Peut-on éteindre l'Internet ?

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 23 janvier 2011

http://www.bortzmeyer.org/eteindre-internet.html

Ce jeudi 27 janvier, l'Epitech organisait une intéressante conférence <http://www.programmez.com/actualites.php?id_actu=8868> sur le thème « Peut-on éteindre l'Internet ? ». Je n'ai malheureusement pas pu y aller alors je livre mes réflexions ici. (Jean-Michel Planche a fait un compte-rendu <http://www.jmp.net/2011/01/internet-la-reponse-est-non-mais-quelle-est-la-question/> de la conférence.)

Le sujet fait évidemment allusion à un certain nombre de cas connus : projet états-unien de doter le Président d'un gros bouton rouge pour éteindre l'Internet <http://news.techworld.com/security/3228198/obama-internet-kill-switch-plan-approved-by-us-senate-panel/>, pannes spectaculaires comme celle due à l'attribut 99 de BGP <http://www.bortzmeyer.org/bgp-attribut-99.html> ou celle du DNS chinois <http://www.bortzmeyer.org/panne-dns-chine.html>, « attaques accidentelles » comme celle de Pakistan Telecom contre YouTube <http://www.bortzmeyer.org/pakistan-pirate-youtube.html> ou celle de China Telecom <http://www.renesys.com/blog/2010/11/chinas-18-minute-mystery.shtml>, mesures liberticides prises par des États qui trouvent l'Internet trop libre (filtrage systématique, allant jusqu'au détournement du DNS <http://www.bortzmeyer.org/detournement-racine-pekin.html> en Chine, loi LOPPSI en France, etc), tentatives (assez ridicules, surtout en France) de faire taire WikiLeaks <http://www.bortzmeyer.org/a-propos-wikileaks.html>. Tous ces faits mènent à se poser des questions : si un excité du menton veut censurer Internet, est-ce possible ? Une attaque par les chinois rouges et communistes peut-elle nous priver de services indispensables à la vie humaine, comme Facebook ? La prochaine bogue dans IOS ou Windows va-t-elle stopper tout l'Internet ?

Il n'a pas manqué d'articles sensationnalistes sur ce thème. Selon eux, l'Internet serait tellement fragile que deux ou trois lycéens dans leur garage, a fortiori une organisation comme Al-Quaida, pourrait tout casser. Par exemple, lors de la bavure de China Telecom en avril 2010, on a vu apparaitre une quantité d'articles ridicules sur la soi-disant vulnérabilité de l'Internet (par exemple sur Fox News <http://www.foxnews.com/politics/2010/11/16/internet-traffic-reportedly-routed-chinese-servers/> ou Computer World <http://www.computerworld.com/s/article/9175081/A_Chinese_ISP_momentarily_hijacks_the_Internet_again_>). Ces articles sensationnalistes ont évidemment eu plus de succès que la froide technique <http://bgpmon.net/blog/?p=323>.

À l'opposé de ce discours apocalyptique « on va tous mourir », on voit des neuneus se présentant comme hackers qui prétendent que l'Internet est invulnérable, que les puissants de ce monde n'arriveront jamais à le censurer, et qu'on ne peut pas arrêter le libre flot de l'information.

Qu'en est-il vraiment ? Peut-on éteindre l'Internet ou pas ? Est-il très robuste ou très fragile ? Ces questions n'ont pas de réponse simple. Si on me presse pour fournir une réponse binaire, je dirais « On ne peut pas éteindre complètement l'Internet. Besson et Mitterrand rêvent, ils n'ont pas ce pouvoir. Et l'Internet, très résilient, résistera toujours aux pannes comme celle de l'attribut 99 <http://www.bortzmeyer.org/bgp-attribut-99.html>. ». Mais la vraie réponse mériterait d'être bien plus nuancée. Pour citer Pierre Col, « L'Internet est globalement robuste et localement vulnérable ».

