La note du CESA
N°90
11 / 2016

Stagiaire Elie Benmamar-Badel

Quel avenir pour la cryptologie face aux défis du cyberespace ?

Les cyber-attaques contre des entités étatiques, notamment le ministère des Finances en 2011, ont mis en lumière les failles sécuritaires des systèmes de communication étatiques. Cette prise de conscience des gouvernements mondiaux a impulsé une vague d'investissements substantielle dans le domaine de la cryptologie afin de s'assurer de la résilience de leurs systèmes d'information. De nouvelles méthodes de cryptage ont vu le jour et promettent, comme souvent, l'inviolabilité des transferts de données.

La *blockchain* appliquée au monde de la Défense

La *blockchain* est considérée comme une révolution numérique majeure de la prochaine décennie. Ce système est à l'origine de la monnaie virtuelle Bitcoin et intéresse par ailleurs les institutions financières et les gouvernements. En effet, la *blockchain* repose sur un registre de transactions en *peer-to-peer*, entièrement décentralisé impliquant que chaque ordinateur du système possède une copie du registre évoluant en temps réel. De plus, son contenu est consultable à tout moment et sa méthode de cryptage lui permet d'être résilient aux cyber-attaques. Ainsi, toutes les modifications du registre sont transparentes, ce qui garantit la validité de toutes les opérations effectuées sur le registre sans intervention d'un organisme. Ce protocole rend théoriquement le registre infalsifiable.

La *Defense Advanced Research Projects Agency* (*DARPA*) et le *Department of Defense (DoD)* ont compris les possibilités qu'offrent cette technologie et pensent s'en inspirer pour créer un système de messagerie sécurisé. Ce système de communication permet de coordonner sur une même plate-forme, les données logistiques, le cryptage des messages et un registre opérationnel partagé. Cette architecture prévient les menaces de cyber-attaques, réduit les délais de communication au sein du *DoD* et sécurise la destruction des documents sensibles ce qui, au regard de l'affaire des mails d'Hillary Clinton, devient crucial. La *DARPA* a décidé de créer une infrastructure dite « *permissioned ledger* » où seules les personnes autorisées peuvent participer à la *blockchain*. De plus, cette dernière est particulièrement appropriée à l'Internet des objets, un des éléments de réflexion de l'armée américaine pour son projet de « soldat du futur ». L'OTAN s'est également intéressée à ce nouveau protocole informatique *via* le *2016 innovation challenge* et veut intégrer cette technologie à ses capacités logistiques et C4ISR[1].

Les nouvelles perspectives de la communication quantique

La République Populaire de Chine (RPC) a, elle aussi, entrepris de se positionner comme un *leader* de la cryptologie mondiale mais à sa manière. En effet, elle a procédé à des investissements importants dans la technologie quantique. Le programme d'État dédié à la recherche fondamentale (dont la physique quantique), est passé d'un financement de 1,9 milliards à 101 milliards de dollars entre 2005 et 2015. L'aboutissement de cette volonté politique a été le lancement en orbite du satellite Mozi, premier satellite de l'Histoire à embarquer un laboratoire quantique capable d'effectuer des communications réputées indéchiffrables. En effet, ce satellite devrait réaliser des transmissions quantiques de clés cryptographiques sur de longues distances, entre deux stations au sol. Mozi sera l'intermédiaire entre une station émettrice d'un signal contenant une clé à photons et une station réceptrice du message décrypté.

Ce système exploite les théories de téléportation et d'intrication quantiques entre deux photons, ce qui est supposé rendre le contenu du message inviolable. L'intrication quantique implique que si l'un des photons contenant la clé est altéré, le second photon jumeau est modifié immédiatement. Ce phénomène permet de déceler toute tentative d'interception ou d'observation. Ce satellite garantirait à la RPC un bénéfice exceptionnel dans le cryptage des communications et lui procurerait un avantage indéniable. Si les expériences sont réussies, la RPC compte étendre le réseau de communication quantique jusqu'en Europe et lancer une constellation de 30 satellites de communication quantique d'ici à 2030 pour couvrir toute la planète. L'Europe n'a pas les moyens financiers de la Chine mais le commissaire européen Günther Oettinger, a annoncé un programme d'un milliard d'euros en 2018 dédié à la technologie quantique et en particulier aux applications en cryptographie et en communication.

L'amélioration des techniques de cryptologie est à double tranchant. En effet, elle permet aux États et à leurs armées de renforcer la sécurité de leurs transmissions. Toutefois, l'affaire Snowden a créé une demande des consommateurs pour des applications chiffrées. La démocratisation de ces dernières via WhatsApp *ou* Telegram *complique le travail des services de renseignement. Ainsi, la multiplication des outils cryptés a poussé les ministres de l'Intérieur français et allemand à demander à l'Union européenne de légiférer sur la question.*

Ces propos ne reflètent que l'opinion de l'auteur.

1 *Computerized Command, Control, Communication, Intelligence, Surveillance, Reconnaissance.*