepteurs de produits et d'expériences, d'experts en marques et en technologie qui développent de nouveaux services digitaux, produits, expériences et modèles d'affaire pour une croissance durable.

Capgemini Invent fait partie du groupe Capgemini, un leader mondial, responsable et multiculturel, regroupant 340 000 personnes dans plus de 50 pays. Partenaire stratégique des entreprises pour la transformation de leurs activités en tirant profit de toute la puissance de la technologie, le Groupe est guidé au quotidien par sa raison d'être : libérer les énergies humaines par la technologie pour un avenir inclusif et durable. Fort de 55 ans d'expérience et d'une grande expertise des différents secteurs d'activité, Capgemini est reconnu par ses clients pour répondre à l'ensemble de leurs besoins, de la stratégie et du design jusqu'au management des opérations, en tirant parti des innovations dans les domaines en perpétuelle évolution du cloud, de la data, de l'Intelligence Artificielle, de la connectivité, des logiciels, de l'ingénierie digitale et des plateformes. Le Groupe a réalisé un chiffre d'affaires de 18 milliards d'euros en 2021.

*Get The Future You Want**

Plus d'informations sur www.capgemini.com/invent

** Capgemini, le futur que vous voulez*