SCADA, SALADES ET ESCALADES

LE 11 OCTOBRE 2010 ***PHILIPPE QUÉAU***

Quinze jours après les premiers signes d'agitation autour du virus Stuxnet, le soufflé n'est pas encore retombé. Face à l'emballement, Philippe Quéau freine des quatre fers.

On parle beaucoup dans les milieux *"informés"* du virus Stuxnet qui a récemment pris pour cible l'Iran, en s'attaquant aux infrastructures industrielles, et en paralysant des systèmes sensibles de contrôle et d'acquisition de données (Supervisory Control And Data Acquisition, ou SCADA). La centrale nucléaire de Bushehr, en Iran, en aurait été la principale victime ainsi que le centre de recherche Natanz.

Il est fort intéressant de lire les commentaires divergents et les diverses interprétations données à cette affaire. Les uns disent que c'est la première phase d'une cyber-guerre d'ampleur considérable qui vient d'être lancée par une ou plusieurs puissances, et que l'expertise développée pour l'élaboration des séries de virus qui s'abattent sur les systèmes iraniens ne peut être disponible que dans le cadre d'États armés pour ce faire. D'autres affirment qu'il ne s'agit que de ballons d'essais d'équipes d' "universitaires" qui testeraient de nouvelles méthodes virales. Certains affirment qu'il ne s'agit en fait que d'une campagne d'intoxication, destiné à booster le marché de la sécurité. Au total, la presse abonde en informations fort parcellaires et en désinformations plus ou moins farfelues.

Parmi les plus savoureuses, citons **celle rapportée par le *New York Times***, qui affirme (au premier degré, apparemment) que le virus contiendrait quelque part enfoui profondément dans son code le mot "myrtus", ce qui serait une allusion fort subtile au nom d'Esther, héroïne biblique, jadis engagée dans une guerre contre l'empire perse. En effet le nom originel d'Esther serait en fait Hadassah, qui veut dire "myrte" en hébreu. Pour ceux que cela intéresse on peut lire l'argument développé par de fort compétentes autorités universitaires **ici**.

Le site ReadWriteWeb, généralement bien informé, **relate l'attaque de Stuxnet** mais conclut d'une bien étrange manière:

> ***A l'heure où de nombreuses voix s'élèvent pour dénoncer les failles de sécurité que pourrait faire apparaître la mise en place d'un système généralisée de surveillance de la population française, SCADA pourrait être une façon radicale d'éteindre la machine afin de faire réaliser pleinement au gouvernement qu'il n'en possède pas les clés.***

Sic.

Les rédacteurs de ce site agitent ainsi la menace d'un déploiement ravageur de virus qui pourraient s'attaquer prochainement aux infrastructures françaises. Des hackers feraient ainsi part de leur opposition radicale à certaines évolutions récentes du droit français en matière de piratage par exemple. Ils *"puniraient"* le gouvernement par des actions de sabotage viral à grande échelle, dont les récentes attaques DDoS (Distributed Denial of Service) contre des sites comme celui d'Hadopi ne seraient qu'une modeste préfiguration.

La société civile en renfort?

Ici, deux remarques et une prédiction.

1. Le virus Stuxnet est très vraisemblablement le fait d'un ou plusieurs États. Ceux-ci sont facilement reconnaissables. Ils ont d'ailleurs annoncé haut et clair leur capacité offensive en matière de **cyberguerre**, et ont déployé une doctrine stratégique de prééminence absolue en matière de contrôle mondial du cyberespace. Dans cette hypothèse, Stuxnet n'aurait rien à voir avec des hackers, par exemple du genre anti-Hadopistes, et son degré de

sophistication dépasserait de plusieurs ordres de grandeur le niveau de nuisance de groupes de tels hackers civils aussi doués soient-ils.

2. Une attaque virale anti-SCADA en France aurait un effet si puissant sur l'opinion et sur le gouvernement que des mesures d'une grande férocité seraient immédiatement prises contre l'Internet de papa, tel que nous l'avons connu jusqu'à présent, avec son côté parfois libertaire. Et il serait difficile d'objecter aux très vigoureux tours de vis de la part d'un gouvernement ainsi provoqué. Résultat des courses: une attaque anti-SCADA de grande ampleur aurait pour premier résultat de légitimer la prise totale de contrôle d'Internet par les sécuritaires (largement secondés par les "ayants-droits", qui y verraient tout bénéfice).

La prédiction maintenant: une telle attaque (ou la simulation d'une telle attaque, à des fins de "provocation") est en effet ce qui pourrait arriver dans un proche avenir, dans des pays comme la France. Loi du talion? Tests en vraie grandeur de nouvelles cyber-puissances? Je ne sais. Mais on peut prédire qu'Internet n'a plus que quelques années à vivre sa relative liberté apparente.

Il faudrait que la société "civile" commence dès maintenant à en tirer toutes les conséquences d'un tel scénario. Peut-elle encore changer la donne?

Bien sûr! Là où il y a une volonté, on trouve un chemin, pour reprendre la formule.

Au cas où cette prédiction se révèlerait fondée, ce que je ne souhaite vraiment pas, c'est bien le tissu social même des soi-disant "sociétés de la connaissance" qui en sera affecté de façon irrémédiable.

Billet initialement paru sur Metaxu, le blog de Philippe Quéau

–

Crédits photo: Flickr CC ***The Official CTBTO Photostream***