Car tout dépend de l'objectif qu'on se fixe en disant « éteindre l'Internet ». Il est très difficile de couper l'Internet pendant une longue période. Mais des attaques réussies l'ont déjà sérieusement perturbé pendant plusieurs minutes, avant que les protocoles et les humains ne réagissent. L'Internet n'est pas invulnérable. Une des meilleures raisons pour lequelles la question « Peut-on éteindre l'Internet ? » n'a pas de réponse simple est qu'il est **très facile** de perturber l'Internet (BGP, par exemple, n'offre pratiquement pas de sécurité et il n'en aura pas de si tôt), mais **très difficile** de faire une perturbation qui dure plus de quelques heures (dans tous les cas existants, la réaction <http://www.bortzmeyer.org/securite-bgp-et-reaction-rapide.html> a pris bien moins de temps que cela).

De même, il est **très facile** de planter un service donné. Même pas besoin de pirates chinois pour cela. Une erreur de configuration, et un service fondamentalement stratégique est inaccessible <http://www.bortzmeyer.org/facebook-joue-bgp.html>. Pour beaucoup de simples utilisateurs, de ceux qui ne travaillent pas quotidiennement sur l'Internet, « Facebook est en panne » n'est pas très différent de « l'Internet est en panne ». Mais, pourtant, pendant de telles pannes, tout le reste de l'Internet fonctionne (et même mieux, les tuyaux étant moins encombrés). Si on peut comprendre que Jean-Kevin Michu ressente douloureusement l'arrêt de son service favori, les analystes qui prétendent produire un discours sérieux sur l'Internet devraient un peu raison garder et ne pas parler de « vulnérabilité de l'Internet » à chaque fois que Twitter a une panne.

Il est aussi **très facile** de rendre l'utilisation de l'Internet plus difficile. Tous les censeurs du monde ont appris que couper complètement l'accès était **irréaliste**. En revanche, le rendre difficile, imposer aux utilisateurs l'emploi de mesures de contournement complexes <http://www.bortzmeyer.org/proxy-http-server.html>, est possible. Cela ne découragera pas l'informaticien déterminé et compétent, mais cela peut gêner tellement l'utilisateur ordinaire qu'il renoncera à certains usages. C'est le pari d'organisations répressives comme l'Hadopi, qui sait très bien que les "*geeks*" continueront à télécharger quoi qu'il arrive, mais qui compte sur le fait que 95 % de la population ne les suivra pas. Et cela marche dans certains cas. Les censeurs ne sont hélas pas sans dents.

Enfin, on peut aussi noter qu'il est **très facile** d'éteindre l'Internet en un lieu donné. Chez moi, je peux couper l'accès à ma famille facilement. Dans un pays donné, on peut empêcher l'accès Internet. Cela se fait en Birmanie ou en Corée du Nord. En Tunisie, la mise en place du système de censure connu sous le nom d'« Ammar404 » avait été précédée d'une coupure complète de l'Internet pendant six mois, bloquant tous les usages légitimes. Il a fallu une révolution pour mettre fin au système de filtrage installé à cette occasion. Bref, si une coupure complète dans le monde entier est **très difficile**, un dictateur local a toujours des possibilités, comme l'a montré le cas de l'Égypte <http://www.bortzmeyer.org/egypte-coupure.html>. (À propos de l'Égypte : le lendemain de la coupure de l'Internet dans ce pays, un utilisateur de Google tape la recherche « Comment peut-on couper un pays entier d'Internet ? » qui l'amène sur cet article. Mitterrand et Hortefeux se renseignent ?)

Arrivé à ce point, certains lecteurs trouvent peut-être que je suis trop prudent et qu'il devrait être quand même possible de répondre en deux mots à une question aussi simple que « peut-on éteindre

l'Internet ? ». Mais, si la question est compliquée, c'est parce que l'Internet n'est pas un objet unique et localisé dans l'espace, qu'on peut détruire facilement. C'est plutôt une espèce vivante. Chaque individu est très vulnérable, on peut le tuer et, si on est suffisamment dénué de scrupules, on peut même en tuer beaucoup. Mais éradiquer l'espèce entière est plus difficile. La résistance de l'Internet aux pannes et aux attaques n'est pas celle d'un blockhaus passif, qu'on peut toujours faire sauter, avec suffisamment d'explosifs. C'est la résistance d'une espèce vivante, et intelligente (les professionnels qui font fonctionner l'Internet réagissent, corrigent, modifient, et rendent la tâche difficile pour les censeurs et les agresseurs, comme l'a montré la mobilisation autour de WikiLeaks). L'Internet peut être blessé mais le tuer nécessitera beaucoup d'efforts.

