Cyberguerre : l'impréparation est plus généralisée qu'il n'y parait

- Informatique - Sécurité Informatique -

Date de mise en ligne : jeudi 25 fÃ©vrier 2010

Spyworld Actu

La France est peut-être bien moins en retard, en matière de cyberdéfense, que certains discours ne pourraient le laisser à penser. Le Royaume-Uni et les Etats-Unis ne seraient, en fait, guère mieux lotis. C'est ce que laissent à penser un rapport encore confidentiel du nouveau centre opérationnel de sécurité informatique britannique et le témoignage, devant de le Sénat américain, d'un ancien directeur des services de renseignement des Etats-Unis.

« Si la Nation devait être, aujourd'hui, engagée dans un conflit cybernétique, nous perdrions. » Mike McConnel, vice-amiral en retraite et ancien directeur des services américains de renseignement, a ainsi résumé le niveau de préparation des Etats-Unis face à la perspective d'un cyberconflit, lors d'une récente audition devant la Commission du Sénat pour le Commerce, les Sciences et les Transports, en préparation d'un projet de loi sur la cybersécurité. Pour lui, la situation est simple : « nous sommes très vulnérables, nous sommes hyper connectés, nous avons beaucoup à perdre. » Pire, selon lui, « nous ne contiendrons pas ce risque [...] et cela conduira à un événement catastrophique. » Pourquoi ? « Parce que dans notre merveilleuse démocratie, il faut souvent un déclencheur pour nous pousser à l'action. » Bref, pour lui, « on va en parler, on va agiter les bras », mais rien de concret n'en ressortira avant une « catastrophe. » Au-delà, le gouvernement américain sera néanmoins appeler à jouer un rôle plus important sur le marché des télécommunications. Surtout, il faudra faire évoluer Internet vers plus d'authentification, « la base de la sécurité », selon lui, plus que le chiffrement des données. Par « rôle » du gouvernement, Mike McConnel entend régulation, ce qu' il explique au travers de l'exemple historique du développement des chemins de fers outre-Atlantique, à la fin du XIXème siècle. Bref, pour lui - et quelques autres experts entendus à la même occasion -, à l'issu de son développement, Internet a des airs de World Wild West en manque de pacification.

Situation guère plus brillante au Royaume-Uni

Outre-Manche, le tableau n'est pas source de plus d'enthousiasme. Selon nos confrères du Register, l'agence d'interception de signaux GCHQ (héritier des efforts britannique de déchiffrage de signaux adverses pendant la seconde guerre mondiale, et hôte pour l'Europe des équipements d'écoute du réseau d'interceptions électroniques Echelon) a récemment attiré l'attention du gouvernement sur cette question. En particulier, son nouveau centre opérationnel de sécurité informatique (CSOC) estimerait que l'administration s'appuie de plus en plus sur Internet pour les services publics et que le « point de non retour » est proche : « la moindre interruption d'accès haut débit devient intolérable et peut avoir un impact sérieux sur l'économie et sur le bien être du public. » Qui plus est, une attaque informatique réussie contre les services publics en ligne aurait un « impact catastrophique sur la confiance qu'accorde le public au gouvernement. » Au-delà des intérêts économique et du public, le rapport s'intéresse donc aux intérêts des gouvernants eux-mêmes. De quoi tirer sur une corde sensible ?

Quelle menace ?

Reste que, pour Mike McDonnel, la menace n'est pas une cyberguerre ouverte, entre Etats. Il estime en particulier que que « la Chine n'a aucun intérêt à déstabiliser l'économie américaine. » Une allusion à peine voilée aux récents débat autour de l'attaque de plusieurs grandes entreprises américaines. Pour lui, la menace est plutôt à chercher du côté de groupes de cyber-guerilla, ou de groupuscules « extrémistes » plus ou moins autonomes et peu contrôlables. Du côté britannique, le CSOC va plus loin, évoquant la menace « d'acteurs étatiques louant les services de criminels ou exploitant des 'hacktivistes' pour engager des opérations de cyber-offensives qu'ils pourront nier. » Et d'anticiper sur la menace, pour la sécurité des transmissions, de l'analyse cryptographique quantique. Un domaine dans lequel, selon nos confrères, la NSA aurait commencé à investir lourdement. Entre autres.

Au final, ces analyses renvoient directement à celles que'effectuaient les participants au Forum International de la Cybercriminalité de mars 2009, à Lille : la plupart des acteurs présents s'accordaient pour souligner les limites des efforts déjà engagés en matière de prévention et de répression.

Post-scriptum :

http://www.lemagit.fr/article/etats...