Cyber-attaques : l'Amérique désigne ses ennemis

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 4 août 2022

https://www.bortzmeyer.org/amerique-designe-ennemis.html

Auteur(s) : Mark Corcoral
ISBN n°978-2-343-22452-7
Éditeur : L'Harmattan
Publié en 2021
———————-

On le sait, l'**attribution** d'une cyber-attaque (« c'est les Chinois ! ») est un exercice difficile. Il faut analyser l'attaque, parvenir à une certitude et, ensuite, assumer de révéler publiquement l'origine. Comme le répète souvent Guillaume Poupard « L'attribution, c'est politique ». Le livre de Mark Corcoral <https://www.editions-harmattan.fr/livre-cyber_attaques_l_amerique_designe_ses_ennemis_mark_corcoral-9782343224527-68453.html> étudie cette question de l'attribution notamment sous l'angle des accusations par les États-Unis : comment se fait l'attribution publique et suivant quels méandres politiques ?

La phrase de Guillaume Poupard, citée plus haut, a un amusant double sens. Elle dit que ce n'est pas à une agence technique comme l'ANSSI d'attribuer une attaque ; cette attribution publique peut avoir des conséquences et c'est donc au pouvoir politique de prendre ses responsabilités. Mais la phrase dit aussi qu'accuser publiquement tel ou tel pays est aussi un choix politique. Plus cyniquement, on pourrait reprendre la phrase d'un collègue de Topaze : « les coupables, il vaut mieux les choisir que les chercher ». Eh oui, quand un État en accuse un autre, l'accusation n'est pas forcément sincère…

Déjà, se faire une opinion est difficile : contrairement à une attaque physique qui va forcément laisser pas mal d'indices, une cyber-attaque ne laisse pas beaucoup de traces, et celles-ci peuvent facilement être imitées (une chaine de caractères en hébreu dans un logiciel malveillant ne signifie pas forcément que c'est un coup du Mossad, il est trivial d'en copier/coller une). Et l'interprétation de ces IOC peut être délicate. J'ai entendu des analystes expliquer que, comme les opérations de la cyber-attaque étudiée prenaient place entre 9 h et 17 h, heure de Beijing, cela menait à soupçonner les Chinois, comme si l'APL était tenue aux horaires de bureau. Et même une fois qu'on a acquis une conviction, il n'est pas facile d'en convaincre des tiers puisque, presque toujours, ceux qui font l'attribution d'une attaque ne donnent aucune information concrète sur les preuves récoltées (pour ne pas donner d'informations aux ennemis, mais aussi parfois pour cacher la faiblesse des preuves).

Et une fois qu'on a son intime conviction, l'attribution publique n'est pas automatique, elle relève de choix politiques, qui peuvent évoluer. C'est ainsi qu'avant, en gros, 2014, les États-Unis ne se livraient pas à des attributions publiques, avant de changer de politique et de multiplier les accusations. (La Russie et la Chine continuent à ne pas faire d'attribution publique pour des attaques précises, même si ces deux pays dénoncent de façon très générale les cyber-attaques dont ils sont victimes. Ils insistent beaucoup sur la difficulté à produire des preuves convaincantes.) Et à partir de 2017, les attributions faites par les États-Unis ne sont plus unilatérales mais impliquent parfois des pays alliés. Le choix dépend de la culture politique de chaque pays, et de sa conviction que l'attribution publique servira à quelque chose, par exemple en terme de propagande, ou bien pour faire avancer des négociations internationales sur une certaine régulation des attaques ou encore pour intimider un adversaire (« je t'ai vu ! »). Le choix est complexe et l'auteur explique très bien les innombrables questions géopolitiques qui sont liées à l'utilisation (ou pas) de l'attribution publique. Cette analyse des raisons qui poussent à attribuer publiquement est le gros du livre.

Un ouvrage que je recommande beaucoup, pour comprendre la complexité des questions de cyber-attaques et la difficulté des décisions à prendre.

(En plus léger, l'excellente BD « Cyberfatale <https://www.bortzmeyer.org/cyberfatale.html> » tourne essentiellement autour d'une question d'attribution, comment savoir qui a fait le coup et, une fois qu'on le sait, que faire de cette information.)

---

https://www.bortzmeyer.org/amerique-designe-ennemis.html