

La sécurisation des communications par la technologie quantique

Le 17 novembre 2022, le commissaire européen Thierry Breton officialise le projet « Infrastructure de Résilience et d'Interconnexion Sécurisée par Satellites » (IRIS²). Cette constellation de connectivité a pour objectif d'assurer l'autonomie européenne en matière de communications haut débit dès 2027. Son fonctionnement repose sur les phénomènes physiques, à l'échelle atomique, autorisant des communications d'un niveau de sécurité renforcé, entre les acteurs civils et militaires de l'Union européenne (UE).

L'intérêt des communications quantiques

La sécurité des communications repose sur l'échange d'une « clef » connue des seuls interlocuteurs, dont ils se servent pour chiffrer ou déchiffrer leurs messages. Elles ne sont pas pour autant inviolables. L'amélioration des capacités de calcul – permise par les supercalculateurs – augmentera la probabilité de casser la clef. À l'heure du quantique, ces clefs sont élaborées et partagées grâce à l'intrication quantique¹.

Il est en théorie impossible de dupliquer une information circulant par ce canal sans compromettre l'intégrité des informations collectées². Cette « distribution des clefs » (QKD, *Quantum Key Distribution*) permet l'émergence d'un canal de communication, dont la garantie de sécurité de l'information suscite l'intérêt de nombreux États. La simple observation de ces échanges engendre une perturbation (une « décohérence ») qui alerte immédiatement les interlocuteurs. La cryptographie quantique est un moyen de protection contre les attaques cyber passives (modification et disponibilité), actives (divulgaration et interception).

IRIS², la promesse de communications sécurisées

L'intérêt de l'IRIS² repose sur ces principes. Cette constellation permettra de fournir un accès internet haut débit, de renforcer la résilience des communications par la redondance avec les infrastructures terrestres et d'offrir un service sécurisé. Un premier satellite *Eagle1* devrait être mis en orbite d'ici 2024 pour mener une expérimentation de la QKD.

Ce projet s'inscrit dans le cadre plus général du plan *Infrastructure Européenne de Communication Quantique (EuroQCI)* lancé en 2019 par l'UE. En complémentarité de l'IRIS², cette initiative se double d'un maillage terrestre relié par un réseau en fibre optique. S'appuyant sur le comportement des photons, son fonctionnement doit permettre là aussi de garantir la sécurité des échanges. Initiée en janvier 2023, la première phase du projet, dénommé *TeQuantS*, doit aboutir à la construction de terminaux en Allemagne et aux Pays-Bas afin de valider la faisabilité du projet à l'échelle européenne d'ici 2026³.

Un intérêt partagé par de nombreux États

La Chine est le premier pays à avoir réalisé une QKD depuis l'espace en 2017 entre le satellite *Micius*⁴ et une station sol. À l'instar de l'UE, le segment spatial chinois s'accompagne d'un réseau terrestre de communication quantique.

Plusieurs États asiatiques s'inscrivent dans une trajectoire similaire (Singapour et le Japon) et les États-Unis ne sont pas en reste. Avec le *National Quantum Initiative Act* de 2018, Washington a pris à bras le corps la question des applications quantiques dans le domaine des communications, des radars, des GPS et des ordinateurs⁵. Ils portent cette dynamique au sein de leurs partenariats. Dans le cadre de l'*AUKUS Quantum Agreement* d'avril 2022, Canberra, Londres et Washington réfléchissent à l'opportunité que pourraient représenter ces technologies. Pour James Andrew Lewis, directeur de recherches au CSIS, les communications quantiques incarneraient le moyen le plus efficace de garantir leurs échanges, en particulier ceux entre l'Australie et les États-Unis dans le cadre d'un conflit dans l'Indopacifique⁶.

Cet engouement pour les communications quantiques ne doit pas occulter certaines limites. L'emploi de la QKD dans le domaine commercial a mis en lumière des vulnérabilités financières et matérielles. Le recours à ces échanges risque de rediriger les actions de l'attaquant sur les terminaux physiques de l'adversaire plutôt que sur sa couche logicielle. Enfin, on peut s'interroger sur l'endossement final des communications quantiques à l'heure où certaines agences d'État – comme la National Cyber Security Center britannique ou la National Security Agency américaine – émettent des réserves quant à leur intégration au sein d'organismes publics.

1 Le professeur Alain Aspect, prix Nobel de physique en 2022, a démontré le phénomène d'intrication quantique, soit le fait que deux particules très éloignées pouvaient rester corrélées.

2 [Cryptographie quantique \(cea.fr\)](https://cea.fr)

3 [Communications indéchiffrables \(clubic.com\)](https://clubic.com)

4 [QUESS - \(diplomatie.gouv.fr\)](https://diplomatie.gouv.fr)

5 [Quantum Initiative \(congress.gov\)](https://congress.gov)

6 [AUKUS Develop QOC \(nationaldefense.org\)](https://nationaldefense.org)