

Le FBI constate des cyber-attaques de pays particulièrement « doués »

Même s'il faut lui reconnaître quelque peu le sens du dramatique, James Finch, directeur adjoint de la division cybercrime du FBI rappelle que la Russie et la Chine figurent en tête de leurs préoccupations.

« *Certains Etats frappent à notre porte tous les jours et sont une **menace pour la sécurité nationale*** » ajoute le responsable. Preuve en est les récentes attaques de la Russie contre son voisin géorgien. Signe que la cyber-guerre est désormais courante dans les conflits. Ce week-end, en parallèle des [bombardements](#) des villes de Gori et de Tbilissi, les **services géorgiens auraient donc été rendus aveugles**.

Dès lors, le gouvernement américain voit se poser les mêmes problèmes que ceux de son secteur privé. A savoir que la maintenance de certains réseaux informatiques sont délégués à des infrastructures privées, il peut alors leur être difficile de ne pas se faire dérober certaines données sensibles.

Certains officiels pensent désormais que le gouvernement devrait plus se préoccuper de l'infrastructure des réseaux y compris **celle des gros calculateurs configurés en batteries ('grid')**. Cette proposition soulève cependant un problème de taille que relève James Finch : « *si vous avez un modèle de fonctionnement basé sur le profit, ce n'est pas au gouvernement seul de supporter la responsabilité d'un risque de crash* » .

D'un autre côté, Mischel Kwon, le directeur de l'U.S CERT pense qu' « *il n'est pas concevable pour des agences émanant du gouvernement de créer un réseau 'sécurisé' qui divorcerait d'Internet* » .

Les services américains s'interrogent donc quant à la politique à suivre en matière de cyberdéfense. Nul doute qu'ils en sauront en peu plus dès la rentrée lorsque les [candidats à la Maison Blanche](#) se positionneront clairement sur la question.