Peut-on éteindre l'Internet ?

Stéphane Bortzmeyer

AFNIC
Immeuble International
78181 Saint-Quentin-en-Yvelines
France bortzmeyer@nic.fr

Résumé Depuis un ou deux ans, la question « Une extinction complète (ou quasi-complète) de l'Internet est-elle possible ? » revient souvent. Cette question est parfois posée pour le cas où un État souhaiterait priver d'Internet ses citoyens (cas du projet *Kill switch* aux États-Unis). Mais elle est aussi d'actualité pour le cas où un groupe de craqueurs souhaiterait arrêter l'Internet, dans le cadre d'un conflit plus classique, ou bien simplement pour s'amuser. Au vu de plusieurs cas concrets, certains se demandent même si une simple panne involontaire pourrait obtenir le même résultat.

Alors, l'Internet est-il réellement invulnérable à toute attaque, comme le veut la légende de sa résistance aux bombes nucléaires ? Ou bien est-il ultra-fragile ? Peut-il être éteint par une panne, par l'action d'une poignée de bricoleurs, ou par celle d'un État déterminé à le civiliser ? Qu'est-ce qui explique la résistance dont il a fait preuve jusqu'à présent ?

Et, s'il n'est pas invulnérable, qu'est-ce qui peut être fait pour améliorer sa résistance ? Des projets comme ceux de l'ENISA au niveau européen, ou de l'ANSSI [1] au niveau français sont-ils pertinents ?

Cet article a été écrit à l'occasion d'un exposé à la conférence SSTIC [2] à Rennes (France) en juin 2011.

1 Quelques perturbations fameuses

Voyons d'abord rapidement quelques « plantages » fameux, qui pourraient permettre de penser que l'Internet est très vulnérable.

Le 24 février 2008, la planète entière, saisie d'horreur, a été dans l'incapacité de se connecter à YouTube pendant deux heures [16] [4]. Deux heures pendant lesquelles il n'était pas possible de regarder des vidéos de LOLcats. L'opérateur Pakistan Telecom, voulant censurer YouTube (mal vu dans son pays) avait annoncé une route menant vers un trou noir. Plus par incompétence que par volonté délibérée de réaliser une coupure planétaire, Pakistan Telecom avait propagé cette annonce en BGP à son fournisseur de transit, PCCW. Celui-ci avait accepté cette annonce pourtant anormale et l'avait ensuite transmise. La

1. L'ANSSI a un groupe de travail, associant acteurs publics et privés, sur la question de la résilience de l'Internet. Il se nomme SCRIBE.
2. http://www.sstic.org/2011/

route 208.65.153.0/24, plus spécifique que celle issue de l'annonce normale de YouTube, avait ensuite été largement utilisée. Cet incident mettait en évidence la vulnérabilité de BGP : comme chaque opérateur fait confiance à tous les autres, une erreur d'un maladroit local peut perturber tout l'Internet.

Un cas analogue a été le résultat d'une fausse manœuvre de China Telecom en avril 2010. Cet opérateur avait annoncé en BGP des préfixes équivalent à environ 11 % de l'Internet [19]. Presque personne, à part les lecteurs du blog BGPmon, ne l'avait noté sur le moment, mais cette affaire avait connu un certain retentissement médiatique en novembre 2010 lorsque des lobbyistes états-uniens l'avaient fait mentionner dans un rapport officiel au Congrès.

Une autre panne fameuse fut celle de l'« attribut 99 » en août 2010 [7] [17]. Il s'agit d'un attribut des annonces BGP inconnu, et pour cause, puisque le but du RIPE-NCC était de tester la possibilité d'utiliser des nouveaux attributs BGP, par exemple pour les futures versions sécurisées de ce protocole. Pour un test, ce fut un test. L'annonce faite par le RIPE-NCC déclencha une bogue dans les routeurs Cisco utilisant le logiciel IOS XR, qui corrompit les annonces BGP. En recevant ces annonces corrompues, le routeur pair du Cisco fermait la session BGP. Le RIPE-NCC a rapidement détecté le problème et arrêté son annonce. Cet incident illustrait le fait que l'Internet dépend de logiciels, et que ces logiciels ont des bogues. Réformer BGP, ou le remplacer par un autre protocole ne résoudrait rien, sauf si on découvre un moyen de faire du logiciel sans bogues. On notera que la résilience de l'Internet peut rentrer en conflit avec d'autres demandes, par exemple celle d'avoir toujours plus de nouvelles fonctions rigolotes dans les routeurs, ce qui ne va pas dans le sens de la fiabilité du code, toujours plus complexe et mal testé.

Il y a aussi des pannes d'origine purement matérielle, l'archétypale « femme de ménage » lorsque la panne se produit dans les locaux, ou la non moins archétypale « pelleteuse » lorsque la coupure se fait dehors. Ce fut le cas le 12 mai 2011 lors de l'incident « Prosodie » (du nom du propriétaire du principal *data center* affecté) à Vélizy dans les Yvelines. Une seule pelleteuse a pu couper trois fibres optiques d'un coup, arrêtant plusieurs sites Web à forte visibilité et tous les abonnés à Free du département [10]. C'est un problème de même nature qui avait affecté l'Égypte en 2008 [22].

