Les inquiétantes failles de sécurité de nos grandes institutions face aux pirates informatiques

Le scandale des écoutes de la NSA a déjà mis en lumière le danger auxquels les institutions internationales et les Etats doivent faire face aujourd'hui : celui de ne plus pouvoir défendre leurs intérêts, principalement économiques. Changer la situation appelle à un changement total de paradigme vis-à-vis de l'information.

Avec Fabrice Epelboin

Atlantico : Récemment, la Banque centrale européenne a annoncé avoir été victime d'un vol de données et d'une demande de rançon. L'éditeur de logiciel anti-virus McAfee avait également révélé que depuis 2007, 72 gouvernements et organisations internationales avaient été espionnés par des hackers, dont l'ONU et le gouvernement américain. Nos institutions internationales sont-elles suffisamment protégées aujourd'hui ? En quoi ne le sont-elles pas ?

Fabrice Epelboin : Deux constats s'imposent. Tout d'abord, ces attaques existent depuis un bon bout de temps, il n'y a rien de neuf à l'horizon, en dehors de la communication de certains et de l'intérêt soudain de la presse grand public pour le sujet. Le tout est rendu plus visible, il est vrai, par la (bonne) habitude, de la part des victimes d'attaques, de signaler celles-ci, ce qui n'était pas toujours la norme dans le passé.

Ensuite, **il y a l'intérêt soudain des médias *mainstream* pour les "hackers",** un terme qui remplace peu à peu le mot fourre-tout de *"pirate"*. **Derrière ce terme - *hacker* - se cache une très vaste collection de profils divers et variés, allant de l'adolescent passionné d'informatique qui vit chez ses parents à une équipe de professionnels aguéris travaillant pour la NSA.** Tous ces gens là (et bien d'autres encore) tombent dans la catégorie des *"hackers"*. Cette catégorie est presque aussi floue que le terme d'*"informaticien"*, qui, encore aujourd'hui, désigne tout et n'importe quoi.

Cette remarque liminaire étant faite, venons en à votre question : nos institutions internationales sont-elles suffisamment protégées aujourd'hui ? A celà, on pourrait se demander contre quoi ? L'adolescent précité ? Oui, nous sommes suffisament protégés contre cela, enfin, la plupart du temps. La NSA ? L'affaire Snowden a montré que les renseignements américains étaient en mesure d'obtenir toutes les informations dont ils pouvaient avoir besoin au sein de toutes les institutions comme l'ONU, le Parlement européen, l'OMC, etc. , préparant ainsi de façon très efficace toutes les négociations internationales et faussant gravement le jeu de la diplomatie internationale. Donc, non, en aucun cas, **nos institutions internationales ne sont pas en mesure de se protéger aujourd'hui.** A titre d'anecdote, l'armée française s'est équipée l'année dernière en Microsoft, malgré les hurlements de bon nombre de spécialistes français, quelques mois à peine avant que des documents Snowden montrent que les services américains pouvaient, grace à cela, les surveiller.

Au mois de mars de cette année, l'Otan avait fait part d'une attaque informatique par déni de service, consistant en une saturation des connexions au site pour le mettre hors-service. Quelles sont les différentes sources de motivations des hackers ?

Là encore, il est important, à l'heure où la presse qui s'adresse au grand public se saisit de ce genre de sujet d'être clair sur le terme *"attaque"*. Un DDoS - une attaque par déni de service - est une attaque bénigne. Quand les *Anonymous* mettent en place de telles attaque, on considère que c'est l'équivalent, *online*, d'une manifestation. Aucun dégat ne résulte d'une *"attaque"* DDoS, juste un blocage d'un site web le temps de l'attaque, de la même façon qu'une avenue va être bloquée le temps d'une manifestation. Le terme *"attaque"* est quelque peu exagéré, tout du moins aux oreilles de non-spécialistes, qui l'assimilent à une aggression avec une intention de destruction ou de vol.

Les motivations pour effectuer une attaque DDoS sont multiples. Les *Anonymous* s'en servent généralement comme d'une façon de manifester leur mécontentement face à une institution ou une entreprise, en paralysant son site web durant quelques heures. **On peut aussi utiliser une attaque DDoS pour nuir à un concurrent - une pratique assez courante entre différents groupes de cybercriminels. Il est courant que des Etats utilisent de telles attaques pour paralyser des sites médias, afin d'éviter qu'une information ne sorte - les Russes sont des adeptes de ce genre de pratique**, même s'ils les sous-traitent, la plupart du temps à des groupes mélant hacktivisme nationaliste et cybercriminalité.

