26/06/2019 08:09:09

Cyberattaque américaine contre l'Iran: le brouillard de la guerre sur le net

Des responsables américains ont affirmé qu'une cyberattaque ordonnée par la Maison Blanche avait neutralisé des systèmes de lancement de missiles iraniens. Mais, comme toujours dans les cyberconflits, la réalité de ce qui s'est passé sera quasiment impossible à établir, préviennent des experts.

Sous couvert de l'anonymat, des sources officielles ont assuré à des médias américains qu'une offensive lancée par le Cyber Command de l'US Army était parvenue à mettre hors service les systèmes informatiques de l'unité aérospatiale des Gardiens de la Révolution iraniens, chargée des tirs de roquettes et de missiles.

C'est une arme sol-air de cette unité qui a abattu, le 20 juin, un drone de surveillance de l'US Navy au-dessus de la mer d'Oman, contribuant à exacerber les tensions dans le Golfe.

Téhéran, par la voix de son ministre des Télécommunications Mohammad Javad Azari-Jahromi, s'est empressé d'affirmer "qu'aucune" cyberattaque de représailles n'avait "réussi, alors qu'ils (les Américains, NDLR) font beaucoup d'efforts en ce sens".

"Le problème, c'est que dans ce genre d'histoire, tout le monde bluffe", assure à l'AFP Julien Nocetti, de l'Institut français des relations internationales (Ifri). "C'est caractéristique en matière cyber: le flou est permanent".

"Il ne faut pas dévoiler votre jeu. Si vous le faites, vous révélez vos capacités d'action et de renseignement. C'est un jeu de chat et de souris extrêmement subtil. Ce n'est pas surprenant que les Iraniens affirment que cela a échoué. Nous n'avons aucun moyen de vérifier la véracité des dires de part et d'autre. C'est ce qui est déroutant", dit-il.

En matière de cyberconflit, le "brouillard de la guerre", selon l'expression du théoricien militaire Carl von Clausewitz, est plus épais que partout ailleurs. Sans front, sans observateurs, avec des preuves et des indices facilement manipulables, l'affrontement se joue au coeur de serveurs informatiques.

Le fait que des officiels américains ont choisi (ou reçu l'instruction) de révéler aussi rapidement cette cyber-offensive est révélateur, estiment des spécialistes, de la volonté de l'administration Trump de montrer qu'elle ne restait pas inactive, même si les chasseurs qui avaient reçu l'ordre de bombarder l'Iran après la destruction du drone avaient été rappelés à la dernière minute.

Mais la réalité de cette cyberattaque, ses modalités, ses objectifs exacts et surtout son efficacité resteront à jamais dissimulés par la brume du conflit, assure à l'AFP Nicolas Arpagian, expert en cyber-sécurité.

"Dans ce cas, des cibles militaires iraniennes ont été choisies", dit-il. "Si cela avait été des cibles civiles, ce serait différent. Des centrales électriques, le courant aurait été coupé. Une compagnie des eaux, des gens auraient fait la queue pour récupérer des bouteilles".

"Là, il n'y a que les Iraniens qui peuvent savoir si leurs infrastructures ont été touchées. La réalité de l'attaque, sa portée? Il n'y a qu'eux qui la connaissent. Tant qu'ils ne sont pas amenés à utiliser leurs missiles, il n'y a pas de matérialité", ajoute-t-il.

"L'arme numérique permet au président Trump de montrer au monde, et surtout à ses partisans, qu'il riposte", conclut-il. "Mais le fait que la cible soit militaire fait que seuls les Iraniens pourraient dire s'ils ont subi des dégâts. Ce qu'ils se garderont de faire, bien sûr".

Un célèbre précédent existe bien: en 2010, une étrange série de pannes avait affecté les centrifugeuses iraniennes utilisées pour l'enrichissement de l'uranium. Téhéran avait alors accusé les Etats-Unis et Israël de les avoir infectées avec un puissant virus informatique.

Il avait toutefois fallu des années pour que le brouillard se dissipe et qu'apparaissent les contours de la fameuse opération Stuxnet, qu'encore aujourd'hui Israéliens et Américains refusent de reconnaître.

Quasiment une décennie est passée, et le Cyber Command (CyberCom) est devenu en mai le dixième commandement de combat de l'armée américaine. L'attaque contre les systèmes de missiles des Gardiens de la Révolution est la première cyber-offensive à lui être --de façon semi-officielle, via des fuites dans la presse-- attribuée.

"Cela fait partie de la dimension cyber", explique à l'AFP Loïc Guezo, secrétaire général adjoint du CLUSIF, le club français de la sécurité de l'Information. "C'est la volonté de montrer qu'on a les ressources et la maîtrise technique suffisantes pour, sur une décision politique, neutraliser un système de l'ennemi".

"C'est l'établissement d'un rapport de force, l'équivalent sur le théâtre des guerres du futur d'un défilé sur la place Rouge avec des centaines d'ogives nucléaires".

Pour Julien Nocetti, "c'est un signal envoyé aux Iraniens. Mais aussi, et peut-être surtout, au reste du monde. Moscou et Pékin vont regarder ça de près".

mm/gk