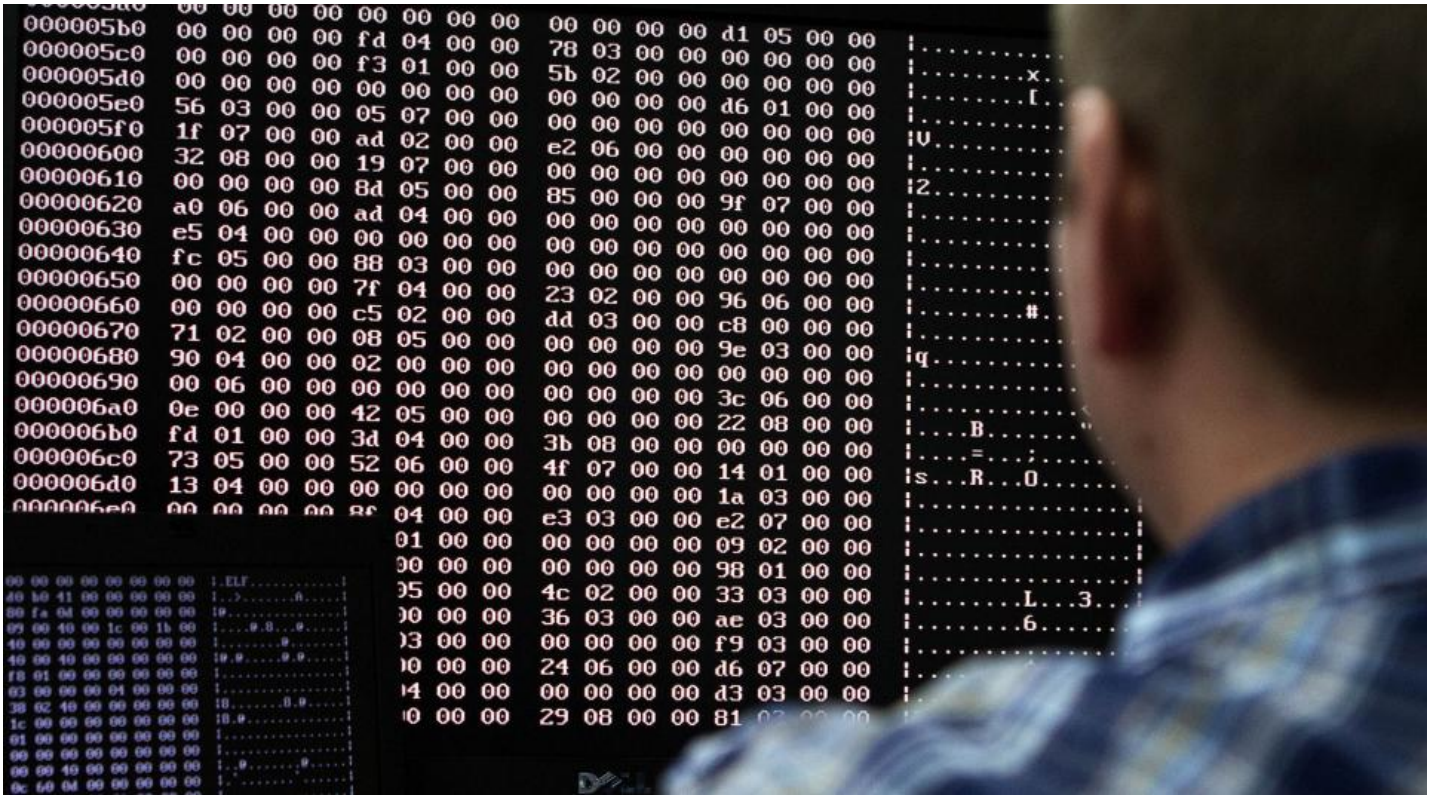
19 août 2016

Guerre 2.0

Cyber-ingérences russes dans la présidentielle américaine : mais au fait, qui est vraiment le pays le plus agressif (et efficace) en matière d'attaques informatiques ?



On parle beaucoup des hackers russes et de leur capacité de nuisance. Mais la récente accusation - après la fuite des documents du Parti démocrate américain - qui ciblait la Russie, ne doit pas faire oublier qui est réellement le leader de la cyberguerre aujourd'hui.

