Les 3 propositions de la France pour enrayer la course aux armements cyber

Dans un entretien au *Monde*, David Martinon, représentant spécial de la France pour les négociations internationales sur la société de l'information et l'économie numérique, a détaillé les positions que le pays comptait défendre dans le cyberespace. Alors que se tient à Paris, une conférence intitulée « Construire la paix et la sécurité internationale de la société numérique », la France espère stabiliser un espace en pleine ébullition. Et où les tensions sont plus que perceptibles, comme en témoignent les récentes accusations de Washington pointant la responsabilité de Moscou dans les piratages qui ont émaillé la campagne présidentielle outre-Atlantique.

La France espère s'appuyer sur la conférence qui se tient les 6 et 7 avril à l'Unesco, et qui réunit diplomates, chercheurs, fonctionnaires et experts en cybersécurité à l'initiative du SGDSN (Secrétariat général de la défense et de la sécurité nationale) et de l'Anssi (Agence nationale de la sécurité des systèmes d'information), pour peser sur le prochain round de négociations sur le sujet à l'ONU, des discussions qui se tiendront fin juin. Objectif : parvenir à des règles plus précises, dans ce que David Martinon décrit aujourd'hui comme « *un Far-West* ». « *Le droit est applicable, mais il est peu appliqué, tout le monde agit ou peut agir de manière offensive, et il n'y a pas grand-chose pour brider les intentions malveillantes* », détaille-t-il dans le quotidien du soir.

Freiner le marché des cyberarmes

Concrètement, la France devrait venir à ce round de négociations avec trois propositions sous le bras. D'abord responsabiliser les 'proxies', ces serveurs sur lesquels transitent les attaques et qui servent aux assaillants à masquer leurs traces. Paris voudrait rendre les pays hébergeant ces infrastructures relais en partie responsables des offensives qui transitent par leurs opérateurs ou FAI. Afin de les pousser à faire cesser les attaques dès qu'ils en sont informés. Ce que David Martinon présente comme un « *mécanisme collectif de responsabilité* ». Notons que cette notion figure déjà dans un rapport de 2015 écrit par le groupe des experts gouvernementaux mandatés par l'ONU afin d'établir des règles dans le cyberespace. Mais le cyber-ambassadeur hexagonal entend approfondir cette logique.

Second point d'attention : le marché des cyberarmes. Paris voudrait que l'arrangement de Wassenaar, qui établit un contrôle à l'exportation des technologies pouvant à la fois servir à des fins défensives et offensives – un cas très courant dans le domaine cyber -, devienne universel. Là où seulement 41 pays l'ont signé aujourd'hui (dont la France, les Etats-Unis et la Russie). Enfin, David Martinon voudrait interdire toute forme de *hack back* – de contrattaque – par des organisations privées. « *Un facteur hautement déstabilisateur* », selon le diplomate, qui y voit une forme d'internationalisation du second amendement de la Constitution des Etats-Unis (qui établit le droit de porter une arme).

En pleine course aux armements cyber

Les propositions de Paris risquent toutefois d'être accueillies froidement par nombre de pays, qui trouvent dans le numérique un espace pour lancer des attaques à bas coût et pour lesquelles ils pourront toujours nier toute implication (l'attribution d'un piratage restant un exercice hautement difficile). Mieux : dans le cyberespace, les puissances peuvent même réexploiter les armes développées par d'autres, pour mener des attaques bon marché et qui pointeront vers un autre Etat. La France risque ainsi de trouver sur son chemin la Russie et la Chine – deux puissances soupçonnées d'exploiter le cyberespace pour combler leur retard technologique ou déstabiliser des pays jugés hostiles -, mais aussi les Etats-Unis, où la logique de *hack back* figure dans une proposition de loi.

En particulier, la proposition visant à engager un cyber-désarmement risque fort de tomber à plat, dans un contexte où la plupart des pays ont engagé une politique de renforcement de leurs moyens en la matière. Y compris en Europe, l'Allemagne venant ainsi d'annoncer une unité de 13 500 soldats, vouée explicitement à contrer en priorité les piratages russes. Et, comme dans le domaine conventionnel, c'est toute une industrie qui profite de cette course aux cyber-armements. Dans la préface à une étude sur les cyberattaques publiée à l'occasion de la manifestation de ces 6 et 7 avril, à l'Unesco, Guillaume Poupard, le directeur général de l'Anssi, parle ainsi « *d'un marché des vulnérabilités IT qui a émergé* », un marché qui, s'il était transposé dans le monde physique, « *serait vu comme totalement inacceptable par l'opinion publique* ».

A lire aussi :

Le droit à la cyber-riposte pour tous inquiète l'ANSSI

Hacking des élections : les partis politiques français sont-ils prêts ?

François Hollande veut protéger la présidentielle des cyberattaques

Photo : byzantiumbooks via VisualHunt.com / CC BY