**La surveillance de masse compromise ?**

**Alors que des lanceurs d'alertes comme Edward Snowden nous informent de la préoccupante situation de la surveillance systématique de tous les citoyens du monde, l'évolution technique rend accessible à tout un chacun des moyens simples pour y échapper.**

Le code de César était déjà utilisé au Ier siècle avant J.-C par l'armée romaine pour s'échanger des messages déterminants la réussite ou l’échec d'une campagne militaire.

Alan Turing cassant le code de la machine Enigma aurait réduit la durée de la Seconde Guerre mondiale de deux ans selon plusieurs historiens.

Connaître à l'avance tel ou tel mouvement tactique de l'ennemi anéanti en effet totalement les bénéfices de l'effet surprise.

Les techniques ont évoluées mais les enjeux restent les mêmes.

A présent les communications sont principalement électroniques mais la quasi totalités des messages transitant sur les réseaux ne sont pas réellement cryptés pour tout le monde. Ainsi la NSA peut en toute impunité se servir des backdoors soigneusement installées par ses soins dans les systèmes d'exploitations comme Windows, Mac OS, Android ou directement sur les adresses de messagerie comme celles de Google, Yahoo, Facebook...

Utiliser ces moyens de communication revient à envoyer tout son courrier avec des cartes postales :

[**http://www.frandroid.com/actualites-generales/287050\_nsa-chiffrement-communications-backdoor**](http://www.frandroid.com/actualites-generales/287050_nsa-chiffrement-communications-backdoor)

Naturellement l'envoi du courrier du monde entier avec des cartes postales n'est pas vraiment compatible avec la démocratie :

Les hommes politiques français ne donnent pas vraiment l'exemple puisque même au plus haut niveau de l'État on utilise des cartes postales pour le courrier :

[**http://www.liberation.fr/monde/2015/06/23/chirac-sarkozy-et-hollande-trois-presidents-sur-ecoute**](http://www.liberation.fr/monde/2015/06/23/chirac-sarkozy-et-hollande-trois-presidents-sur-ecoute_1335767)

Le jeu du chat et de la souris continue car en cryptographie il suffit d'avoir suffisamment d'astuce pour déjouer les ruses de son adversaire.

Le pied de nez récent fait par une équipe française à la surveillance mondiale orchestrée par la NSA permet en tout cas à présent de communiquer à l’abri des regards indiscrets pour ceux qui le souhaitent :

Dans le balbutiement de l'histoire qui ne se répète jamais mais donne une impression permanente de déjà vu, le comportement des mathématiciens est amusant.

Ils s’entêtent souvent à vouloir défendre les intérêts du faible contre le fort comme si cela venait perturber l'équilibre de leurs équations.

Et après avoir fait tant d'effort pour trouver la solution cryptographique, ils l'oublient dans un coin pour se consacrer à d'autres sujets plus intéressants.