The Daily 202 : De l'évolution de la nature de la cyber-guerre

15 avril 2019 Par James Hohmann *Avec Joani Greve et Mariana Alfaro*
https://www.washingtonpost.com/news/powerpost/paloma/daily-202/2019/04/15/daily-202-how-the-nature-of-cyberwar-is-changing/5cb394d9a7a0a475985bd432/?noredirect=on&utm_term=.c1915d778efb
[Daily 202 est un point quotidien du Washington Post au croisement de la technologie et la politique, NdT]

Vladimir Poutine visite une entreprise de moteurs de fusée à Louhansk, en Russie, vendredi. Le président russe a visité l'usine à l'occasion de la Journée des cosmonautes, un jour férié commémorant le vol dans l'espace de Youri Gagarine, il y a annoncé un investissement majeur dans le développement de nouvelles technologies de fusées. (Alexei Nikolsky/Sputnik/Kremlin Pool Photo/AP)

SAUSALITO, Californie - Une course au cyber armement est en cours, et peu d'Américains en sont conscients.

Lisa Monaco, qui a été conseillère en matière de sécurité intérieure à la Maison-Blanche sous Barack Obama, a déclaré que de nombreux pays étaient en train de changer leur approche du champ de bataille numérique, passant de l'espionnage, domaine initial, à une " surenchère géopolitique ".

" Le jeu s'en trouve déstabilisé ", dit-elle. " Si nous avions eu cette conversation il y a deux ans et demi, j'aurais décrit la menace que je percevais à l'époque comme étant plus diffuse, plus

sophistiquée et plus dangereuse qu'à tout autre moment de ma carrière au gouvernement. Aujourd'hui, j'ai le sentiment accablant que si nous considérons les acteurs de la menace comme fondamentalement alignés dans une course de vitesse - États nations, acteurs non étatiques, hacktivistes, groupes criminels - les États nations se sont, et de loin, mis hors circuit ".

Monaco s'est exprimée vendredi soir lors d'un cycle de conférences de quatre jours sur la cybersécurité, financé par la Fondation Hewlett, une organisation non partisane, qui a réuni quelques dizaines d'initiés de la communauté de la sécurité nationale ainsi que des dirigeants d'entreprises technologiques afin de discuter des menaces auxquelles les États-Unis sont confrontés dans le meilleur des mondes numériques et des stratégies pour mieux y faire face.

Alors que l'ingérence russe dans les élections suscitaient toujours de nombreux commentaires, beaucoup d'interventions ont porté sur d'autres risques émergents - et qui donnent à réfléchir. Il y a chez nombre d'experts le souhait de ne pas mener l'ultime bataille, mais de se préparer pour la prochaine.

" On ne peut pas sous-estimer les dégâts réellement causés par Edward Snowden parce que ce qu'il a fait, c'est de révéler à quel point les efforts des États-Unis étaient ingénieux, et maintenant tout le monde a le sentiment qu'il faut rattraper le retard ", a déclaré Matthew Prince, directeur général de la société de sécurité Internet Cloudflare, faisant référence à l'ancien sous-traitant de la NSA qui est maintenant un fugitif à Moscou.

Monaco a fait état d'informations récentes selon lesquelles le Vietnam s'en prendrait aux multinationales de l'automobile, sans doute dans l'intérêt de sa propre industrie automobile. Elle a ajouté que les Américains doivent alourdir les coûts pour les mauvais acteurs et les isoler. " Nous ne devrions pas être naïfs quant à la difficulté de la dissuasion dans le cyberespace, a-t-elle dit, mais nous ne la mettons pas suffisamment en pratique. "

-- Il est plus facile que jamais pour les pays qui en ont les moyens d'engager des mercenaires pour faire ce qui leur est demandé dans le cyberespace. De nombreux régimes à travers le monde semblent de plus en plus offensifs en matière de contrats passés avec des sociétés commerciales de logiciels espions. Ron Deibert, directeur du Citizen Lab de l'Université de Toronto, supervise une équipe de chercheurs qui surveillent l'utilisation commerciale abusive des logiciels espions et des technologies de surveillance contre les dissidents, les journalistes et les autres piliers de la société civile. Ils disposent de preuves indiquant que des entreprises à but lucratif de pays comme Israël ont aidé les forces gouvernementales de pays comme l'Arabie saoudite et le Mexique à piéger les téléphones de gens qui critiquent leurs politiques. Ils incitent les gens à cliquer sur des liens d'hameçonnage permettant de prendre le contrôle de leur téléphone à leur insu. Une fois que c'est fait, ils peuvent mettre en route microphone, caméra et services de localisation et même lire des textes sur des applications cryptées. Les technologies ont des capacités de mode furtif qui permettent aux méchants de couvrir leurs traces.

" Nous pensons que c'est en passe de devenir une sorte de crise ", a déclaré M. Deibert lors d'un exposé d'une heure sur ses recherches. " Les organisations de la société civile sont ciblées, mais elles ne disposent pas des mêmes mécanismes de défense que le gouvernement ou l'industrie."

-- Le président de Microsoft, Brad Smith, s'est dit préoccupé quant à la possibilité que l'intelligence artificielle émergente et la technologie de reconnaissance faciale tombent entre de mauvaises mains. " Pour moi, la violation la plus grave serait l'utilisation par des gouvernements autoritaires de ces moyens pour tenter de paralyser, voire même d'interdire tout droit de réunion pour exprimer des opinions ", a-t-il dit au cours d'une conversation lors d'un déjeuner vendredi dernier. " C'est en tout cas un grand défi parce que la reconnaissance faciale... encourage ceux qui ont le plus de données.

