CYBERSÉCURITÉ : EXTENSION DU DOMAINE DE LA LUTTE

Introduction

« Ventre mou » de nos sociétés ultra-connectées[1], la cybersécurité n'est désormais plus un sujet obscur, exigeant la publication d'ouvrages alarmistes pour capter l'attention. Voici quelques années encore, cette notion se limitait aux piratages informatiques de banques et d'entreprises, et ses logiques – il est vrai complexes – ne parlaient qu'à d'étroits cénacles d'experts techniques. Avec la multiplication des vulnérabilités, portées par la connectivité toujours plus importante des activités économiques et humaines, nos sociétés prennent conscience de l'ampleur des enjeux.

Parler et écrire sur la cybersécurité en 2018 impose de se détourner d'une myriade d'essais annonçant l'imminence d'un Pearl Harbor ou d'un Fukushima numérique, qui dévasteraient sur leur passage les acquis de la révolution numérique et plongeraient la vie internationale dans l'abîme. Il n'en demeure pas moins que le piratage informatique est désormais partie intégrante des relations internationales. Dans l'année écoulée, l'intensité des cyber-menaces, comme le spectre des acteurs concernés, se sont considérablement élargis. Les attaques *WannaCry* et *NotPetya* ont servi de signal d'alarme : quand le bon fonctionnement des hôpitaux est menacé, quand des données critiques deviennent soudainement inaccessibles, quand des acteurs économiques de premier plan sont touchés, la stabilité et la sécurité internationales sont affectées[2].

Pour les États, la menace cyber s'articule désormais autour de trois facteurs. Tout d'abord sa dangerosité, sous le quadruple effet de la multiplication des acteurs, de l'accroissement des capacités offensives de certaines puissances, de la prolifération des armes informatiques, et de la démocratisation des techniques d'attaque. Ensuite, l'imbrication des enjeux de cybercriminalité et de sécurité nationale. Les outils traditionnellement utilisés à des fins de fraude et d'extorsion de fonds – tels les rançongiciels comme *WannaCry* – peuvent causer des dommages aux systèmes d'information de l'État ou des opérateurs en charge

1. S. Landau, *Listening In: Cybersecurity in an Insecure Age*, New Haven, Yale University Press, 2017.
2. Discours de Jean-Yves Le Drian devant l'Assemblée générale des Nations unies, New York, 18 septembre 2017.

d'infrastructures critiques, paralysant ainsi la continuité de leurs activités. Enfin une exposition accrue de nos sociétés à la menace, du fait d'une numérisation plus étendue et de l'utilisation à grande échelle d'objets connectés[3].

Pour la première fois, des acteurs non étatiques – sociétés de sécurité privées, hackers individuels ou organisés en réseau, visibles ou non – peuvent avoir des effets globaux au moyen d'actes de piratage informatique. De Julian Assange ou Edward Snowden – pour les plus connus, dont les motivations sont politiques ou idéologiques –, à des hackers criminels opérant dans l'ombre, les actes de certains individus peuvent avoir un effet systémique, déstabilisant une entreprise, une organisation ou même un État.

Les particularités du domaine cyber imposent un défi intellectuel clair : comment intégrer les nouveaux risques dont il est porteur dans un cadre conceptuel et stratégique ? Pour le décideur politique, la difficulté est inverse et plus risquée, puisqu'il s'agit d'adapter des axiomes « datés » pour réduire la menace. Ces problèmes de stratégie ne sont pas propres à l'ère des accélérations numériques ; plusieurs générations de décideurs ont été confrontées à des dilemmes de nature similaire lors des précédentes ruptures technologiques. Les difficultés de conceptualisation sont aujourd'hui amplifiées par les conditions d'instabilité stratégique qui prévalent dans le cyberespace : prééminence de l'attaque sur la défense, problématique de l'attribution[4] des attaques informatiques, volatilité des armes numériques et, plus globalement, diffusion de la puissance[5].

Pour l'analyste des relations internationales, la tendance des spécialistes du cyberespace à le concevoir comme un domaine distinct, immunisé contre les effets de la conjoncture internationale et des processus politiques, peut dérouter. Les problématiques internationales concernant le domaine cyber ne sont pas déconnectées des contextes politiques locaux et régionaux. Les spécialistes de l'espace postsoviétique n'ont pas été surpris que l'Estonie subisse des cyberattaques russes en 2007 ; ou que l'Ukraine

3. Secrétariat général de la défense et de la sécurité nationale, *Revue stratégique de cyberdéfense*, février 2018, disponible sur : <www.sgdsn.gouv.fr>.
4. Sur l'attribution des cyberattaques, voir T. Rid et B. Buchanan, « Attributing Cyber Attacks », *Journal of Strategic Studies*, vol. 38, n° 1, 2014, p. 4-37. Pour les auteurs, l'exercice d'attribution consiste à minimiser les incertitudes sur trois plans : tactique (« art », l'attribution est aussi une science), opérationnel (il s'agit d'un processus aux ramifications quasi-infinies) et stratégique (elle est fonction d'enjeux et d'objectifs politiques).
5. B. Valeriano et R. Maness, *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*, Oxford, Oxford University Press, 2015.

