Droits et devoirs

Cybersécurité : anticiper la menace quantique

Les experts en cybersécurité conseillent aux entreprises et organismes de se préparer dès maintenant à passer à la cryptographie post-quantique pour résister à la menace qui pèse sur la protection des systèmes d'information.

Alain Bensoussan.

Avec l'utilisation des propriétés du monde quantique, un nouveau stade dans le traitement des données est franchi, avec la promesse d'opérations réalisables à une vitesse jamais atteinte.

Mais ces avancées posent de nouveaux défis en matière de cybersécurité lorsqu'il s'agit de protéger les systèmes d'information contre les attaques utilisant des ordinateurs quantiques. Les autorités de cybersécurité tant nationales qu'européennes prennent très au sérieux ces risques.

La vulnérabilité des systèmes d'informations face à la révolution quantique

La sécurité des solutions cryptographiques déployées aujourd'hui est menacée par le développement des ordinateurs quantiques. Selon l'ANSSI, « *à grande échelle, ils seraient capables d'effectuer certaines tâches beaucoup plus rapidement que les ordinateurs d'aujourd'hui* »[1]. Et notamment être utilisés pour casser les dispositifs de cryptographie conventionnels, mettant à mal la sécurité de nos données.

Certes, les prototypes d'ordinateurs quantiques existants ne sont pas suffisamment puissants pour pouvoir casser le cryptage conventionnel et ne constituent donc pas, à court terme, une menace pour la cryptographie à clé publique. Mais les spécialistes ne doutent pas de l'avènement de l'ordinateur quantique sous la prochaine décennie, ce qui fait craindre à l'ANSSI la « *menace d'attaques rétroactives* » consistant à « *enregistrer dès aujourd'hui des communications chiffrées dans le but de les déchiffrer plus tard* ».

Cette crainte est également partagée par l'agence européenne pour la cybersécurité (ENISA), laquelle alerte sur le fait que « *toute communication chiffrée interceptée aujourd'hui*

© Lexica Art

peut être déchiffrée par l'attaquant dès qu'il a accès à un gros ordinateur quantique, que ce soit dans 5, 10 ou 20 ans »[2].

Cette menace inquiète d'ores et déjà les entreprises américaines. Interrogées par l'un des plus importants cabinets d'audit et de conseil mondiaux, la majorité d'entre elles (50,2 %) indiquent que leur organisation est exposée aux risques d'attaques de cybersécurité de type « *harvest now, decrypt later* (HNDL) », littéralement, « *récolter maintenant, déchiffrer plus tard* »[3] et prévoient de mener des évaluations de risques quantiques au cours des 12 prochains mois.

La menace quantique inquiète d'ores et déjà les entreprises américaines.

La menace est également prise en compte par le Gouvernement français. Le plan France 2030[4] classe comme « prioritaires » les projets subventionnés permettant de répondre à la menace croissante que représentent les ordinateurs quantiques émergents pour les algorithmes de cryptographie actuels.
Dotée de plus de 1 milliards d'euros en deux ans, la stratégie nationale quantique aurait déjà produit des résultats concrets autour de solutions basées sur la cryptographie post-quantique[5].

L'ANSSI recommande de migrer vers la cryptographie post-quantique

Pour contrer cette menace, les experts en cybersécurité se tournent vers la cryptographie post-quantique (PQC), laquelle couvre les « *dispositifs de chiffrement de l'information résistant à un attaquant qui disposerait d'un ordinateur quantique capable de déjouer les méthodes de chiffrement classiques* »[6].

Selon l'ANSSI, la cryptographie post-quantique « *représente la voie la plus prometteuse pour contrecarrer la menace quantique* »[7]. Elle préconise de mettre en place, sans attendre, un planning prévisionnel de migration en 3 phases « *visant à offrir une protection longue durée des informations (jusqu'après 2030) ou qui seront potentiellement utilisés après 2030 sans possibilité de mise à jour* ».

> Les experts en cybersécurité se tournent vers la cryptographie post-quantique (PQC) qui représenterait, selon l'ANSSI, « *la voie la plus prometteuse pour contrecarrer la menace quantique* ».

L'ANSSI rapporte que plusieurs autorités nationales de cybersécurité ont publié des avis similaires recommandant de préparer une migration post-quantique de la cryptographie. Ainsi, le point de vue de l'ANSSI rejoint la position du BSI[8] allemand sur de nombreuses questions comme la nécessité de la migration, l'hybridation ou la « crypto agilité ».

Si l'informatique quantique soulève des préoccupations quant à la confidentialité et l'intégrité des données de nos systèmes d'information, les réglementations sur la protection des données (RGPD notamment), pourraient nécessiter une adaptation face aux défis posés par l'informatique quantique.

Les recommandations du CEPD en matière de cybersécurité

Le Contrôleur européen de la protection des données (CEPD) rappelle que le RGPD[9] pose la sécurité comme l'un des grands principes relatifs au traitement des données à caractère personnel et qu'à ce titre, l'amélioration de la cybersécurité est essentielle.

Consulté sur la proposition de directive européenne SRI sur la cybersécurité adoptée le 27 décembre dernier, le CEPD a souligné la nécessité pour les Etats membres, dans le cadre de leur stratégie nationale en matière de cybersécurité, « *de développer de nouvelles formes de cryptage plus sûres offrant une protection contre les cyberattaques dans le contexte du déploiement d'une infrastructure de communication quantique (ICQ) sûre pour l'Europe, qui offrira un niveau de confidentialité élevé* »[10].

Par ailleurs, dans sa stratégie pour 2020-2024, il prévoit d'organiser des discussions fondées sur « *les pratiques intrusives, émergentes ou hypothétiques, telles que (…) l'informatique quantique et l'informatique de pointe* ».

▶ Alain Bensoussan

1. ANSSI, Point de vue sur la transition de la cryptographie post-quantique, 4 janvier 2022.
2. ENISA, Cryptographie post-quantique : état actuel et atténuation quantique, Mai 2021 (EN).
3. Wall Street Journal du 17 octobre 2022.
4. Plan d'investissement pour la France présenté par le président de la République en octobre 2021.
5. France 2030, Rapport d'activité des deux ans de la stratégie quantique, Mars 2023.
6. Avis CELF, Vocabulaire de l'informatique quantique, JO du 20 décembre 2022.
7. Avis scientifique et technique de l'ANSSI sur la migration vers la cryptographie post-quantique, 14 avril 2022.
8. BSI, Migration zu Post-Quanten-Kryptografie, août 2020.
9. Articles 5 et 32 du RGPD.
10. Avis 5/2021 sur la stratégie en matière de cybersécurité et la directive SRI 2.0, 11 mars 2021.