Une attaque DDoS peut également être le préliminaire d'une attaque plus complexe: cela a été le cas, par exemple, quand la société HBGary, un sous-traitant de l'armée et des renseignements américains, a subi une attaque DDoS - menée par *Anonymous* là encore - ce qui a permis ensuite, du fait d'une faille découverte à l'occasion, d'accéder à la messagerie de l'entreprise. L'ensemble des emails de l'entreprise ont, par la suite, été rendus public, révélant au monde une multitude d'informations, dont certaines était aussi croustillantes que certaines révélations de Snowden, comme l'opération CyberDawn de l'armée US.

Les motivations donc sont très variées, mais on peut les classer dans quatre catégories : des motivations d'ordre réputationel, quand un individu ou un groupe cherche à se faire un nom à travers une prouesse technique qui prend la forme d'une attaque; les motivations financières, la base de la cybercriminalité; les motivations politiques, une catégorie dans laquelle on va trouve aussi bien les *Anonymous*, que - surprise - la NSA, qui elle aussi réalise un nombre incroyable d'attaques informatiques dans le but de fournir des renseignements à l'Etat américain afin de lui conférer une supériorité politique sur ses alliés ou ses ennemis. Enfin, on a des motivation d'ordre militaire, qui concernent quasi-exclusivement les Etats, à des fin de renseignement ou à des fins offensives, comme quand les centrifugeuses iraniennes servant à enrichir de l'uranium ont été détruites par un virus informatique.

Si l'on devait imaginer, au regard des failles constatées plus haut, le pire scénario, quel serait-il ?

Le pire scénario serait sans conteste une attaque sur l'ensemble des infrastructures françaises par les Etats-Unis: autant dire que vous avez intérêt à avoir des bougies pour vous éclairer à la maison et une cheminée pour vous chauffer. Il n'est pas impossible que d'autres Etats soient en mesure d'infliger des dégats comparables, **mais pour ce qui est de simples *hackers*, même les plus doués, un scénario catastrophe est hautement improbable**. Même si la figure du cyber-terroriste a un brillant avenir médiatique devant elle, détronant le célèbre "pédonazi" qui va pouvoir prendre une retraite bien méritée, on reste là dans la communication, pour ne pas dire la propagande. Cela n'est guère qu'un *artefact* destiné à détourner l'attention.

Ceci dit, le scénario catastrophe que nous vivons actuellement est presque aussi alarmant qu'une cyberguerre avec les Etats-Unis. Nous savons aujourd'hui que nos institutions, nationales ou internationales, n'ont aucun secret pour les Etats-Unis, ce qui fausse totalement tout le jeu des négociations internationales, et notamment des négociations commerciales, c'est-à-dire la capacité d'entités telles que la France ou l'Europe de défendre leurs intérêts économiques. C'est une situation très grave, dont peu de personnes semblent saisir l'importance.

Le ministre de la Défense, Jean-Yves le Drian, a annoncé en janvier qu'un milliard d'euro sera débloqué pour améliorer la sécurité informatique. Ce genre de mesure fait-elle face à une obsolescence des systèmes déjà en place, ou essaye-t-on de prendre de l'avance sur les techniques des hackers ?

Là encore, méfions-nous du vocabulaire : les politiques sont friants de tours de passe-passe sémantiques. Ce terme de *"sécurité informatique"* ne veut pas dire grand chose dans ce contexte. Depuis la loi de programmation militaire votée en décembre dernier, et plus encore avec la future loi antiterroriste et son volet "cyber" qui ne devrait pas tarder à être votée, **nous avons instauré, en ligne, l'équivalent de la loi martiale.**

Si nous faisions une analogie avec le monde réel, nous somme passés d'un monde tel que nous le vivons aujourd'hui, avec quelques voitures de police qui parcourent la ville de temps à autre, parfois sirènes hurlantes, pour assurer notre *"sécurité"*, à un monde où, loi martiale aidant, nous aurions plusieurs chars d'assaut stationnés sur chaque place de Paris, et des véhicules blindés surmontés d'un mitrailleuse à chaque coin de rue, toujours, bien sûr, pour assurer notre *"sécurité"*.