Avec François-Bernard Huyghe

Le Parti démocrate s'est dit victime d'une cyberattaque russe après que *Wikileaks* ait diffusé des informations lui appartenant. Pourquoi en arrive-t-on à ces conclusions aujourd'hui ?

François-Bernard Huyghe : Premièrement, ce qu'on a appelé cyberattaque contre le Parti démocrate a été revendiqué par *Wikileaks* et Julian Assange. C'est donc le fait d'une organisation non-alignée de hackers publiant des documents confidentiels. L'*intelligentsia* en a fait les louanges quand ils soutenaient les printemps arabes ou célébraient les bavures de l'administration Bush.

Deuxièmement, il s'agit d'une attaque certes, mais d'une attaque qui consistait à entrer dans des disques durs pour prendre des documents et les publier. C'est une opération qui consiste malgré tout à révéler la vérité ; c'est au fond tout le mal que ces gens ont fait ici.

Troisièmement, il y a cette question de **savoir pourquoi on relie cette affaire aux Russes.** Tout cela est très embrouillé. Apparemment, pour rentrer dans des détails techniques, on dit qu'il y aurait dans cette affaire une adresse IP qui mènerait vers la Russie. Et que le pirate, qui s'appelle Guccifer2.0, ne serait pas roumain comme il le prétend mais aurait une adresse IP sur le territoire russe.

En réfléchissant bien, si cette opération avait été menée par des professionnels du SVR (ex-KGB), auraient-ils eu la stupidité d'utiliser des ordinateurs russes en laissant une trace bien visible, alors qu'ils peuvent parfaitement utiliser des ordinateurs américains ou chinois dont ils auraient pris le contrôle ? De plus, **il est possible qu'il y ait des éléments russes, ou résidant sur le territoire**

russe, qui soient intervenus dans cette affaire. Pour autant, en quoi serait-ce un coup de Poutine ? Personnellement, je n'en sais rien. **Si les adresses IP étaient venues de France, aurait-on pointé la responsabilité de François Hollande ?**

Ce n'est pas la première fois que cela se produit :**les sociétés de sécurité américaines accusent presque systématiquement les Russes dès qu'il se passe quelque chose.** Il y avait eu, par exemple, un cas typique en août dernier lors d'une attaque du département d'État. On avait accusé systématiquement des pirates russes, comme on accusait systématiquement des pirates chinois à une certaine époque. Ce sont les *"usuals suspects"* qu'on ressort à tous les coups.

Cela dit, je ne suis pas un agent de Poutine ! Je pense que, de temps en temps, les services russes doivent faire des choses illégales. **Il y a plusieurs cas où des hackers russes sont intervenus pour mener des actions de sabotage, en symbiose avec le Kremlin, que ce soit contre l'Estonie il y a quelques années, ou encore contre la Géorgie.**

1. **Sabotage, espionnage : en quoi consistent principalement les actions de cyberguerre aujourd'hui ?**

Il y a trois options : on peut tout d'abord**voler des informations**, pour faire de l'espionnage industriel par exemple, ou encore pour les révéler comme c'est le cas de *Wikileaks*. Ensuite pour gêner sa victime, on peut**saboter un système**. Enfin, on peut modifier ou effacer un site, **faire une opération d'ordre psychologique.**

Les Russes sont-ils coupables ?

La culpabilité russe ne me paraît pas évidente ; en tout cas, elle n'est pas prouvée. Mais il faut bien savoir que cette affaire impliquant toutes ces informations qui ne sont pas officielles, émanant d'agences employées par le Parti démocrate, ressemble furieusement à **une opération de détournement de *data*.** Ce qui est gênant dans ce cas, ce n'est pas le moyen utilisé pour les obtenir, mais bien le contenu. Les données récupérées montrent plus ou moins que le Parti démocrate n'a pas été équitable et fonctionnait uniquement pour Hillary Clinton. Alors qu'il s'agisse des Russes, des Chinois ou d'autres qui soient derrière cette affaire et liés à Julian Assange, cela a peu d'importance. C'est comme s'il s'agissait d'une révélation dans le *Canard enchaîné* ou dans *Médiapart*.

N'est-ce pas ironique de voir ces critiques émerger des Etats-Unis, eux qui semblent être nettement plus impliqués dans la cyberguerre que toute autre nation ?

