De la guerre clausewitzienne à la cyber-guerre

27 juillet 2015

Il y a encore trente ans, tout était, d'une certaine manière, très « normé ». La conduite de la guerre se résumait à un schéma classique, clausewitzien (1) : des belligérants clairement identifiés, s'affrontant sur un territoire géographique circonscrit, avec un arsenal plus ou moins conventionnel. La croissance exponentielle d'Internet a bouleversé la donne, mettant au rebut l'ordre westphalien des équilibres et rapports de force né au mitan du XVII^{e} siècle.

En se jouant des frontières physiques traditionnelles, le cyberespace, cette *« interconnexion mondiale des réseaux servant à transmettre, à traiter ou à stocker les données numériques »*, a tracé de nouvelles perspectives. Un horizon chargé de promesses, mais aussi empreint de menaces. Au point que se pose désormais une question cruciale : l'humanité est-elle à l'aube d'un gigantesque conflit numérique ?

Dans un ouvrage collectif intitulé *La première cyber-guerre mondiale ?* (2) et paru en juillet, plusieurs experts issus des sphères publique et privée, rassemblés sous la houlette du criminologue Xavier Raufer, livrent quelques éléments de réflexion utiles – bien qu'assez techniques sur certains aspects – à propos des répercussions de la révolution numérique sur le monde tel que nous le connaissons.

Certes, estiment-ils, le champ du virtuel, dépourvu par essence de limite spatio-temporelle, offre un terreau fertile en matière de communication, d'accès à la connaissance, de croissance économique, de liberté ou encore de progrès scientifiques. Mais il porte aussi en germes le danger d'une infiltration pernicieuse par des *« prédateurs, qu'ils soient criminels, terroristes, mercenaires ou guerriers »*.

Pour les Etats modernes, l'enjeu est d'autant moins négligeable que le cyberespace, construit *ex nihilo* par la main de l'homme, brouille lignes et repères. Avec lui, ni *« champ de bataille »* ni *« zone de sécurité prioritaire »* ; le péril est ubiquitaire et intangible. Du moins jusqu'à un certain stade. Une cyber-attaque de grande ampleur pourrait, de fait, causer des dommages très concrets au pays qui en serait victime : paralysie de l'économie, destruction d'infrastructures vitales (aux niveaux énergétique et sanitaire), catastrophe écologique...

Conscientes de cette nouvelle réalité, les grandes puissances mondiales repensent progressivement leurs méthodes. Leur priorité : investir dans des cyber-armes, moins coûteuses, plus efficaces et difficilement « traçables ». Ces dernières années, les Etats-Unis et la Chine ont montré la voie. Mais, observent à raison les auteurs, il serait réducteur de se limiter au seul duel entre Washington et Pékin, dont les médias se repaissent à l'excès.

A leurs yeux, en effet, le principal théâtre de confrontation se trouve plutôt au Moyen-Orient, avec, comme acteurs centraux, Israël et l'Iran. La preuve ? *Stuxnet* et *Flame*, deux des plus puissants virus informatiques jamais élaborés, mis au jour en 2010 et 2012 par Kaspersky Lab (3). L'Etat hébreu, appuyé par les Etats-Unis, les aurait conçus dans le but de saboter les installations nucléaires iraniennes de Bouchehr et Natanz. Avec le succès que l'on sait.

Si la stratégie israélienne s'appuie sur un triptyque éprouvé – sensibilisation des jeunes aux problématiques cybernétiques, recherche scientifique et universitaire, sécurisation des systèmes d'information –, celle de la République islamique, en revanche, demeure lacunaire. Ce qui n'empêche pas Téhéran de perfectionner en secret sa force de frappe virtuelle dans le quartier beyrouthin de Dahiyeh, tenu par la milice chiite du Hezbollah...

En croissance perpétuelle, le cyberespace a, par son opacité et sa plasticité, fait naître de nouvelles règles. Fini les concepts éculés liés à la guerre traditionnelle d'antan, place désormais aux conflits sans début ni fin marqués, aux duels à l'asymétrie renforcée où la différence de pouvoir entre « grands » et « petits » tend à s'effacer ; un cadre *« plus propice aux attaquants qu'aux défenseurs »*. Les fous d'Allah l'ont bien compris, qui déversent leur logorrhée empoisonnée sur les réseaux sociaux. Comme le résume Jean-Pierre Filiu, spécialiste de l'islam contemporain cité dans l'ouvrage : *« La Toile est pour le djihad global le vecteur privilégié de diffusion d'une vulgate homicide qui réduit quatorze siècles de tradition islamique à une poignée de citations assénées en boucle et hors de leur contexte. »*

Les hiérarques d'Al-Qaïda, Oussama Ben Laden en tête, avaient très tôt perçu le rôle providentiel que pouvait jouer Internet dans la conduite du djihad, notamment pour donner davantage d'écho à leur propagande. Coûts de matériel réduits, absence de censure, capacité de diffusion mondiale : les avantages potentiels étaient nombreux.

Aujourd'hui, le groupe Etat islamique (EI) – dont on peut regretter qu'il ne soit évoqué nulle part, tant sa capacité de nuisance numérique est de loin supérieure à celle d'Al-Qaïda – a pris la relève des vétérans de la guerre sainte. Comment lutter ? En partant du principe que *« le cybermonde d'octets est une partie intégrante de tous les autres milieux (aérien, maritime, terrestre, spatial) »*, d'abord et avant tout – rappel salutaire. En se préparant au combat, ensuite. Ce qui implique *« d'être dynamique, de réduire (sa) vulnérabilité, de mener une défense (pro)active, de gérer les menaces et de faire preuve de résilience »*. Des pistes intéressantes abordées dans le livre, mais seulement à la marge.

Comme l'expliquent avec justesse les auteurs, le cyberespace, dans lequel se meuvent désormais près de quatre milliards d'internautes (dont un milliard de Chinois), s'est mué en un territoire politique et idéologique qu'il est important d'investir et de conquérir, au nom de *« tous ceux qui ont une certaine idée de l'homme »*. Une cyber-guerre pour mieux préserver l'esprit des Lumières face aux démons sans cesse renaissants de l'obscurantisme...

Aymeric Janier

(1) La guerre clausewitzienne [en référence au général et théoricien militaire prussien Carl von Clausewitz (1780-1831)] s'appuie sur le principe de souveraineté des nations et sur la codification de leurs rapports par le droit international, y compris le droit de la guerre.
(2) La première cyber-guerre mondiale ?, ouvrage collectif coordonné par Xavier Raufer, MA Editions, juillet 2015, 205 pages.
(3) Kaspersky Lab est une société spécialisée dans la sécurité des systèmes d'information. Elle a été fondée en 1997. Son siège social se trouve à Moscou.

Pour aller plus loin : lire « Géopolitique du cyberespace », grand dossier de la revue *Diplomatie* (octobre-novembre 2014).