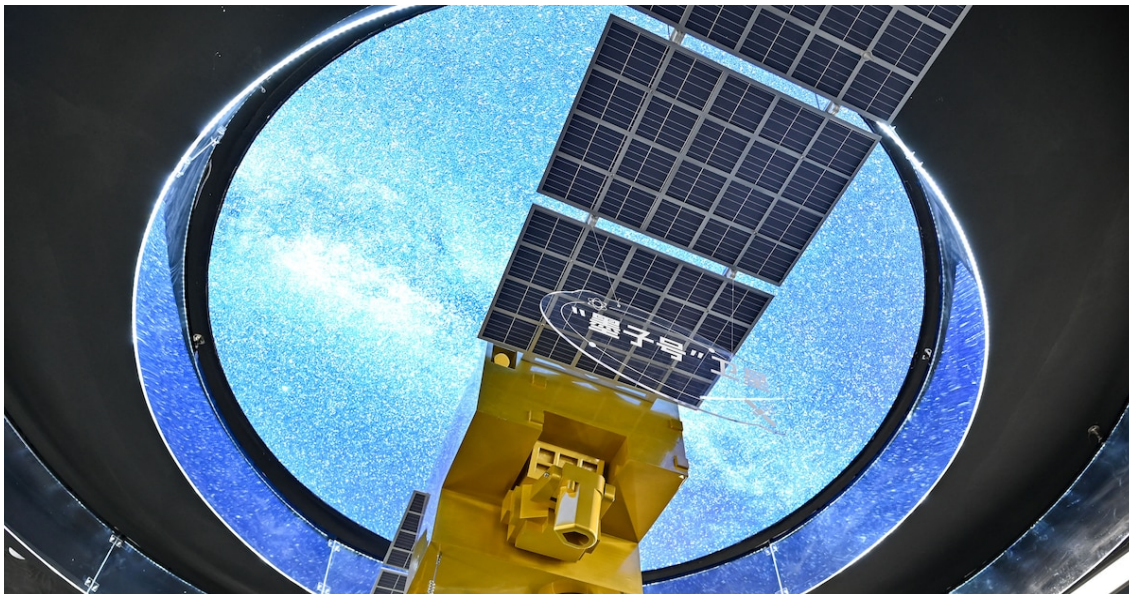


Le quantique, champ de bataille du futur entre les Etats-Unis et la Chine

Tech. La Chine mène aux points dans les communications, les Etats-Unis dans le domaine plus lucratif du calcul.



La Chine a déjà déployé un réseau combinant fibre, satellites (ici, une maquette de Mozi, de China Telecom Quantum) et stations au sol.

Zhang Cheng / Xinhua News Agency/Newscom/MaxPPP

C'est une bien étrange collection que constituent les espions chinois. Depuis quelques années, ils accumulent des messages cryptés interceptés à l'étranger et impossibles à déchiffrer. Pour en percer le secret, un ordinateur classique devrait réaliser des calculs pendant des millions d'années. Les Chinois savent que le temps joue en leur faveur. Bientôt, l'informatique quantique permettra de casser le chiffrement en quelques secondes. Certes, les informations en question ne seront plus de première fraîcheur. Mais même des années plus tard, des secrets industriels, des transactions financières, des correspondances diplomatiques peuvent valoir le détour. La méthode s'appelle "Harvest now, decrypt later" : récolter aujourd'hui pour déchiffrer demain. Les Américains - qui la pratiquent sans doute autant que leur rival - s'emploient activement à s'en protéger.

Deux méthodes le permettent. "La première est d'utiliser de nouvelles méthodes de chiffrement que même des ordinateurs quantiques ne pourront pas percer", explique Edward Parker, chercheur principal en sciences physiques du think tank américain Rand. Un long chantier informatique à lancer dès maintenant pour être prêt à temps. Les Américains avancent méthodiquement. Ils ont choisi de dévoiler les dispositifs de cryptographie post-quantique qu'ils prévoient d'employer. "Une transparence qui les sert, explique Olivier Tonneau, fondateur et associé du fonds d'investissement Quantonation. Les spécialistes du monde entier peuvent ainsi vérifier la solidité de leurs algorithmes et les alerter sur d'éventuelles failles."

La Chine garde, elle, le secret, mais travaille également sur le sujet. Surtout, Pékin a pris une belle avance sur l'autre méthode qui permettra, demain, de protéger ses secrets : les réseaux de communication quantique. "Ils s'appuient sur certaines propriétés de la physique quantique, notamment le fait qu'en observant un photon, on modifie son état", détaille Lionel Martellini, directeur de l'Edhec Quantum Institute. Si un espion intercepte des données, les destinataires légitimes seront ainsi alertés par l'apparition d'anomalies. La Chine est l'auteur de 39 % des publications mondiales sur ce thème précis, contre 12 % aux Etats-Unis. Et elle a déjà déployé un réseau de communication quantique, combinant fibre, satellites et stations au sol sur 12 000 kilomètres.

Les Américains se rattrapent dans un autre pan essentiel de la filière : le calcul quantique. C'est lui qui bouleversera la filière des matériaux, celle de l'énergie et, bien sûr, la pharmacie où cette formidable puissance de calcul aidera à prédire les interactions entre médicaments potentiels et pathogènes. Le monde de la finance pourrait aussi en bénéficier. "Les cas d'usages envisagés ici sont par exemple l'optimisation de portefeuilles ou encore la gestion des risques et la valorisation de produits complexes grâce à des simulations de Monte-Carlo accélérées (NDLR : des modèles mathématiques probabilistes)", pointe Lionel Martellini.

Google, IBM et Microsoft sont les piliers du quantique aux Etats-Unis. Une riche galaxie de start-up y prospère également, adossée à la profondeur sans équivalent du capital-risque américain. Entre 2012 et 2024, les jeunes pousses y ont levé 4,9 milliards de dollars, tandis que leurs concurrentes chinoises plafonnaient à 398 millions, selon le Quantum Index Report du MIT. Une prééminence fragile. Selon le Prix Nobel de physique 2025, John Martinis, les Chinois ne sont qu'à quelques "nanosecondes" des Américains.