On est certain que**les Américains ont mené plusieurs cyberattaques, car eux l'ont plus ou moins avoué, contrairement aux Russes.** Le cas le plus célèbre est le sabotage du système d'enrichissement d'uranium en Iran, la fameuse affaire Stuxnet. Par ailleurs, on connait **la doctrine américaine, qui comporte l'usage d'armes informatiques offensives.**Et **si l'on regarde d'ailleurs d'où viennent la plupart des attaques internet, elles ont pour origine le plus souvent des adresses IP du territoire américain.** Ce qui ne veut pas dire que le coupable soit Barack Obama bien sûr. Mais dans ce domaine, il me semble que les Américains n'ont pas tout à fait le nez propre.

Quelles sont aujourd'hui les grandes nations en terme de cyberguerre ?

La principale est**la nation américaine.** En Chine, il y a aussi beaucoup d'attaques, dont la plupart visent d'ailleurs plutôt à pomper de la recherche et du développement, donc à servir l'espionnage industriel. La Russie est aussi une grande nation du Net, à la fois par ses services, mais aussi du fait d'un groupe assez flou de mercenaires-hackers russes, dont on ne sait pas réellement s'ils agissent avec l'accord du gouvernement. On leur attribue souvent beaucoup d'attaques.

Qu'est-ce qui pose problème dans la compréhension de ces conflits 2.0 ? Pourquoi est-ce que les États-Unis parlent d' ''agression'' dans l'affaire concernant le Parti démocrate ?

Le problème, c'est qu'on mélange souvent un roman de guerre, d'espionnage et de police. Pour parler d'acte d'agression, il faudrait qu'il y ait vol de connaissances précieuses. Mais à la fin, comme dans un Agatha Christie à la fin d'une enquête, on se demande qui a fait quoi, en ne disposant que de faibles indices, qui sont peut-être truqués ou qui ont été posés là pour qu'on les interprète d'une certaine façon. Un exemple me passe à l'esprit : quand il y a eu la fameuse attaque contre *TV5 Monde*, celle-ci avait été signée "cybercalifat". On a ensuite découvert que cela était passé par des relais russes. Ce qui, bien entendu, ne veut pas dire qu'il s'agit des Russes ou de Poutine. Enfin, on a considéré que les hackers venaient certainement de France. Vous pouvez constater qu'on reste dans l'hypothèse : on sait d'où vient l'IP, avec quels horaires de bureau cela peut coïncider à Moscou ou Pékin... mais tout pourrait être truqué.

Comment se positionne la France en matière de cyberdéfense ?

I**l faut vraiment distinguer l'espionnage, qui consiste à aller prendre des données soit pour ne pas payer les brevets, soit pour alimenter la presse d'informations occultées, de la vraie cyberattaque qui peut paralyser une banque, un média, des feux de circulation, etc.** Ce sont sur ces attaques-là que la France se concentre, pour éviter une vraie paralysie. Sur ce point, on est sujet et attentif à des attaques sur les fameux systèmes informationnels qui pourraient paralyser les hôpitaux, les banques ou autres.

Quels sont les risques aujourd'hui ? Sont-ils importants ?

Là encore, cela dépend des critères. Si on parle d'espionnage, on estime qu'en termes de propriété intellectuelle, il y a sûrement des milliards qui filent sur internet. On est dans ce cas aux limites de la délinquance. **Pour ce qui est des super-attaques, la plus grosse actuelle reste Stuxnet qui a réussi à retarder la nucléarisation de l'Iran**. De temps en temps, on apprend que des systèmes électriques ont été paralysés en Ukraine. Dans ces cas, on peut en effet soupçonner les Russes. Mais pour ce qui est des grosses attaques, qui priveraient un pays d'électricité ou d'eau, de banque ou d'administration, on ne les a encore jamais vues. Peut-être parce que c'est un fusil à un coup, et que celui qui appuiera le premier ne sait pas encore ce qu'il déclenchera. Il y a des milliers de gens - dont moi ! - qui vivent de cette crainte d'une grosse attaque. On fait alors des boucliers de plus en plus solides pour répondre à des capacités offensives de plus en plus fortes.

Propos recueillis par Camille Delmas