Analyse de Nicolas ARPAGIAN*

La cyberstratégie

Début novembre 2010, le Nicaragua s'est appuyé sur des images de Google Maps, le service de cartographie de Google, pour justifier l'entrée de ses troupes au Costa Rica. Ces soldats ont en effet franchi le fleuve San Juan pour planter leur drapeau national sur l'île costaricaine de Calero. Google Maps avait attribué au Nicaragua cette terre reconnue au Costa Rica depuis 1897. Même si Google explique désormais que ses équipes s'efforcent de fournir des cartes le plus à jour possible, la firme de Moutain View (Californie) précise qu'en « aucun cas il ne faut s'y référer pour décider d'opérations militaires entre deux pays ». Cet épisode diplomatico-numérique illustre la place majeure qu'occupe désormais Internet dans les relations entre les organisations. À l'instar de la mobilisation des internautes qui a secoué la Toile ces dernières semaines quand le fabricant de vêtements GAP a décidé de changer son logo. On imagine des sujets plus sensibles dans le monde actuel... Et pourtant ! La polémique née du nouvel emblème (pétitions en ligne, forums Internet dédiés, tombereaux de courriers électroniques adressés à l'enseigne...) qui s'est propagée sur le Net a conduit le géant du textile à faire marche arrière. Malgré ses investissements préalables et la remise en cause de sa stratégie d'évolution d'identité visuelle. La force de la mobilisation collective ! Au-delà de ces assauts numériques qui se fondent sur des contenus, on constate la généralisation d'attaques informatiques visant à prendre le contrôle à distance d'installations stratégiques. Le cas du virus StuxNet, apparu mi-2010 et rendu largement public cet automne, qui a frappé notamment des infrastructures industrielles iraniennes, est particulièrement éclairant. Il s'épanouissait notamment dans les équipements dotés de solutions Siemens. On voit donc que l'attaque peut s'appuyer sur des briques technologiques utilisées à l'insu de leurs légitimes installateurs, propriétaires ou gestionnaires. Toute faille technologique étant alors bonne à exploiter. Lors du conflit russo-géorgien de l'été 2008, les dix-huit appareils composant l'aviation militaire de Tbilissi ont été cloués au sol par des interventions informatiques. Là encore, plutôt que de les abattre lors d'un duel aérien, l'adversaire semble avoir opté pour la neutralisation préalable. Créant en outre un sentiment d'impuissance parmi la population géorgienne. C'est une chose de perdre au combat. C'en est une autre de ne pouvoir même pas entrer sur le ring. Preuve supplémentaire du caractère éminemment sensible de cette thématique cybernétique, l'annonce faite début novembre 2010 par les États-Unis de la mise en place opérationnelle d'un Cyber-Command. Un état-major dédié – aux côtés de ceux des marines, de l'US Navy et de l'Air Force – aux domaines cybernétiques. Longtemps discuté, cet organe serait donc désormais en ordre de marche, selon le communiqué du Pentagone. Un dispositif qui plaide pour la prise en compte de la maîtrise des technologies de l'information en général et d'Internet en particulier dans les composantes de souveraineté d'un État. Et l'impérieuse nécessité pour les entreprises d'élaborer une véritable stratégie en ce qui concerne la protection de leur patrimoine numérique. Il ne s'agit certainement pas de science-fiction, mais bel et bien de conserver sa capacité à être présent, audible et actif sur le réseau mondial.

---

* Rédacteur en chef de la revue « Prospective Stratégique ».
Auteur de « La cybersécurité » (coll. Que sais-je ?, PUF, 2010).
Directeur scientifique du cycle « Sécurité numérique » à l'Institut national des hautes études de la sécurité et de la justice (France).
Professeur à l'ESA – Beyrouth.

En coopération avec : Ecole Supérieure ESA des Affaires