Faut-il craindre une cyberguerre ?

Faut-il craindre une cyberguerre ?

Leurs PC sont leurs armes et leur guerre se mène en ligne. Après les attentats à Paris, des cyberattaques ont été menées contre des sites internet français, par des hackers affirmant agir au nom du groupe Etat islamique (EI). Dans le même temps, des « hacktivistes » se revendiquent d'Anonymous ont piraté des sites et comptes sur les réseaux sociaux des organisations islamistes et de leurs membres.

Mais c'est loin d'être terminé. Des comptes YouTube et Twitter appartenant au commandement militaire américain au Moyen-Orient (Centcom) ont également été visés, et une attaque d'envergure est annoncée pour jeudi 15 janvier. Sommes-nous à l'aube d'une cyberguerre ? Non, toujours pas, répond Gérôme Billois, expert en sécurité informatique au cabinet Solucom et administrateur du Club de la sécurité de l'information français (Clusif).

Francetv info : Peut-on parler de cyberguerre lorsque l'on évoque les attaques informatiques menées par des hackers qui se revendiquent du jihad ?
Gérôme Billois : Non, on n'y est pas du tout. Ce serait exagéré de parler de « guerre ». Aujourd'hui, nous parlons d'actes qui n'ont pas d'effets dans le monde réel. Il n'y a pas d'explosions, pas d'interruption de services essentiels comme l'énergie ou les transports. Il n'y a pas non plus de pertes humaines. On reste dans le monde virtuel.

Alors comment pourrait-on appeler cela ?
Il n'existe pas vraiment de mot pour déterminer ces actes. Après l'attaque contre la société Sony Pictures, qui a subi une destruction massive de son système d'information et le vol d'une importante quantité de données, Barack Obama parlé de cybervandalisme. Le terme semble assez juste. Ce qui se passe aujourd'hui, c'est comme si des activistes entraient dans des centaines de boutiques pour y coller leurs affiches et repartir. Les propriétaires de ces magasins n'avaient pas bien fermé la porte en partant et en revenant le lendemain matin, ils trouvent des affiches qui font la publicité de l'Etat islamique.

Pour vous, ces actions restent plutôt d'ordre symbolique ?
Extrêmement symbolique, puisqu'il s'agit d'une lutte entre deux idéologies. Avec d'un côté l'#opFrance (pour « Opération France », lancée par des cyberjihadistes), annoncée pour le 15 janvier, qui vise à ternir l'image de la France en attaquant un grand nombre de structures dans l'Hexagone, et de l'autre l'#opCharlieHebdo, qui vise à dénoncer et rendre indisponibles des sites jihadistes.

Qui se trouve derrière cette contre-attaque ? Certains revendiquent leur appartenance aux Anonymous…
On ne peut pas dire qu'il s'agit « des » Anonymous. Ce sont, en fait, des groupes très divers. Il faut d'ailleurs savoir que certains des groupes qui attaquent la France aujourd'hui ont pu participer à des opérations des Anonymous, ou s'en revendiquer. Il y a des acteurs en commun, qui œuvraient auparavant dans une même direction et se divisent aujourd'hui sur ce cas particulier. La logique de « l'hacktivisme » au sens large c'est : « Il se passe un événement, je me positionne par rapport à celui-ci et à chaque nouvel événement je redéfinis ma doctrine ».

Quelle est la force de frappe des cyberjihadistes aujourd'hui ?
Aujourd'hui, ils mènent des attaques de faible intensité. Sur une échelle de 1 à 10, ils atteignent 5, au maximum. Ces piratas utilisent des vulnérabilités connues depuis longtemps ainsi que des outils disponibles facilement sur internet. De plus, ils s'attaquent à des sites peu sécurisés et pas mis à jour. Il existe tout de même un risque à moyen terme. Ces groupes de pirates, petit à petit, vont apprendre, se développer, et augmenter ainsi leurs capacités d'attaque pour viser des services plus importants. On sait que l'EI dispose d'importants moyens financiers. Il n'aura, de toutes façons, pas de problème de matériel : avec un simple PC, vous pouvez lancer des attaques.

