Peut-on éteindre l'Internet ?

1. Contexte

Le thème de la *résilience* de l'Internet est très discuté en ce moment. La résilience est la capacité de l'Internet à continuer à fonctionner, même en présence de pannes ou d'attaques délibérées. Les pannes peuvent être dues à une défaillance matérielle mais aussi à une bogue logicielle. Les attaques peuvent être menées par par un petit groupe de vandales, de militants ou de criminels, mais elles peuvent aussi être dues à un État, qui va chercher à priver sa population de l'accès à l'Internet, ou bien à une partie de celui-ci.

L'Internet est-il fiable ? Résistera t-il à la prochaine panne ? Trois personnes dans un garage peuvent-elles stopper l'Internet ? Vue l'importance qu'a désormais l'Internet dans la vie de tous les jours, il s'agit de questions cruciales.

2. Analyse

Plusieurs pannes ou attaques spectaculaires ont défrayé la chronique en 2009-2010. Le traitement médiatique de ces pannes ou attaques a en général privilégié le sensationnel. La réalité est que ces pannes ou attaques ont eu des conséquences très limitées dans l'espace (un seul pays, ou bien un seul service Internet) ou dans le temps.

Il est très facile de *perturber l'Internet*, mais très difficile de faire une perturbation *mondiale* qui dure plus de quelques heures. Comme le dit Pierre Col, « L'Internet est globalement robuste et localement vulnérable ». Il est très facile de perturber l'Internet car celui-ci ne dispose pas de mécanismes de sécurité de niveau militaire : le but de l'Internet est de permettre la communication, y compris entre personnes qui ne se connaissent pas, cela implique donc un niveau d'ouverture qui le rend vulnérable. Mais il est très difficile d'arrêter l'Internet sur le long terme car l'Internet est vivant : les professionnels agissent, corrigent, remplacent, déploient de nouveaux systèmes et les perturbations ont toujours connu une fin rapide. Ainsi, la censure de WikiLeaks n'avait duré que peu de temps, montrant la capacité de réparation de l'Internet. Rigidifier les procédures, augmenter le niveau de contrôle aggraverait donc le problème au lieu de le résoudre, puisque cela empêcherait ces réactions intelligentes.

Néanmoins, la dépendance de plus en plus grande de notre société vis-à-vis du réseau, la sophistication grandissante des attaques, l'évolution des techniques, fait qu'il serait imprudent de se reposer sur ce constat. Un grand nombre d'efforts sont donc menés à tous les niveaux pour améliorer la résilience de l'Internet. Citons le déploiement de DNSSEC[1] en 2010, les efforts de l'ANSSI en France, pour rassembler les acteurs de l'Internet sur ce thème de la résilience, les travaux de l'IETF[2] pour, entre autres, sécuriser le *routage*, etc. Toutefois, il faut mesurer la difficulté de tels projets :

1 Permettant de vérifier l'authenticité des informations DNS
2 Principale organisation de normalisation de l'Internet

la valeur de l'Internet vient de son ouverture et déployer des systèmes de sécurité qui rendraient l'Internet lent et pénible à utiliser serait tuer le malade pour mettre fin à la maladie. D'autant plus que cette ouverture et cette absence de centralisation sont justement les forces de l'Internet, celles qui expliquent sa résilience.

Pour le cas particulier du DNS, les opérateurs de ce service sont occupés en permanence à récolter des données, à analyser les attaques, à détecter les vulnérabilités, et à partager l'information entre eux, au sein de l'OARC www.dns-oarc.net/. Le registre du *.fr*, l'AFNIC, a mis en œuvre de nombreuses techniques de résilience, fondées notamment sur la variété des logiciels pour ses serveurs de noms[3], sur le recours à plusieurs hébergeurs desdits serveurs… Il faut espérer que des mesures inappropriées de filtrage ne viendront pas fragiliser cet édifice : www.lepoint.fr/high-tech-internet/l-afnic-s-inquiete-pour-l-avenir-d-internet-14-02-2011-1295076_47.php

3. Pour aller plus loin

- Deux récits très vivants de coupure due à une panne matérielle :
www.zdnet.fr/blogs/infra-net/le-viticulteur-la-tractopelle-et-les-reseaux-39758040.htm

et www.mailarchive.com/frnog@frnog.org/msg13825.html.
Un autre exemple fut la coupure accidentelle de l'Égypte en 2008 : www.renesys.com/blog/2008/12/deja-vu-all-over-again-cables.shtml>. Mais les pannes matérielles n'ont qu'un impact très local, le vrai danger vient des éventuelles pannes logicielles qui, par manque de diversité, pourraient paralyser une grande partie de l'Internet.
- Un exemple d'une panne logicielle qui aurait pu avoir des conséquences sérieuses fut l'affaire de « l'attribut 99 » : www.bortzmeyer.org/bgp-attribut-99.html
- Coupure de l'Internet par l' l'Etat égyptien : http://www.bortzmeyer.org/egypte-coupure.html
Cela illustre le pouvoir d'un gouvernement, dans un pays où les connexions sont peu nombreuses. Cela serait-il possible en France ? Voir www.01net.com/www.01net.com/editorial/527741/couper-internet-en-france-possible-ou-pas/>.
-Technique du gouvernement libyen pour freiner et couper l'Internet :
www.lemonde.fr/technologies/article/2011/03/07/quatrieme-jour-de-coupure-d-internet-en libye_1489281_651865.html
- Analyse de cas : China Telecom en avril 2010 bgpmon.net/blog/?p=323. Article austère, bien loin de *Die Hard*. Un autre exemple basé sur le même cas de figure : www.foxnews.com/politics/2010/11/16/internet-traffic-reportedly-routed-chinese-servers/>.

À propos de l'AFNIC

(Association Française pour le Nommage Internet en Coopération)

Association à but non lucratif, l'AFNIC est l'organisme chargé de la gestion administrative et technique des noms de domaine *.fr* et *.re*, suffixes internet correspondant à la France et à l'Île de la Réunion. L'AFNIC est composée d'acteurs publics et privés : représentants des pouvoirs publics, utilisateurs et prestataires de services Internet (bureaux d'enregistrement). En savoir plus

3 BIND et NSD