Dans le *online*, nous nous dirigeons vers cela. Vous réalisez bien que si nous devions stationner un véhicule blindé léger à chaque coin de rue en France et des chars sur chaque place et devant chaque entrée d'autoroute, l'armée française aurait soudainement besoin d'acheter tout un tas de véhicules et devrait recruter pas mal de monde, toujours, cela va sans dire, pour assurer notre *"sécurité"*.

Le milliard évoqué par le ministre de la Défense, qui sera suivi de tout un tas d'autres milliards, va servir à cela.

"Nous" n'essayons pas du tout de *"prendre de l'avance sur les hackers", "nous"* cherchons à assoir une domination militaire dans un espace qui était jusqu'ici civil, l'Internet.

Un service de renseignement russe a d'ailleurs décidé de faire marche-arrière sur l'informatique en revenant à l'utilisation de machines à écrire. Pour autant, la "rematérialisation" des données est-elle la seule solution qu'il nous reste ? Qu'est ce que les entreprises publiques pourraient mettre en oeuvre pour vraiment limiter les risques ?

Le retour à la machine a écrire… J'ai franchement un gros doute sur cette information. Je ne peux m'empêcher de penser à une blague imaginée par le FSB dans le but de rire de sa reprise par la presse occidentale. Une simple analogie peut vous permettre de comprendre l'aspect comique : **si vous vouliez stocker sur du papier les informations que traite la NSA aujourd'hui, il vous faudrait un batiment dont la superficie serait proche de celle du continent africain.** Autre abération, **nous sommes dans un monde où l'information n'a de valeur que si elle circule.** Le papier n'est pas idéal. Franchement, il va me falloir des preuves en béton armé pour croire à une telle information.

Mais ceci étant dit, la question que vous soulevez est pertinente.**La seule voie réaliste pour se protéger est en effet la rematérialisation**, le retour au tout papier, synonyme, au mieux, d'un retour à la France des années 1950, la croissance en moins, et la dette en plus. Franchement, ce n'est pas vraiment une solution, mais c'est peut être bien la seule, ce qui constitue un paradoxe interessant, sur ce qu'il dit de notre époque.

Une solution durable serait plus à rechercher dans un changement de paradigme vis à vis de l'information, et ce n'est pas pour demain. On pourrait, par exemple, imposer la transparence par défaut, et réserver le secret à un nombre très limité d'informations, qui du fait de leur petit nombre, seraient ainsi bien plus faciles à sécuriser efficacement.

Prenons l'exemple concret de négociations internationales sur un sujet critique, le climat par exemple. Aujourd'hui, le processus consiste à ce que les parties prenantes - Etats, ONG, lobbies, etc, préparent de façon plus ou moins secrète ces négociations à travers une multitude d'échanges et de négociations préalables, de façon à ensuite négocier ensemble, bien souvent de façon plus ou moins secrète, ce qui aboutira à un accord international.

Un tel process est aujourd'hui biaisé, du fait de la capacité de renseignement et de surveillance de certaines de ces parties prenantes. Cela explique en grande partie le résultat de tels accords : Kyoto, ACTA, TAFTA… Tous ces accords internationaux sont parfaitement biaisés, tout comme le seront ceux qui vont suivre.

Maintenant, imaginons un monde dominé par l'idée de transparence. Toutes les étapes intermédiaires menant à un accord mondial sur un sujet affectant tous les habitants de la planète, seraient faites de façon parfaitement transparente, tout le monde pourrait assister aux moindres étapes, chez chacune des parties prenantes, voir même participer à certaines d'entre elle, et ce jusqu'à l'aboutissement d'un accord mondial régissant tel ou tel aspect de la marche du monde.

Techniquement, ceci n'est pas un problème majeur, c'est tout à fait faisable, Internet permet de faire cela. Politiquement, c'est une autre histoire, on est loin de pouvoir envisager de faire de la politique ainsi. **Nous sommes même incapables de gérer une simple municipalité de cette façon, alors des accords internationaux, vous pensez bien.**

Une telle façon de procéder résoudrait le problème de la confiance et de l'implication des citoyens dans la vie politique, amènerait - si c'est conçu pour cela - à une culture du consensus plutôt que de la confrontation, et serait, accessoirement, peu sensible à la surveillance.