Les Etats-Unis ne sont pas prêts pour la cyberguerre

« *Le territoire des Etats-Unis n'est* ***pas préparé à une attaque hostile*** *de taille majeure contre ses intérêts et réseaux vitaux* », voilà ce que rapporte l'agence de presse *Reuters*à l'issu d'une **simulation de cyberguerre**.

Pendant deux jours, **230 représentants du gouvernement et des industries** se sont livrés à un cas d'école de type cyber-attaque des réseaux. Ces responsables des agences de sécurité, du gouvernement ou encore de compagnies privées en sont arrivés au même constat : des **failles** dans les communications ou bien dans la **chaîne de commandement** ont été révélées au grand jour.

Ce cycle de simulations mis en place un an après l'arrivée au pouvoir de Georges W. Bush a pour objectif d'aider les responsables américains à **connaître les défauts du système** et apprendre des éventuelles méthodes d'attaques imaginées par des hackers. Une prise de conscience du président républicain au vu des conséquences que pourrait entraîner une attaque d'envergure sur les **systèmes bancaires** ou sur l'ensemble des **infrastructures énergétiques du pays.**

Au titre des ennemis potentiels, les responsables américains n'ont pas établi de « liste noire » des Etats vers lesquels les menaces pourraient provenir mais disent s'attendre à des **attaques du type que celle qu'a connu l'Estonie** en 2007. A savoir des intrusions sur les sites officiels et les services vitaux d'un pays.

Durant cette simulation, visant à observer une « **vulnérabilité économique**« , le but recherché par les participants était d'améliorer les connexions entre industries privées et le Gouvernement.

Le secrétaire d'Etat à la Sécurité Intérieure **Michael Chertoff** a averti les participants que ce type de **cyber-attaques allait devenir chose commune dans les années à venir** afin de « *dégrader la chaîne de commandement avant une attaque bien physique. En addition à une menace d'attaque criminelle ou terroriste*« . Un avertissement à la nouvelle équipe mise en place par Barack Obama (voir encadré) qui devra se faire à l'idée d'être sous la **menace constante** pour protéger ses réseaux.

Déjà, le futur président, alors simple candidat, s'était penché sur la question du cyber-terrorisme. Lors d'un discours, il préconisait déjà quelques mesures: « *Si j'étais président, je mettrais la* ***cybersécurité à la place qu'elle doit être, c'est-à-dire, une priorité principale****. Je déclarerais notre infrastructure informatique comme un* ***avantage stratégique*** *et nommerait un conseiller national du cyber, sorte de conseiller personnel*« .

Barack Obama, après avoir été le premier président Web 2.0, sera-t-il l'instigateur d'une **nouvelle politique de défense américaine**, reléguant le bouclier de défense antimissiles de son prédécesseur à un positionnement digne de la guerre froide ?

Les hommes (de sciences) du Président Les tenants de la cyber-guerre feraient-ils leur entrée dans le bureau ovale ? Une sorte de « *Thinktank* » (centre de réflexion) pourrait voir le jour, **plutôt qu'un unique Monsieur sécurité** au sein des services gouvernementaux américains.C'est donc **John Holdren**, l'actuel patron du *Woods Hole Research Center*(organisme spécialisé dans l'environnement, les eaux et forets ou encore le cycle du carbone…), qui a été nommé **directeur du bureau science et technologie de la Maison Blanche.** Il sera épaulé par Steven Chu, un expert reconnu dans les énergies nouvelles.Au-delà des nominations, c'est le **caractère particulier donné aux scientifiques** au sein de l'administration Obama qui peut étonner. Un **statut de première importance** conféré à la science et à ses scientifiques. Une place qui peut amener des **changements dans la politique américaine**. Loin, très loin des discours créationnistes évoqués sous l'ère Bush.