Qu'est-ce qui pourrait rendre ces groupes plus dangereux ?
Pour eux, il s'agit d'abord de gagner en expérience. Mais ils peuvent aussi acheter ce qu'on appelle des « vulnérabilités zero day », c'est-à-dire des connaissances sur une vulnérabilité qui n'est pas encore connue des éditeurs de sécurité. Quand vous possédez cet atout, vous pouvez attaquer un système, même s'il est mis à jour. Pour poursuivre l'analogie des boutiques vandalisées : imaginons que quelqu'un, comme un chercheur, découvre que pour la marque de serrure XYZ il existe un pass universel. Avec cette information, il peut faire deux choses : soit prévenir le fabricant de la serrure pour qu'il corrige son produit, soit vendre cette vulnérabilité à des criminels sur le marché noir.

Les pirates ont donc toujours un temps d'avance sur les systèmes de sécurité…
Oui et non. Une partie des pirates, les plus pointus, certains groupes de cybercriminels, peuvent aller jusqu'à dédier une partie de leurs moyens à faire de la recherche en attaques et trouver ces « vulnérabilités zero day ». Ces groupes-là, oui, peuvent avoir cette capacité. Il peut s'agir soit d'Etats un peu belligueux, soit de cybercriminels pointus. Mais il n'y en a pas des milliers. Dans le cas qui nous intéresse, les pirates n'ont pas cette avance. Ils utilisent simplement des failles connues, dont certaines ont été rendues publiques depuis 2012. Or, nous sommes en 2015 et les systèmes qu'ils attaquent n'ont pas été corrigés. On parle de petites mairies, d'universités, de PME… Ces structures-là n'ont pas forcément l'expertise ni les moyens pour maintenir leurs systèmes à jour.

D'autres structures, susceptibles de devenir des cibles plus importantes comme les grandes banques françaises par exemple, sont-elles mieux protégées ?
Oui, les systèmes sensibles sont mieux protégés. Les grandes sociétés ont les capacités nécessaires pour investir dans la sécurité. Les banques en ligne, par exemple, réalisent quotidiennement, voire plus encore, des tests de vulnérabilité automatisés, qui mènent les mêmes actions que les pirates. Les résultats de ces tests remontent aux services de sécurité informatique qui peuvent très rapidement effectuer les mises à jour nécessaires. Ce qui n'empêche qu'un site d'une grande banque est tombé, pendant une des attaques. Mais il s'agissait d'un site satellite sur lequel il n'y avait aucune transaction financière.

Là, nous parlons de sites internet. Qu'en est-il des systèmes informatiques internes ?
Ces systèmes-là disposent d'un niveau de sécurité, a priori, plus fort. Ne peuvent y rentrer que des employés ou des collaborateurs connus. Soit parce qu'il existe une protection physique : il faut entrer dans le bâtiment de la société. Soit parce qu'il y a des mots de passe ou des cartes à puce pour accéder à distance aux données. On n'est pas pour autant à l'abri d'une attaque visant le système d'information interne. C'est ce qui est arrivé chez Sony. Le FBI l'a dit : 90% des sociétés américaines seraient tombées si elles avaient été confrontées à la même méthode de piratage. C'est énorme.

Donc la menace existe…
Oui. La vraie question est de savoir si les jihadistes passeraient à ce type d'actions. Leur logique, pour l'instant, est plutôt de faire du bruit, de multiplier les cibles, de casser des milliers de sites, pour pouvoir dire mille fois qu'ils l'ont fait. Une attaque plus poussée, qui ferait plus de mal, aurait peut-être moins de résonance médiatique.

