Le Point

# Cybersécurité : "Une faille reste toujours possible"

Titulaire de la chaire de cybersécurité de Saint-Cyr, Daniel Ventre revient sur l'attaque informatique subie par TV5Monde. Interview.

*Par* *Jean Guisnel*

*Modifié le 22/04/2015 à 06:41 - Publié le 22/04/2015 à 06:06 | Le Point.fr*


*i*

Ingénieur au CESDIP (Centre de recherches sociologiques sur le droit et les institutions pénales, CNRS), Daniel Ventre est également titulaire de la chaire de cyberdéfense et cybersécurité des écoles militaires de Saint-Cyr Coëtquidan. Après la cyberattaque contre TV5Monde, il pointe les vulnérabilités criantes que l'on retrouve dans de nombreuses entreprises. Entretien.

**Le Point.fr : Quelles sont vos premières réflexions après l'attaque subie par TV5Monde ?**

**Daniel Ventre :** Je m'interroge comme tout le monde sur l'identité réelle des pirates qui ont réalisé cette attaque. N'importe qui peut en effet signer "Cybercalifat", et c'est vraiment la première question à laquelle les autorités vont s'attacher à répondre : qui est véritablement derrière cette opération ? Sous la signature Cybercalifat, d'autres attaques se sont récemment produites, parfois présentées comme majeures même quand elles ne le sont pas vraiment (par exemple des piratages de comptes Twitter, des défigurations de sites internet). Pirater un compte Twitter, d'autres le font... Même si cela peut paraître déstabilisant, il n'y a là rien d'extraordinaire. Dans le cas présent, l'attaque prend de l'importance car elle est visible, médiatique, car il y a perturbation d'un média à large échelle.

**Ne faut-il pas répondre aussi à la question "comment ?" pour éviter que cela se reproduise ?**

Tout ce qui est connecté est vulnérable. On peut déployer d'importants systèmes de sécurité, mener des séries de tests, voire faire auditer les systèmes de protection par les autorités françaises comme cela l'a été fait pour TV5Monde : une faille reste toujours possible. Cette attaque semble être le fruit d'acteurs déterminés qui ont pris le temps de préparer leur opération.

**La ministre de la Culture Fleur Pellerin a parlé d'une attaque "terroriste". Ce terme est-il justifié à vos yeux ?**

On peut qualifier de "terroriste" toute action en lien avec une organisation terroriste. L'attaque étant revendiquée par des sympathisants ou membres de l'État islamique, on associe naturellement cette opération à un acte de terrorisme. Le discours sert la cause terroriste. Mais contrairement aux réactions et sentiments que suscitent des attentats terroristes meurtriers, comme ceux de ces derniers mois en France, cette cyberattaque, pas plus que toutes celles que l'on a connues jusqu'ici, n'a déclenché de sentiment de "terreur". Le Premier ministre a évoqué une "atteinte inacceptable à la liberté d'information et d'expression". Selon moi, il ne s'agit pas uniquement de cela. Les hackers ne cherchaient pas, me semble-t-il, à porter atteinte à la liberté d'expression. Ils voulaient simplement prendre le contrôle d'un média puissant assurant une large diffusion de leur message. L'attaque peut s'inscrire dans le cadre de la guerre de l'information que mène l'État islamique contre ses ennemis. Mais il se pourrait aussi que des hackers sans lien aucun avec la cause islamique aient juste utilisé cette bannière pour semer un peu de désordre. Seuls les résultats des enquêtes permettront de se faire une idée plus précise de la nature de cette attaque.

**On peut observer qu'à ce jour aucune cyberattaque contre des infrastructures critiques n'a été rendue publique - à l'exception de celles visant Areva - contre EDF, la SNCF ou des réseaux de distribution d'eau potable...**

De mémoire, il y a effectivement eu peu de médiatisation sur le sujet. L'attaque subie par l'Iran, dont les centrifugeuses nucléaires ont enduré des cyberattaques importantes révélées en 2012, reste le cas le plus médiatisé. Il y a d'autres cas recensés dans le monde, de cyberattaques contre des systèmes de distribution électrique, ou de transports. Mais tout dépend de ce que l'on entend par cyberattaque. Elles ne sont pas toutes de même importance. Prendre la main sur des panneaux d'affichage ou pirater des fichiers clients n'est sans doute pas à mettre au même niveau que les cyberattaques capables de perturber, paralyser, voire détruire des systèmes industriels. Même si on en parle peu, on peut cependant penser légitimement que des tentatives de ce type ont eu lieu.

**Si le gouvernement vous demandait conseil pour améliorer la sécurité informatique en France, que lui proposeriez-vous ?**

L'organisation actuelle, même si elle n'est pas optimale face à l'ampleur de la tâche, me paraît constituer un bon socle. Les efforts se concentrent sans doute trop sur la protection des grandes entreprises, des opérateurs d'infrastructures critiques. Les start-up, PME et TPME, qui sont souvent des partenaires contractuels de ces grands

groupes, des sous-traitants, ne disposent pas encore de la même attention. Or c'est par leur biais que des cyberattaques peuvent être menées pour toucher les grandes industries, voire l'administration de l'État.

La bonne démarche, c'est aussi la sensibilisation en amont, la prise de conscience, l'anticipation des problèmes, et comme le disent les experts de la cybersécurité, la mise en application de principes parfois très simples, comme éviter d'apposer ses mots de passe sur un post-it collé sur le bord d'un écran, éviter de partager ses identifiants, ne jamais changer de mots de passe, ou en choisir de trop simples. La cybersécurité est bien entendu plus complexe que cela, mais c'est déjà un très bon début. Cette sensibilisation, elle doit être faite à tous les niveaux, PME et grands groupes. Il est dit que 75 % des entreprises du CAC 40 auraient fait l'objet de cyberattaques ces dernières années. Il reste donc un important travail à faire pour que les chefs d'entreprise prennent leurs responsabilités dans ce domaine.

**Vous êtes titulaire de la chaire de cyberdéfense de l'école spéciale militaire de Saint-Cyr. Comment ces questions sont-elles abordées par les officiers ?**

Cette chaire ne s'adresse pas qu'aux seuls officiers mais à un public bien plus large. Rappelons qu'elle est essentiellement tournée vers des problématiques de sciences humaines et sociales, et n'aborde donc pas les choses d'un point de vue technologique. Nous abordons les questions soulevées par la cybersécurité et la cyberdéfense à travers la sociologie, le droit, l'anthropologie, les sciences politiques, les relations internationales, les études stratégiques. Nous nous intéressons à l'ensemble de l'écosystème de la cybersécurité, en analysant les pratiques des États, les enjeux de pouvoir, les questions économiques, etc.