Et la coupure presque complète de l'Internet en Égypte en janvier 2011, pendant les manifestations contre la dictature ? Cette fois, contrairement aux cas précédents, la coupure était volontaire, le gouvernement ayant choisi de supprimer l'accès Internet du pays, pour empêcher son peuple d'accéder à l'information [12] [20]. Pour un gouvernement autoritaire, couper l'Internet ne nécessite que quelques coups de téléphone menaçants [2].

Très connues des professionnels de la sécurité, il y a bien sûr les attaques par déni de service (DoS) notamment celles par déni de service distribué (dDoS). Un exemple parmi de nombreux autres était l'attaque contre les serveurs DNS de la racine le 6 avril 2011 [8]. On n'a toujours pas de protection générale contre ces attaques. La réaction est difficile et nécessite la coordination étroite de plusieurs acteurs.

Figure 1. Les fibres arrachées à Vélizy (Photo de _GaLaK_)

À noter que tous ces problèmes (à part peut-être les problèmes de la racine du DNS en avril 2011) ont bénéficié d'une certaine couvertures dans les médias, mais qui n'était pas forcément proportionnelle à leur importance réelle. La bavure de China Telecom a ainsi été transformée en attaque majeure par une chaîne de télévision habituée au sensationnalisme [15]. Pourtant, les détournements BGP font partie du quotidien de l'Internet et ceux de Pakistan Telecom ou de China Telecom n'étaient, ni les premiers, ni les derniers.

2 Limites des perturbations

Toutes ces pannes ont en commun d'avoir été spectaculaires, très commentées... et d'avoir eu uniquement de faibles conséquences au niveau mondial. Pour paraphraser Abraham Lincoln, « On peut perturber un peu pendant longtemps, ou bien beaucoup pendant un temps très court, mais on ne peut pas éteindre tout l'Internet durablement. » Ou, pour citer Pierre Col, « L'Internet est globalement robuste et localement vulnérable. » Ces pannes peuvent donc être lues comme

la preuve de la vulnérabilité de l'Internet, ou au contraire comme la preuve de sa **résilience**, de sa capacité à fonctionner malgré les pannes et les attaques.

Ainsi, dans le *hijacking* de YouTube, la société victime elle-même a pu mitiger les effets du détournement en annonçant un préfixe légitime de la même taille, puis l'annonce pirate a été retirée. Si elle ne l'avait pas été, elle aurait vite été filtrée partout. Finalement, le problème n'aura duré que deux heures et affecté qu'un seul service.

Pour la bogue de l'attribut 99, les effets de cette annonce ont vite été détectés par l'émetteur, le RIPE-NCC, et celui-ci aurait immédiatement suspendu l'annonce [3], qui n'aura duré que trente minutes. Si l'émetteur avait été un méchant, refusant de retirer l'annonce, celle-ci aurait quand même rapidement été neutralisée par du *depeering* avec l'émetteur ou bien du filtrage en aval.

Dans le cas de la coupure de la fibre dans les Yvelines, la réparation a certes pris beaucoup de temps, mais elle a fini par avoir lieu : là encore, effets très limités dans l'espace et dans le temps. Si cette panne était très gênante pour les gens directement affectés, on n'en était pas moins très loin d'une « extinction de l'Internet ».

Dans le cas de la coupure de l'Internet en Égypte, le même gouvernement qui a décidé de la coupure a décidé de rétablir la liaison quelques jours après. C'est que la coupure n'affectait pas que les opposants mais elle gênait aussi toute l'activité économique du pays. Certaines sources estiment la perte aux alentours de cent millions de dollars états-uniens[14]. Cette coupure, comme celles plus récentes, par exemple en Syrie, ont suscité plusieurs initiatives de contournement, par exemple par ouverture de modems d'accès libre dans d'autres pays.

Enfin, le détournement effectué par China Telecom en 2010 n'aura duré que... dix-huit minutes [11] avant d'être corrigé. À noter qu'il n'existe aucun moyen de savoir si les données qui ont transité par la Chine ont été lues ou pas.

3 Ce qui fait la résilience

Pourquoi l'Internet ne s'est-il pas effondré malgré tous ces problèmes, ces bogues, ces attaques ? Parce qu'il est en fait plutôt résilient. Chaque composant de l'Internet est très vulnérable : les fibres optiques sont fragiles, les logiciels des grosses usines à gaz remplies de bogues, les humains qui les gèrent ne sont pas tous compétents et honnêtes, loin de là. Mais la combinaison de tous ces composants est très bien faite : les différentes parties de l'Internet sont très indépendantes. La chute d'une partie de l'Internet, relativement fréquente, n'entraîne pas le reste de l'édifice.