C'est tout de même une menace prise au sérieux, sur laquelle l'Otan se penche sérieusement. Est-ce à cause des menaces de ces jihadistes ?
Pas seulement. On distingue trois grandes « familles d'attaquants » : les « hacktivistes », qui attaquent par idéologie comme les cyberjihadistes, les cybercriminels, qui volent des données pour les monnayer, et enfin les Etats, qui développent des capacités défensives et offensives. Mais on peut craindre des regroupements entre ces groupes. Dans l'exemple de Sony, l'attaque est attribuée à la Corée du Nord, mais on sait qu'elle aurait été appuyée par des groupes d' »hacktivistes ».

Comment les Etats se préparent-ils face à cette menace ?
La cyberdéfense ne se résume pas à créer des murs en attendant que des pirates tentent de les casser. Cela inclut aussi des techniques de contre-attaque, pour pouvoir neutraliser les attaquants. Tous les Etats s'y préparent. Pour ce qui est de mener des attaques, on peut estimer que tous les pays industrialisés ont déjà des moyens et les renforcent au quotidien.

Concrètement, en quoi consiste la contre-attaque face à des cyberjihadistes ?
Les moyens de contre-attaque sont quasiment les mêmes que les moyens d'attaque. On peut imaginer attaquer leurs systèmes, les rendre inopérants, capturer les données pour bien comprendre qui ils sont. On peut aussi « boucher leurs tuyaux » pour éviter que les attaques ne passent.
Mais la difficulté, dans ce domaine, est de bien savoir qui se trouve en face de nous. Dans le cas Sony, on lit que l'attaque serait partie d'un hôtel en Thaïlande. A mon avis, elle est passée par là, mais ce n'est pas son point de départ. J'ai déjà vu des attaques menées contre certains de mes clients provenir de serveurs d'écoles maternelles au Vietnam. On se doute bien que ce n'est pas un écolier vietnamien qui l'a lancée, qu'il s'agit simplement de brouiller les pistes. Dans des scénarios plus vicieux, il peut s'agir de faire croire que l'attaque vient d'un endroit en particulier, pour provoquer une contre-attaque sur cette cible. Si l'on n'attribue pas l'attaque au bon responsable, on risque d'infliger des sanctions à un leurre.

Quand vous parlez de « boucher les tuyaux », s'agit-il d'attaques par déni de service, méthode qu'utilisent justement certains hackers ?
Cette méthode-là n'est efficace que temporairement, pour freiner une attaque. Mais les Etats ont la possibilité, à distance, de faire tomber les réseaux, de les couper, plutôt que de les boucher. Je parle bien des Etats, car les entreprises privées n'ont pas le droit de contre-attaquer. La légitime défense n'existe pas dans le cyberespace. En France, le seul cadre légal aujourd'hui, c'est la loi de programmation militaire, qui donne cette capacité à l'Agence nationale de sécurité des systèmes d'information (Anssi) ou, en tout cas, aux services rattachés au Premier ministre.

Manuel Valls va annoncer une série de mesures, dont certaines concernent internet. Où placer le curseur, entre la neutralité de net, le verrouillage pour empêcher les cyberjihadistes de nuire et la protection de la vie privée ?
C'est une question idéologique fondamentale, mais on n'y trouvera pas de réponse parfaite. Ce qui est certain, c'est qu'il y a une menace, qui, il faut le préciser, représente une très faible portion des usages d'internet. L'énorme majorité des usages sont très bénéfiques, pour l'économie, la culture, notre quotidien. Le plus important, selon moi, c'est le contrôle des moyens qu'on se donne. Il faut, certes, pouvoir être très réactif, car les attaques peuvent être menées très vite, mais il faut se contrôler pour éviter de tomber dans la surveillance généralisée. Ce contrôle peut être exercé par la justice ou des autorités indépendantes.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.francetvinfo.fr/monde/terrorisme-djihadistes/faut-il-craindre-une-cyberguerre_796909.html