LES TECHNIQUES DE L'INVISIBLE

Une «cyberguerre», vraiment ?


Partie du globe terrestre illustrant l'aspect géopolitique de l'espace cyber © Pete Linforth

La notion de cyberguerre, d'une guerre menée dans l'espace numérique, émerge de plus en plus, mais ne fait pas l'unanimité chez les analystes. Nous faisons le point avec Sébastien-Yves Laurent, spécialiste en cybersécurité et professeur des universités à la faculté de droit et science politique de Bordeaux.

Fini la guerre de tranchées, rangez les tanks et les avions de chasses, le XXIe siècle sera celui de la cyberguerre et les armes seront des logiciels informatiques, commandées par des hackers. Voici ce à quoi nous nous attendions pour ce siècle, envahi par l'informatique. La réalité est pourtant différente. Sébastien-Yves Laurent est catégorique : « Il n'existe pas de cyberguerre ! Les programmes informatiques ne sont pas des armes dans leur nature, c'est grotesque ! » Au-delà d'une erreur dans la nature de l'objet cyber, « parler de cyberguerre masque le fait qu'au moment où il y a des affrontements numériques, il y a de la collaboration, comme le mouvement data, le Peer-to-Peer ou l'envoi de milliards de mails chaque jour », détaille-t-il. La réalité n'est pas aussi manichéenne et « le numérique paraît autant marqué par le conflit que par la collaboration », insiste-t-il. Parlons donc de cyberattaques.

L'enjeu de la sécuritisation

Le monde cyber est souvent perçu comme étant un espace malveillant. Cette impression est notamment due à l'effet de sécuritisation, « le sentiment d'insécurité créé par des acteurs privés ou publics ayant des intérêts à vendre de la peur, que ce soit à des fins commerciales pour les premiers ou politiques pour les seconds, afin de sensibiliser », explique le professeur des universités. Selon lui, « il ne faut pas nier le danger mais il y a un réel effet de torsion de la réalité ».

Les cyberattaques ont commencé au tout début des années 1980 avec des hackers qui testaient les limites de petits systèmes informatiques de l'époque, ce n'était alors qu'un jeu. Mais l'évolution de l'espace numérique est tel que les possibilités de nuire et d'influencer le monde ont explosé. « Une des premières cyberattaques de grande ampleur est l'introduction du virus Stuxnet, par une équipe israélo-américaine, dans la centrale nucléaire iranienne de Natanz en 2009 », évoque Sébastien-Yves Laurent. « L'équipe a réussi à détruire des centrifugeuses de la centrale. ».

Une coopération internationale ?

Pour contrer ces actions malveillantes, la communauté internationale, notamment européenne, s'est réunie à Budapest en 2001, bien avant les premières cyberattaques importantes, pour établir la Convention sur la cybercriminalité. Le problème est que seulement 66 États sur les 194 que compte notre planète ont signé ce traité, à cela s'ajoute la difficulté de déterminer les auteurs des cyberattaques, dans un univers construit pour être anonyme. Mais les États et les entreprises progressent, améliorent leurs outils numériques et identifient régulièrement les hackers. Le choix de révéler ces derniers et de désigner tel groupe étatique ou privé relève, lui, d'une politique propre à chaque pays. On ne plaisante pas avec la politique internationale.

L'heure de l'Armageddon numérique ?

Depuis le début de la guerre qui oppose l'Ukraine à la Russie, le continent européen connaît des cyberattaques qui ne sont pas anodines, et par ailleurs « il n'y a jamais eu autant de coupures de câbles internet sur le continent », révèle Sébastien-Yves Laurent. Si les attaques peuvent cibler le contenant, elles concernent également le contenu. Et pour cause, la bataille de l'information et de la désinformation est primordiale pour gagner l'opinion publique. « Ces cyberattaques, sur le contenu et contenant, stagnent à un niveau relativement élevé depuis le conflit autour de l'annexion de la Crimée par la Russie en 2014. C'est une véritable surprise, car nous nous attendions à un Armageddon ! », s'exclame l'expert en cybersécurité. Pour l'Armageddon numérique, nous attendrons.

Cependant, le cyber est aujourd'hui une composante entière des armées, les armes et les technologies sont connectées. Il faut bien distinguer cette partie cyber des affrontements, des « affrontements cyber », qui ne concernent que la partie informatique. Car à la différence des cyberattaques, la guerre cinétique, celle des mortiers, des fusils-mitrailleurs et des tanks, a tué plusieurs dizaines de milliers de personnes depuis le début de la guerre. Faut-il alors négliger l'évolution des cyberattaques ? Sans doute pas : « Qu'arriverait-il si un jour l'évolution des compétences informatiques permettait d'amorcer des armes nucléaires ? », s'interroge Sébastien-Yves Laurent.

Bastien Florenty


Drône de combat ukrainien R18, illustrant l'utilisation du cyber dans la guerre © Oleksandr Perevoznyk