La Bourse de Tel-Aviv, visée par des hackers propalestiniens. Un défi majeur de sécurité.

JACK GUEZ/AFP

Cyber-djihad contre Israël

Moyen-Orient *Les récentes attaques lancées sur des sites israéliens ne sont rien comparées aux hypothèses de cyber-terrorisme retenues par l'État hébreu. Une vraie guerre a commencé.*

Ox Omar, hacker saoudien, contre Ox Omer, hacker israélien ! Leur affrontement, ces dernières semaines, a fait entrer le Moyen-Orient dans une dimension nouvelle de l'opposition radicale entre l'État hébreu et le monde arabe : la guerre cybernétique, une sorte de cyber-intifada ou de cyber-djihad auquel Israël n'était pas habitué.

Cette bataille a commencé en janvier par la diffusion sur la Toile de 20 000 numéros de cartes de crédit israéliennes, cyber-agression aussitôt revendiquée par Ox Omar. Ont suivi les attaques lancées contre les sites de la Bourse de Tel-Aviv et de la compagnie aérienne israélienne El-Al, menées par le même pirate, associé cette fois à un groupe de "hackers propalestiniens". Les Israéliens ont riposté. Leur contre-attaque, conduite par un groupe de pirates israéliens, a mis en ligne des numéros de cartes saoudiennes, puis a visé les sites de la Bourse d'Abou Dhabi et des Émirats. En retour, des propalestiniens ont piraté les sites de deux hôpitaux de Tel-Aviv et celui du quotidien *Haaretz*.

Un porte-parole du Hamas a rendu hommage aux hackers arabes et encouragé cette « *nouvelle forme de résistance arabe et islamique contre l'occupation israélienne* ». Les autorités israéliennes assurent qu'elles prennent très au sérieux cette campagne de piratage informatique, que le vice-ministre israélien des Affaires étrangères, Danny Ayalon, a qualifiée d'« *attaque terroriste* ».

« *Les récentes attaques menées contre les sites d'organismes israéliens du secteur privé relèvent plus du cyber-vandalisme que du cyber-terrorisme* », estime Yael Shahar, cyber-experte à l'Institut international du contre-terrorisme (ICT). De fait, les hackers arabes ne sont pas parvenus à détruire ou à détourner des informations sensibles. Ils se sont attaqués à des sites-vitrines, dépourvus de bases de données, saturant leurs serveurs pour en bloquer momentanément le fonctionnement.

« *Ces attaques par déni de service, menées par des individus dont l'origine géographique reste d'ailleurs à prouver, sont d'une grande banalité*, observe Gabriel Weimann, spécialiste de la terreur sur le Net, enseignant à l'université de Haïfa. *Elles ont eu pour le moment un impact très limité. Rien à voir avec la première offensive cybernétique de type étatique subie en 2007 par l'Estonie.* » Celle-ci avait fait "buguer" tous les services en ligne du pays.

Rien à voir non plus avec la mise au point d'un logiciel ou d'un ver espion de type Stuxnet, qui a notamment perturbé les installations nucléaires iraniennes en 2010, "empoisonnement" attribué au savoir-faire des services secrets israéliens. Pour l'heure, les dernières escarmouches des hackers arabes n'accréditent pas vraiment l'idée qu'Israël serait particulièrement vulnérable en matière de cyber-défense.

Une cyber-attaque massive contre la centrale de Hadera

Très vigilant, le gouvernement israélien a pourtant pris les choses en main. Début janvier, il a inauguré une cellule chargée de la sécurité informatique. Mais depuis des années, le pays a pris l'habitude de protéger contre cette menace ses sites militaires et ses infrastructures civiles considérées comme les plus critiques.

Pendant l'été 2011, Israël a ainsi testé un scénario de cyber-attaque massive sur sa centrale électrique de Hadera, installation stratégique qui fournit 40 % de l'énergie du pays. Les renseignements militaires israéliens ont aussi créé une nouvelle branche chargée de traiter des aspects offensifs et défensifs de la cyber-guerre. Le Shin Bet (sécurité intérieure) vient d'être chargé de protéger les instituts bancaires et les opérateurs de téléphonie mobile contre les attaques cybernétiques.

« *En définitive le "hacking" arabe est "une chance" pour la cyber-défense israélienne*, juge le consultant Dominique Bourra, fondateur de NanoJV. *Le pays va pouvoir se servir de ces incidents pour débloquer des crédits et muscler ses cyber-compétences, qui ne sont plus à démontrer.* »

De Jérusalem,
NATHALIE HAREL