



# Les cyberattaques sur Bercy, pourquoi pas une bonne nouvelle ?

**Les attaques qui ont visé Bercy peuvent constituer une formidable opportunité pour les responsables politiques, économiques et administratifs français de prendre enfin conscience du caractère éminemment stratégique de la cybersécurité.**

Les cyberattaques qui ont visé Bercy ne seraient-elles pas in fine une bonne nouvelle ?

L'information rendue publique le 7 mars 2011 par [l'Agence Nationale de la Sécurité des Systèmes d'Information \(ANSSI\)](#) selon laquelle une attaque informatique de grande ampleur - on parle de cent cinquante ordinateurs infectés -, a visé la Direction du Trésor au Ministère français de l'Economie, ne constitue-t-elle pas au final **une heureuse nouvelle** ?

C'est en effet une formidable opportunité pour les responsables politiques, économiques et administratifs français de prendre enfin conscience du caractère éminemment stratégique de la cybersécurité. D'une part, pour admettre que l'information représente un actif qu'il convient de protéger. Ce qui suppose, non seulement l'établissement de règles et procédure de sécurité. Mais surtout un respect de celles-ci par chacun, quel que soit son rang hiérarchique. Et que par exemple les usages individuels d'accessoires numériques à la mode mais non sécurisés, même s'ils participent au standing supposé de certains hauts fonctionnaires, ne doivent pas trouver leur place dans le circuit informatique gouvernemental.

Pour ce faire, il s'agit que les autorités en charge de la sécurité des systèmes d'information puissent imposer à tous – à l'instar de l'oukase prononcé par services étatsuniens à l'encontre du Président Barack H.Obama qui souhaitait conserver son smartphone personnel une fois arrivé à la Maison Blanche – ses principes de sûreté. **Il faut une doctrine de cybersécurité.** Et se doter ensuite des moyens de veiller à sa stricte application.

D'autre part, il conviendrait à l'occasion de cette opération d'espionnage informatique de réfléchir à notre dépendance numérique. Et à la capacité de notre pays à s'assurer d'une certaine souveraineté en la matière. En effet, dans une compétition économique de plus en plus violente, il être intéressant de constater l'implication grandissante des autorités étatiques auprès des fournisseurs de solutions technologiques.

Ainsi, lorsque le Département d'Etat a souhaité qu'Amazon cesse d'héberger les fichiers de WikiLeaks, il lui aura suffi – hors de toute procédure judiciaire formelle - d'un simple coup de téléphone pour obtenir satisfaction. Ce qui témoigne pour le moins de relations de proximité. Idem pour le service de paiement de Paypal, MasterCard ou Visa.

Autre illustration : la désignation début mars 2011 de [Paul Otellini](#), le directeur général d'Intel comme conseiller à la Maison Blanche. Ou lorsqu'en février 2010 la [National Security Agency](#) a négocié un accord avec Google dans la foulée des supposées attaques chinoises visant la firme de Mountain View. Sous d'autres horizons, on a constaté les subventions publiques massives attribuées par Pékin à ses deux champions nationaux, les équipementiers télécoms Huawei et ZTE.

Des coups de pouce tels qu'ils leur auraient permis de pratiquer des prix si bas qu'ils ont fini par mettre à genoux financièrement ses concurrents, notamment européens. La liste pourrait être prolongée de cette imbrication public-privé dans cette sphère high tech.

Puisse donc cette intrusion numérique visant les travaux préparatoires du G-20 servir de déclencheur utile dans les esprits des dirigeants gouvernementaux, pas toujours préoccupés jusqu'alors de la cybersécurité de terrain. Celle qui assure la protection continue de nos intérêts vitaux. Et participe donc à notre prospérité future.