...C'est la quintessence même d'un nivellement par le bas [dans laquelle les entreprises acceptent toutes les propositions possibles]. ...Très probablement la seule façon d'éviter un nivellement par le bas est de fixer un seuil réglementaire. Nous avons donc besoin que des lois soient adoptées."

Smith a déclaré que Microsoft a refusé des ventes pour cette raison. " Un marché que nous avons refusé il y a environ un an était celui d'un gouvernement autoritaire qui voulait l'instaurer dans une capitale où nous avons estimé que nous n'aurions tout simplement pas l'assurance que les droits humains seraient respectés ", a-t-il déclaré lors d'une séance de questions-réponses à un déjeuner. " Cependant, s'il y avait un hôpital dans ce même pays qui pouvait l'utiliser de sorte à assurer de meilleurs soins de santé, et si c'était lié à un service fonctionnant avec notre propre centre de données - afin que la technologie ne se retrouve pas dans la nature... et si j'étais certain que nous pourrions la contrôler d'une manière responsable - je ne dirais pas forcément non".

Le président Barack Obama tient une réunion en octobre 2014 dans la salle de crise. Lisa Monaco est assise à l'extrême gauche de la table. (Pete Souza/White House)

-- Au vu de la multiplication des cyber-opérations par d'autres acteurs étatiques, Monaco a averti que les sites du gouvernement américain demeurent vulnérables et a insisté pour que l'accent soit davantage mis sur la sécurité des données. Elle a déclaré que les piratages du Bureau de la gestion du personnel (OPM) en 2014 et 2015 ont mis en évidence des faiblesses systémiques. Des responsables américains ont déclaré que le gouvernement chinois est en cause dans la violation de l'OPM, qui a permis à Pékin d'avoir accès aux principales bases de données et de dévoiler les informations sensibles d'environ 22,1 millions de personnes, y compris non seulement les employés et entrepreneurs fédéraux, mais aussi leurs familles et amis.

" L'OPM a été une collection d'horreurs, à commencer par les systèmes en place qui étaient, avouons-le, impossible à sécuriser parce qu'ils étaient trop vieux ", a déclaré Monaco. " C'est la défaillance du gouvernement fédéral et du Congrès dans le financement d'un réel fonds de roulement pour installer des systèmes pouvant être protégés. On n'imaginerait pas que de tels systèmes obsolètes pourraient équiper son installation personnelle ou l'entreprise pour laquelle on travaille !

Elle a ajouté que les serveurs militaires et les réseaux classifiés sont en bien meilleur état, mais que les organismes civils demeurent des maillons faibles. " Il y a des signes de progrès, mais il y a encore beaucoup de travail à faire du côté fédéral ", a déclaré Monaco, ancienne procureure fédérale qui a été cheffe de cabinet de Bob Mueller lorsqu'il était directeur du FBI et a travaillé au ministère de la Justice pendant le premier mandat du président Obama. "Et par ailleurs, la situation ne s'est pas améliorée maintenant que nous n'avons pas de coordinateur de la cybersécurité à la Maison Blanche."

Le gouvernement Obama a mis en œuvre un plan d'action national en matière de cybersécurité, plan qui prévoyait un fonds de roulement de 300 millions de dollars pour remplacer les systèmes existants au sein du gouvernement fédéral. Elle a précisé qu'il avait été demandé à tous les organismes du gouvernement - jusqu'à la Commission sur les mammifères marins - d'identifier celle de leurs informations qui pourrait être la plus précieuse pour un gouvernement étranger.

" Ce n'est pas encore entièrement financé ", a-t-elle dit. " La leçon à tirer, c'est que nous devons examiner les données d'une façon tout à fait innovante. Il ne s'agit plus seulement de sécuriser vos systèmes. Cela continue d'être un problème, mais beaucoup d'entre nous et beaucoup d'organisations sont formés sur ce sujet. Mais nous devons examiner les données que nous recueillons, que nous consultons et que nous utilisons."

-- Eric Rosenbach, qui a été chef d'état-major du secrétaire à la Défense Ash Carter pendant le second mandat de M. Obama et qui codirige actuellement le Belfer Center à Harvard, a déclaré que les autres pays étaient bien moins vigilants et prudents que les États-Unis dans la gestion de cyber opérations offensives. Il a averti que 2016 n'offrait qu'un petit avant-goût du danger.

" Ce qui s'est vraiment passé avec l'élection a été très, très, très, très minime comparé à ce que cela pourrait être. Même si nous voyons cela comme un risque, c'est peut-être encore plus important désormais parce que ce que les voyous ont constaté que la réaction était timide ", a-t-il dit. " Imaginez qu'il y ait une grosse attaque - peut-être contre le GPS, c'est quelque chose qui est vraiment inquiétant."

Ce qui l'inquiète, c'est qu'il pourrait y avoir une réaction excessive ou une hyper-correction à quelque chose comme ça. " Imaginez le lendemain - par exemple après le 11 septembre 2001 - toutes les mesures qui sont adoptées, en particulier si c'est avec cette administration ", dit Rosenbach. " Qu'est-ce qui est le pire en fait : la réaction et les conséquences pour les libertés civiles, la vie privée et la démocratie? Ou le satellite en panne pour qui sait combien de temps ? C'est en tout cas un peu effrayant."