Cyberguerre : la nouvelle donne stratégique du cyberespace

Quand le cyberespace redistribue les cartes du *hard power* traditionnel dans le grand jeu géopolitique mondial et devient une priorité dans les agendas diplomatiques et stratégiques des États.

En 2018, 53 % de la population mondiale est connectée à Internet. Ce village mondial connecté fait du cyberespace un espace difficilement contrôlable et donc vulnérable dont les enjeux reflètent de plus en plus les tensions entre puissances.

Une complexification des cyberattaques

Ces dernières années, le nombre de centres de données dans le monde a subi une augmentation exponentielle : on en compte plus de 4 800 dont 2 670 aux États-Unis, plus de 500 en Chine et plus d'une centaine en Russie. En France, on en dénombre 157, faisant de celle-ci la troisième cyberpuissance européenne, derrière l'Angleterre (451) et l'Allemagne (442). Les centres de données, infrastructures hautement stratégiques du fait du stockage et du traitement des données qu'ils détiennent, constituent des cibles privilégiées pour les cybercriminels. D'après l'Autorité nationale de la sécurité des systèmes d'information (ANSSI), le nombre de cyberattaques a été multiplié par quatre au cours de l'année 2020. La crise de la Covid-19 et le recours au télétravail ont contribué à accélérer la numérisation des services et des entreprises, au bénéfice des réseaux cybercriminels qui gagnent en influence de par leur structuration bien plus efficace et coordonnée. Pour l'année 2020, on recense 1 600 attaques par rançongiciel (*ransomware*) dans le monde dont 130 pour la France.

Le premier épisode de la cyberguerre mondiale a débuté, en 2007, en Estonie, initié par la Russie, qui visait alors à paralyser les réseaux informatiques estoniens : banques, médias, administrations sont totalement dépassés par cette attaque d'ampleur qui met en exergue la dépendance aux infrastructures numériques et informatiques des États dans le monde, ainsi que les nombreuses failles dans l'écosystème cyber. Ces attaques ne se cantonnent pas qu'aux pays baltes et frappent également d'autres régions comme le Moyen-Orient, l'Asie du Sud-Est ou encore les États-Unis. Derrière ces attaques, on peut lire un affrontement indirect entre des puissances régionales rivales, comme à l'heure de la guerre froide, à l'instar d'Israël et de l'Iran notamment. Les infrastructures nucléaires iraniennes sont à cet égard visées à de nombreuses reprises : en 2010, par le virus Stuxnet et, en avril 2021, par l'attaque contre le complexe de Natanz.

Face à un écosystème numérique mondialisé et partagé par un ensemble d'acteurs étatiques, privés, mais aussi criminels, il faut désormais se prémunir des tentatives de cyberespionnage et d'ingérence via les cyberattaques. Les cybercriminels, mais également des entreprises exploitent fallacieusement les données des internautes, à des fins, par exemple, d'intelligence économique et d'influence dans le monde politique. Ceci peut constituer à terme un véritable danger pour les systèmes démocratiques en manipulant les populations via des campagnes massives de désinformation. Cela s'est avéré lors de la campagne présidentielle américaine de 2016, les services de renseignement

américains accusant le groupe russe Fancy Bear d'avoir interféré directement dans les élections afin de favoriser la victoire de Donald Trump.

Le nouveau désordre mondial du cyberespace

Aujourd'hui, dans le cyberespace, le rapport de force historiquement en faveur des États-puissances s'est inversé. Les cyberattaques touchent majoritairement les pays occidentaux, les États-Unis en tête avec, entre 2006 et 2020, 156 attaques, contre 47 au Royaume-Uni, 27 en Chine, une quinzaine en Inde ou en Iran et une dizaine seulement en Russie. Bien que les infrastructures et industries de l'Internet mondial soient concentrées dans les pays développés, la dissymétrie technologique historique au bénéfice des États modernisés tend à s'inverser, avec notamment la robotisation et la numérisation du champ de bataille, nouvel enjeu des armées en dépendance croissante à la technologie. En France, les livres blancs (2008 et 2013) identifient le cyberespace comme un champ de bataille. Ainsi, la mise en réseau du champ de bataille, les systèmes d'information intégrés (comme le SITCOMDE du système français FELIN) ou les systèmes de positionnement intégrés présentent des failles auxquelles les armées numérisées s'exposent dans le futur. De même, les réseaux de câbles sous-marins augmentent l'interconnexion et l'interdépendance du monde tout en présentant une vulnérabilité de taille, d'autant plus lorsqu'ils sont situés dans des zones où le niveau de cybersécurité est très bas, voire inexistant, comme au large de toutes les côtes africaines.

Les États sont donc en perte de souveraineté dans le cyberespace, tandis que la structuration très dissymétrique des cyberattaquants inquiète. Le développement des applications de messagerie chiffrée et des outils d'anonymisation des connexions, en rendant l'identification des cybercriminels de plus en plus difficile, fait du cyberespace un domaine compliqué à contrôler. Par ailleurs, le droit du cyberespace crée des vides juridiques, tandis que des notions comme « cyberattaque », « cyberterrorisme » ou « cyberguerre » restent juridiquement floues. Ces lacunes du droit international et les difficultés liées à l'imputabilité de la cyberfaute limitent la régulation du cyberespace, déjà complexe à cause des tensions entre les pays, souvent liées aux soupçons d'ingérence. Toutefois, les pays les plus touchés par des cyberattaques depuis 2006 présentent également un indice global de cybersécurité en 2020 le plus élevé, révélant une bonne prise de conscience de la menace et de la nécessité d'une amélioration de la cyber-résilience et une bonne intégration du cyber aux stratégies nationales de défense. La cyberguerre, parce qu'elle est historiquement (à l'échelle-temps relativement courte du cyber) une guerre hybride et asymétrique, les moyens qui devront être déployés par les États ne pourront se limiter aux moyens traditionnels de la guerre. Finalement, la cyberguerre ne serait-elle pas simplement la continuation de la politique par d'autres (cyber)moyens ?

Meggie COPPIN & Marion HASTINGS
Anciennes co-responsables du département Sécurité & Défense internationales de l'Institut d'études de géopolitique appliquée