ait servi de terrain d'essai aux capacités cyber de la Russie depuis 2015[6]. Pour les observateurs de l'Asie, il n'est guère plus étonnant que la Corée du Nord se livre à de régulières cyberattaques contre le Sud ; ou que la Chine cherche à obtenir, *via* l'espionnage informatique, ce qu'elle ne peut acquérir sur le marché traditionnel de la sécurité. Pour les experts du Moyen-Orient enfin, le piratage du pétrolier saoudien Aramco en 2012 (30 000 ordinateurs de la compagnie ont alors été détruits) pointe logiquement vers l'Iran. La majorité de ces crises cyber restent locales. À l'ère de l'intensification de la cyber-conflictualité, il importe donc d'avoir, plus que jamais, une compréhension fine du système international et de la nature des crises existantes. En corollaire, relier la cybersécurité aux *area studies* s'impose, tant les représentations des menaces diffèrent d'une région à l'autre.

À cet égard, le piratage de Sony Pictures, en novembre 2014, est éloquent. En réaction à la diffusion imminente d'une comédie satirique sur un complot de la CIA visant à assassiner le leader nord-coréen Kim Jong-un, un collectif de hackers a menacé les cinémas américains qui commercialiseraient le film, avant de rendre publiques des centaines de milliers de données confidentielles provenant de la filiale de Sony. Barack Obama a alors accusé, à la télévision, la Corée du Nord d'être à l'origine de l'attaque. Sony Pictures a retiré le film qui, sous la pression du public et de la Maison-Blanche, a ensuite été commercialisé dans quelques centaines de salles indépendantes. Ce *hacking* est significatif tant par son caractère massif que par l'effet recherché. Il a montré que certaines des actions les plus agressives dans le cyberespace n'étaient pas motivées par des inquiétudes d'ordre militaire, mais par la simple diffusion de contenus, que d'aucuns pourraient juger anodins.

L'incident ayant visé Sony met en lumière un aspect de la cyber-conflictualité qui n'a reçu qu'une attention modérée jusqu'à l'élection présidentielle américaine de 2016 : le potentiel de déstabilisation politique des armes informatiques et outils numériques pour le fonctionnement des démocraties. À cet égard, des divergences fondamentales d'approches du cyberespace peuvent être observées. Pour certains États (États-Unis, pays européens, Japon, etc.), le cyberespace est avant tout un domaine technique que caractérisent les risques qu'imposent les attaques sur les infrastructures permettant le bon fonctionnement des activités financières,

6. Par exemple, l'objectif de *NotPetya* – le programme informatique malveillant parti d'Ukraine en juin 2017 – était militaire, puisqu'il visait la paralysie du pays ; c'était un test qui devait permettre d'isoler les entreprises russes de leurs filiales ou maisons-mères en Ukraine, avant une éventuelle attaque dans un objectif de conquête.

économiques et sociétales. Pour d'autres (Chine, Russie, Iran, etc.), le cyberespace est une composante parmi d'autres de la sphère informationnelle ; la libre circulation de l'information numérisée est perçue comme la principale menace à la stabilité sociopolitique de ces régimes. Ce que les Occidentaux considèrent comme du contenu protégé à divers titres (liberté d'expression, propriété intellectuelle), est perçu à Pékin, Moscou ou Téhéran comme une « menace informationnelle » qu'il importe de circonscrire en interne, et d'exploiter en politique étrangère. Moyen d'intimidation, de propagande et de désinformation, le domaine numérique est, pour ces États, le vecteur idéal du retour à une politique de puissance et de remise en cause de l'ordre international[7].

Dans ces conditions, élaborer une grammaire commune du cyberespace est une mission périlleuse, autant qu'une nécessité impérieuse. On se heurte là à l'une des limites de la comparaison (récurrente) entre domaine numérique et domaine nucléaire[8]. À la différence de ce dernier, le numérique irrigue toute l'activité humaine et économique, au risque d'une crise systémique aiguë. Déstabilisant nos repères traditionnels, les conflits numériques abolissent la distinction entre civil et militaire, entre temps de guerre et temps de paix, et rendent quasi impossible la distinction entre politique internationale et politiques intérieures des États. La puissance se trouve ainsi diffusée et largement privatisée : ces conflits impliquent aujourd'hui moins les diplomates que les entreprises. Là se situe un véritable défi pour la souveraineté des États, comme pour les libertés fondamentales.

Julien Nocetti
Chercheur à l'Ifri

PF

7. Voir à ce sujet les dossiers « Internet, outil de puissance » et « Internet : une gouvernance inachevée », parus respectivement dans *Politique étrangère*, vol. 77, n° 2, 2012, et vol. 79, n° 4, 2014.
8. Sur cette comparaison, voir par exemple : J. S. Nye, « Nuclear Lessons for Cyber Security », *Strategic Studies Quarterly*, hiver 2011, p. 18-38.