Cyber attaques : bientôt des actes de guerre pour l'Otan

L'Otan va ajouter les cyber attaques à la liste des menaces qui déclenchent **une réponse collective des membres de l'organisation**. Cet ajout au traité de l'Atlantique Nord doit être officialisé en fin de semaine, lors d'une **réunion à Newport, au Pays de Galles**. Reste que les contours de l'accord restent encore flous, notent les experts. D'abord car la nature même de ce qui constituera une cyber attaque aux yeux de l'Otant doit être précisée. Ensuite l'organisation basée à Bruxelles ne dispose **pas d'informations claires sur les cyber-armes de ses membres**, Etats-Unis, Grande-Bretagne, France ou encore Allemagne. Or, sans ces données, difficile de bâtir une cyber-stratégie.

La semaine dernière, dans le *Boston Globe*, Jamie Shea, en charge des menaces émergentes au sein de l'Otan, a clairement laissé entendre que, dans le nouveau traité, « *le domaine cybernétique sera explicitement* couvert par l'article 5 », article prévoyant la solidarité entre les membres en cas d'agression de l'un d'eux. Selon le *New York Times*, cette extension de la clause centrale du traité doit être ratifiée cette semaine, après approbation des ministres de la défense des pays membres en juin.

Cette décision constitue un tournant, l'Otan ayant en 2010 rejeté une proposition visant à inclure les attaques contre les réseaux électriques ou le système financier d'un pays dans l'article 5 du traité. L'extension peut être interprétée comme une volonté d'afficher une **certaine fermeté à l'égard de la Russie**, soupçonnée d'avoir été à l'origine des attaques ayant paralysé l'Estonie en 2007 et la Géorgie en 2008. L'Otan est également à la manœuvre pour tenter d'endiguer la crise en Ukraine. Rappelons que Kiev accuse Moscou d'envoyer des soldats sur place pour soutenir les indépendantistes. Hier, l'Alliance atlantique a annoncé vouloir déployer des milliers de soldats dans l'est de l'Europe, afin d'être « *plus visible* » et de « *frapper fort* » en cas de nécessité. De son côté, par la voix de son Premier ministre, Arseni Iatseniouk, **l'Ukraine a affirmé qu'elle avait l'intention de relancer son processus d'adhésion à L'Otan** face à l' « *agression* » russe.

Les membres gardent leurs cyber-armes pour eux

La signature de Newport apparaît comme un premier pas ; la réelle stratégie de l'Otan en matière de cyber défense étant encore à définir, selon le *New York Times* qui cite des déclarations du secrétaire général de l'organisation, Anders Fogh Rasmussen (en photo). Jamie Shea a, de son côté, confirmé que **la définition de ce qu'est une cyber attaque** déclenchant la mise en œuvre de l'article 5 resterait **pour l'instant volontairement ambiguë**. « *Nous ne disons pas dans quelles circonstances ou quel seuil l'attaque doit franchir pour provoquer une réponse collective de l'Otan et nous ne précisions pas ce que cette réponse collective pourrait être* », glisse Jamie Shea.

Les Etats-Unis, de leur côté, ont déjà affirmé qu'une attaque cyber préparant le terrain à une action militaire classique pouvait déclencher la mise en œuvre de l'article 5. Un cyber assaut entraînant des dégâts matériels importants ou des pertes en vies humaines pourrait également déclencher une réponse militaire classique, a également averti Washington.

Selon Ivo Daalder, un ancien ambassadeur américain auprès de l'Otan et désormais président du Chicago Council on Global Affairs interrogé par le *New York Times*, les états membres comme les Etats-Unis, la Grande-Bretagne ou la France ont refusé de briefer l'organisation sur leurs cyber armes. Les officiels travaillant pour cette dernière en ont donc été réduit à lire les documents soustraits à la NSA par Edward Snowden pour se faire une idée des opérations menées par les Etats-Unis contre la Chine ou l'Iran.

A lire aussi :

Les données des citoyens russes devront rester en Russie
Espionnage de la NSA : les 8 leçons d'Edward Snowden