La cyberdéfense : un enjeu mondial, une priorité nationale

En avant-propos du rapport d'information qu'il a fait, au nom de la commission des affaires étrangères et de la défense, Jean-Marie Bockel rappelle que le Livre blanc sur la défense et la sécurité nationale de 2008 avait déjà identifié les attaques contre les systèmes d'information comme l'une des principales menaces qui pèsent sur notre défense et notre sécurité.

Et de citer les rédacteurs du Livre blanc : « *Les moyens d'information et de communication sont devenus les systèmes nerveux de nos sociétés, sans lesquels elles ne peuvent plus fonctionner. Or, le « cyberespace », constitué par le maillage de l'ensemble des réseaux, est radicalement différent de l'espace physique : sans frontière, évolutif, anonyme, l'identification certaine d'un agresseur y est délicate. La menace est multiforme : blocage malveillant, destruction matérielle (par exemple de satellites ou d'infrastructures de réseau névralgiques), neutralisation informatique, vol ou altération de données, voire prise de contrôle d'un dispositif à des fins hostiles.*

Dans les quinze ans à venir, la multiplication des tentatives d'attaques menées par des acteurs non étatiques, pirates informatiques, activistes ou organisations criminelles, est une certitude. Certaines d'entre elles pourront être de grande ampleur ».

Aujourd'hui, estime Jean-Marie Bockel, le sentiment qui prédomine est que l'ampleur de la menace a été largement sous-estimée et que, « *depuis 2008, les risques et les menaces qui pèsent sur le cyberespace se sont nettement confirmés, à mesure que celui-ci devenait un champ de confrontation à part entière avec la montée en puissance rapide du cyber espionnage et la multiplication des attaques informatiques en direction des Etats, des institutions ou des entreprises. Les risques identifiés par le Livre blanc comme étant de long terme se sont donc en partie déjà concrétisés et la menace atteint désormais un niveau stratégique* ».

Et de rappeler les attaques informatiques massives qui ont frappé l'Estonie en 2007, et en France, celles contre les systèmes d'information du ministère de l'économie et des finances, découverte fin 2010 à la veille de la présidence française du G8 et du G20 ; celles, de grande ampleur, dont la Présidence de la République aurait fait l'objet récemment ; l'affaire, révélée par la presse, d'espionnage via l'Internet du groupe Areva…

Et d'évoquer aussi les virus Stuxnet, qui a gravement endommagé des centrifugeuses du site d'enrichissement d'uranium de Natanz, retardant ainsi de quelques mois ou quelques années la réalisation du programme nucléaire militaire de l'Iran et Flame, vingt fois plus puissant, qui laissent présager l'apparition de nouvelles « armes informatiques » aux potentialités encore largement ignorées.

Avant de poser LA question : dans ce contexte, la France est-elle suffisamment préparée pour se protéger et se défendre face aux attaques informatiques ?

Réponse…et propositions dans le rapport sénatorial, à lire dans notre base « Ressources documentaires », rubrique Législations et réglementations françaises, Sénat, rapports.