Le Monde

Le temps des « cyberguerres »

Dans sa chronique hebdomadaire, Alain Frachon, éditorialiste au « Monde », explique que s'il y a plutôt moins de conflits armés aujourd'hui qu'hier, en revanche, le cyberespace est un lieu sans cesse plus conflictuel.

LE MONDE | 14.09.2017 à 06h43 • **Mis à jour le** 14.09.2017 à 07h04

CHRONIQUE. Imaginez qu'une entité étrangère neutralise le système de santé publique d'Ile-de-France. Puis qu'elle s'en prenne à la distribution de l'électricité à Paris. Qu'elle brouille les services de la météo, manipule les courriels du président Emmanuel Macron et s'attaque aux communications de l'armée et de la police. Tout ça à partir d'un clavier d'ordinateur. Personne n'est tué, au moins directement. Aucun bâtiment n'est détruit. Pourtant, même les plus pointilleux des polémologues diraient unanimement : c'est la guerre – on nous déclare la guerre.

Dans l'ère pré-Internet, il y a très longtemps, la France aurait cherché à identifier la provenance de l'agression et serait entrée en conflit armé avec l'assaillant, Etat ou groupe terroriste. On était alors en terrain connu, le monde physique, celui dans lequel on distingue à coup sûr un pilonnage d'artillerie d'un vol d'étourneaux.
Mais, dans les exemples cités ci-dessus, on est ailleurs, dans le silence du cyberespace. Ni chair ni sang, ici, dans ce lieu constitué très tard depuis la création du monde, mais où, par la grâce de la grande révolution numérique, se déroule désormais une bonne partie de nos activités.

L'endroit est dangereux : les affrontements y sont quotidiens. L'époque est paradoxale. En dépit de la constance des guerres moyen-orientales, il y a plutôt moins de conflits armés aujourd'hui qu'hier et il n'est pas sûr qu'ils fassent plus de morts qu'avant. En revanche, le cyberespace est un lieu sans cesse plus conflictuel. Les cyberarmes sont de plus en plus sophistiquées. Peut-on parler d'un état de « cyberguerre » quasi généralisé ? Prédiction de la majorité des experts : avant longtemps, un Etat répliquera par la guerre (conventionnelle) à une attaque informatique.

Cette nouvelle aire de conflits entre Etats est fort bien décrite dans le Ramses 2018 (Dunod, 350 p., 27 euros) – l'état du monde que dresse tous les ans l'Institut français des relations internationales (IFRI). Julien Nocetti et Nicolas Arpagian, notamment, auscultent ce qu'ils appellent « la face sombre de la révolution numérique ». Ils exposent « la déclinaison belliqueuse du cyberespace ». Le front est multiple.

Le logiciel espion remplace James Bond

Le monde que les géants de l'Internet ont fabriqué a ranimé la bataille idéologico-politique. Il redonne vie à la propagande, l'intox de masse, la manipulation de l'information. Il ne les réinvente pas mais décuple leur capacité d'influence sur l'opinion. Le vol de document tient toujours sa place mais le logiciel espion remplace James Bond.

L'affaire du piratage des courriels du Parti démocrate américain en 2016 empoisonne toujours la relation entre Washington et Moscou. Cette même année, dit le New York Times, des centaines, sinon des milliers, de faux comptes Facebook américains, concoctés par des Russes, ont propagé des bobards sur la candidate Hillary Clinton.

Des pirates ont pénétré les ordinateurs de l'agence de presse qatarie. Ils ont tronqué des citations de l'émir Tamim ben Hamad Al-Thani. Ces déclarations falsifiées ont servi de prétexte à la campagne de boycottage menée contre le Qatar par l'Arabie saoudite. A des fins géopolitiques toujours, de fausses photos de massacres de musulmans indiens (en fait, des victimes d'un tremblement de terre au Tibet) circulent sur Internet. Elles servent à entretenir la tension entre le Pakistan et l'Inde. Travail de hackers pakistanais ?
Le deuxième front est plus brutal. C'est celui des attaques informatiques contre les entreprises, les infrastructures publiques, les centrales électriques d'un pays. L'Estonie, la Géorgie, l'Ukraine ont déjà été ciblées. Et certains ne font pas état des agressions dont ils ont été victimes.

En 2015, le Groupe d'experts gouvernementaux (GEG) de l'ONU sur la cybersécurité pointait « une *hausse spectaculaire du nombre d'actes de malveillance dirigés contre les infrastructures vitales des* Etats ». Commentaire des spécialistes de l'IFRI : « *On peut aisément comparer les dégâts d'une éventuelle cyberattaque avec ceux causés par des pilonnages d'armes conventionnelles.* » Les grandes armées du monde sont toutes dotées d'unités de « cyberguerre ».

Les corsaires de l'Internet

Le cyberespace est une zone de non-droit ou presque. Des conventions internationales s'efforcent de régir le statut des armes conventionnelles, chimiques, bactériologiques et nucléaires. Rien de tel pour les cyberarmes, qui prolifèrent. Le GEG de l'ONU s'est séparé sur un échec. Logiciels espions, logiciels tueurs et autres bombinettes numériques sont livrés à peu de frais sur les sites de quelques corsaires de l'Internet.

L'ONU voudrait élargir au cyberespace le champ d'application de sa Charte. L'enjeu est énorme : le cyberespace, relève l'IFRI, offre un potentiel d'attaques de nature à « *mettre en péril l'infrastructure* globale [d'un pays ou d'une région] et les serveurs qui en assurent le fonctionnement ». Pourtant, « le droit international du cyberespace en reste à un stade embryonnaire », dit Julien Nocetti. La diversité des acteurs, qui rend problématique d'identifier à coup sûr l'origine d'une cyberattaque, est l'une des difficultés rencontrées.

Un début de gouvernance supposerait de mettre autour de la table gouvernants et géants de l'Internet. Ces derniers sont des acteurs clés du cyberespace, donc de la « cyberconflictualité ». Par leurs ressources financières et les millions de personnes qui dépendent d'eux, les grands de l'Internet sont plus puissants que nombre d'Etats. Ils doivent participer à l'établissement d'un code de conduite dans le cyberespace. Doctorants en droit international, à vos claviers !