Cybercoercition : un nouveau défi stratégique

Tribune. Alors que des doutes planent sur la pérennité de la solidarité transatlantique et sur la capacité de l'Europe à s'y substituer, la France doit réagir à deux défis majeurs pour ses intérêts vitaux.

Le premier est la relance de la course aux armements nucléaires entre les superpuissances couplées à la prolifération de ces armes. Les dénonciations américaines, de 2002 et 2019, des deux accords de contrôle des armements ABM (systèmes antimissiles) et INF (missiles de portée intermédiaire) ont servi de justification au développement de nouveaux missiles par la Russie, puis en réaction par les Etats-Unis.

Depuis un an, a lieu une relance de la prolifération nucléaire : blocage du dialogue Washington-Pyongyang et abandon progressif par Téhéran de toutes les contraintes du traité JCPOA *[Joint Comprehensive Plan of Action ou Plan d'action commun]*. L'annonce par le président Erdogan, en septembre 2019, que la Turquie n'acceptait pas qu'on lui interdise d'avoir des armes nucléaires doit être prise au sérieux. Dans ce contexte, la modernisation de la dissuasion nucléaire française est plus que jamais nécessaire pour préserver sa crédibilité contre toute agression ou tentative de coercition visant nos intérêts vitaux.

Lire aussi : Craintes de cyberattaques de l'Iran

Or il existe désormais une autre forme de coercition : celle résultant de cyberattaques contre des infrastructures critiques, entreprises et services collectifs. C'est le risque évoqué par Guillaume Poupard, directeur général de l'Agence nationale de la sécurité des systèmes d'information (Anssi), lors du Forum international de cybersécurité en 2019. Il a révélé l'existence de prépositionnements d'implants logiciels, par des Etats, au sein d'infrastructures critiques pouvant être activés ultérieurement pour saboter celles-ci. Egalement préoccupant est le quadruplement en deux ans des rançonnages numériques qui bloquent l'accès à un système d'information par le chiffrement de ses données et le déverrouillent après paiement d'une rançon.

Une menace majeure

Ainsi l'attaque de novembre 2019 du CHU de Rouen est d'autant plus inquiétante qu'elle a été attribuée au groupe cybercriminel TA505 basé en Russie, pays surveillant habituellement de telles organisations. Ce double type de cybermenace, non explicitée dans la doctrine française de cyberdéfense, est la cybercoercition : action d'un Etat pour influencer et affaiblir les dirigeants d'un autre Etat en démontrant implicitement qu'il peut provoquer, de façon difficilement attribuable, des perturbations sérieuses dans les services collectifs ou des activités industrielles importantes. Une autre illustration de la cybercoercition est la crainte exprimée à propos de la 5G sur la capacité du gouvernement chinois d'interrompre sélectivement le service fourni grâce à sa proximité avec Huawei.

La cybercoercition devient inéluctablement accessible à un nombre croissant de puissances ; elle est une menace majeure pour l'indépendance nationale. Pour y faire face, le renforcement de la protection des infrastructures et entreprises critiques est une condition nécessaire mais non suffisante. Le souhaitable dialogue ne suffit plus ; les Etats agresseurs doivent être convaincus que

la France a la capacité et la volonté de riposter à des tentatives de cybercoercition.

Une cybersécurité défensive forte

L'article L2321-2 du code de la défense qui autorise des ripostes contre des attaques informatiques affectant le potentiel de guerre ou économique national devrait aussi couvrir les prépositionnements d'implants. L'excellente doctrine française de lutte informatique offensive, rendue publique, en janvier 2019, par la ministre des armées, devrait être explicitement élargie à la protection d'objectifs civils critiques en permettant d'engager aussi une riposte proportionnée à toutes poses d'implants ou attaques visant de tels objectifs.

Lire aussi : Les nouvelles cyberattaques qui menacent les banques et leurs clients

Cette « cyberdissuasion » diffère notablement de la dissuasion nucléaire qui est fondée sur des armes de non-emploi alors que la crédibilité de la lutte informatique offensive est assurée par son utilisation effective face à des attaques informatiques quotidiennes. C'est pourquoi nous parlons de « contre-cybercoercition » qui nécessite une cybersécurité défensive forte, associée à une capacité performante et autonome de renseignement permettant d'obtenir une forte probabilité d'attribution des auteurs de ces cyberattaques.

Le développement en propre d'outils techniques complexes doit être une priorité. Dans plusieurs technologies-clés la France possède une excellence scientifique reconnue grâce au très haut niveau de formation de ses ingénieurs et à la qualité de ses organismes de recherche. En revanche, cette excellence n'a pas encore débouché sur une industrie française de logiciels de cybersécurité concurrençant réellement le couple américano-israélien.

Cette dépendance technique pose un problème pour l'autonomie de notre cyberdéfense et elle a un coût économique croissant. L'accélération de la transformation numérique multiplie les vulnérabilités et donc les attaques, ce qui provoque un développement très fort d'une industrie de pointe, la cybersécurité, où la France devrait pouvoir jouer un rôle éminent.

Stratégie, moyens et organisation

Depuis 2008, la France a fourni un effort remarquable de protection des systèmes d'information et de cyberdéfense. Face à l'accélération des nouvelles menaces, il faut adapter notre stratégie, nos moyens et notre organisation selon deux axes : une cyberdéfense associée à une capacité de « contre-cybercoercition » crédible et une industrie au meilleur rang mondial. Les moyens de l'Etat doivent croître beaucoup plus fortement et être mieux mutualisés. Les efforts de création d'un écosystème innovatif doivent être amplifiés. Enfin, une coordination stratégique, comme celle qui existe pour le renseignement et la lutte contre le terrorisme, devrait être créée au plus haut niveau de l'Etat.

Ainsi pourrait se réaliser une nouvelle « œuvre commune » à l'image de celle qui a permis à la France de se doter d'une capacité de dissuasion nucléaire autonome. Cette très forte impulsion lui permettrait de devenir le moteur d'une construction européenne de la cyberdéfense.

Bernard Barbier, ancien directeur technique de la DGSE. Ancien directeur du Laboratoire

d’électronique et de technologies de l’information (LETI), il est membre de l’Académie des technologies.

Jean-Louis Gergorin, chargé de cours à Sciences Po. Ancien chef du Centre d’analyse et de prévision du Quai d’Orsay, il est coauteur de *Cyber. La guerre permanente* (éd. du Cerf).

Amiral Edouard Guillaud, ancien chef d’état-major des armées.