Une autre raison pour laquelle je ne donne pas de réponse ferme est que je ne suis pas trop intéressé par les débats pour observateurs passifs, regardant l'incendie en se demandant gravement s'il va être éteint ou pas. Je préfère travailler à améliorer la situation. Peut-on améliorer la résilience de l'Internet, sa résistance aux censeurs, aux pannes, et aux attaques diverses ? Et là, la réponse est claire : oui, on peut. On peut analyser les vulnérabilités, travailler à repérer les SPOF et à les supprimer, chercher les dépendances cachées qui risqueraient de faire s'écrouler un domino après l'autre, etc. Là, un travail est possible et nécessaire. Pendant que la loi LOPPSI impose un filtrage de l'Internet et donc diminue sa résistance aux pannes (le système de filtrage ralentit, perturbe et, d'une manière générale, ajoute un élément supplémentaire qui peut marcher de travers), d'autres efforts essaient de rendre l'Internet plus fiable. Par exemple, trop de liaisons physiques sont encore peu redondantes et une seule pelleteuse peut couper plusieurs câbles d'un coup <http://www.zdnet.fr/blogs/infra-net/le-viticulteur-la-tractopelle-et-les-reseaux-39758040.htm>.

Plus grave, trop de choses dans l'Internet dépendent d'un petit nombre de logiciels, ce qui fait qu'une bogue a des conséquences étendues. Trop de routeurs utilisent IOS et une seule bogue plante des routeurs <http://www.bortzmeyer.org/bgp-attribut-99.html> sur toute la planète. Comme dans un écosystème où il n'y a pas de variété génétique, un germe peut faire des ravages. Autre exemple, le système ultra-fermé de Skype n'a qu'un seul logiciel, le leur, et une seule bogue peut l'arrêter complètement <http://arstechnica.com/software/news/2010/12/skype-brought-down-by-double-whammy-of-overars>. Ce point illustre d'ailleurs l'illusion qu'il y aurait à essayer de rendre l'Internet plus robuste par des moyens matériels, comme plus de machines, ou logiciels, comme de passer le DNS en pair-à-pair <http://www.bortzmeyer.org/dns-p2p.html>. L'exemple de Skype, qui repose largement sur des techniques pair-à-pair, montre que ces techniques ne protègent en rien si une erreur dans le logiciel plante tous les pairs en même temps.

Il n'y a pas de solution magique au problème de la résilience de l'Internet. Mais il faut accroître sa diversité, qui permettra de faire face aux menaces du futur.

Des articles intéressants sur ce sujet :

- « Couper Internet en France ! possible ou pas ? <http://www.01net.com/www.01net.com/editorial/527741/couper-internet-en-france-possible-ou-pas/> », analyse à la lumière de la coupure égyptienne <http://www.bortzmeyer.org/egypte-coupure.html>.
- Suite à la coupure égyptienne, plusieurs articles ont découvert des techniques que les experts connaissaient bien et qui peuvent présenter davantage de résilience pour la communication, comme UUCP ou Fidonet. Voyez par exemple l'opinion « *"Internet is easy prey for governments"* <http://edition.cnn.com/2011/OPINION/02/05/rushkoff.egypt.internet/index.html> » qui fait l'éloge de Fidonet.
- « *"How Egypt did (and your government could) shut down the Internet"* <http://arstechnica.com/tech-policy/news/2011/01/how-egypt-or-how-your-government-could-shut-down-the-inars> » par Iljitsch van Beijnum.
- Une amusante et intéressante expérience de pensée sur la liste Nanog : Que se passe-t-il si un agent fédéral arrive chez vous et demande d'arrêter l'Internet ? <http://mailman.nanog.org/pipermail/nanog/2011-February/032325.html>.
- Le rapport sur la résilience de l'Internet en France <http://www.bortzmeyer.org/rapport-resilience-int

Enfin, j'ai écrit un article plus long sur cette question, pour la conférence SSTIC <http://www.bortzmeyer.org/sstic-eteindre-internet.html>.