L'Internet est plutôt résistant aux pannes matérielles, comme l'a montré sa bonne tenue lors du grand tremblement de terre de la côte Pacifique du Tohoku en mars 2011. Mais le principal danger pour le futur n'est évidemment pas là, il est dans le risque d'un problème plus logiciel : une panne, ou une attaque délibérée, visant une bogue d'un logiciel ou une faiblesse d'un protocole. Un

3. Elle était prévue pour être de courte durée et a donc cessé avant que le problème ne soit compris.

exemple d'une telle attaque est décrite dans [18], où il s'agit de perturber ou de couper suffisamment de sessions BGP pour que, passé un certain seuil, le seul trafic de changements BGP dûs à ces perturbations plantent tous les routeurs. Bien que purement théorique, cette description peut inquiéter. Si un attaquant est suffisamment compétent et déterminé (l'attaque en question nécessite un bon botnet, et de longs travaux d'étude préalables), est-il possible d'arrêter tout l'Internet par un tel moyen ? Il n'y a pas encore de réponse ferme à ce problème.

Mais la modularité de l'Internet et son caractère distribué ne sont pas les seules explications à la résistance constatée jusqu'à présent : une autre raison de la résilience est que l'Internet n'est pas un bloc de béton, attaqué par des forces naturelles auxquelles il ne sait répondre que par la passivité. L'Internet est géré par des humains, qui observent ce qui se passe, comprennent et prennent rapidement des décisions pour réparer le problème. De même que les fibres optiques cassées par les mémés géorgiennes [9] sont réparées parce que des travailleurs sortent par n'importe quel temps pour aller les remettre en service [4], les problèmes logiciels sont surmontés par ce qu'une correction ou un contournement sont rapidement disponibles [5] et vite installés.

On peut donc, sans trop d'exagération, comparer la résilience de l'Internet à celle d'un être vivant : chaque cellule est très vulnérable, blesser l'animal est relativement facile (mais il guérit ensuite), le tuer nécessite un vrai effort, car l'animal ne va pas rester passif devant le danger, il va fuir ou combattre (ou les deux). La résilience de l'Internet doit donc être analysée sous cet aspect, plutôt que comme celle d'une machine passive.

4 Comment améliorer la résilience

Vous l'avez compris, je n'ai guère de sympathie pour les attitudes contemplatives du genre pronostic « L'Internet va-t-il connaître une panne majeure en 2012 ? » D'abord, on ne sait pas assez de choses sur les pannes logicielles pour pouvoir faire des prévisions sérieuses. Ensuite, plutôt que de se demander gravement si l'Internet va casser ou pas, il vaut mieux passer son temps et ses efforts à améliorer sa sécurité. L'expérience des pannes passées nous fournit plusieurs pistes de travail.

D'abord, le premier point est de veiller à la **variété génétique**. Il s'agit d'éviter qu'une seule bogue ne plante tout l'Internet (ou ne fournisse une porte d'entrée aux méchants). Ce point a été particulièrement mis en évidence par la panne « attribut 99 » qui n'affectait que Cisco IOS XR. Si ce logiciel avait été

4. Voir le témoignage d'un employé de Free sur la liste Frnog en `http://www.mail-archive.com/frnog@frnog.org/msg13565.html`.

5. Grâce à l'Internet, justement. C'est pour cela que couper l'accès Internet en cas d'attaque est souvent une mauvaise idée.

présent sur un plus grand nombre de routeurs [6], l'Internet aurait en effet pu être très perturbé.

Un autre exemple est fourni par les logiciels utilisés dans les serveurs DNS. Malheureusement, un grand nombre d'administrateurs système, sans réfléchir, installent BIND. Celui-ci a connu de nombreuses failles de sécurité permettant son arrêt à distance [7]. Si tous les serveurs DNS de l'Internet étaient des BIND, un petit nombre de paquets pourrait arrêter le DNS et donc quasiment arrêter l'Internet. Il est donc nécessaire, pour la résilience de l'Internet, que d'autres logiciels tels que NSD soient utilisés [8].

« Ne pas mettre tous ses œufs dans le même panier » est un conseil de bon sens et bien connu. Alors, pourquoi n'est-il pas davantage appliqué dans ce domaine de l'Internet (et de l'informatique en général) ? Pourquoi tant d'entreprises sont-elles fières d'être 100 % Microsoft ou 100 % Cisco, malgré la dépendance que cela entraine ? Parce que la résilience n'est pas le seul objectif. Le pauvre DSI doit aussi jongler avec d'autres critères, à commencer par le coût. Ainsi, pour un opérateur DNS, gérer un parc mixte (BIND & NSD) coûte clairement plus cher que d'uniformiser autour d'un seul logiciel. À une réunion de l'ENISA à Bruxelles en 2010, le représentant d'un gros opérateur français avait franchement mis les pieds dans le plat en déclarant que, puisque la résilience augmentait ses coûts, il n'en ferait que si « on » le payait pour cela. Par delà sa brutalité, cette déclaration illustre bien une certaine faiblesse des discours sur la résilience. C'est bien de dire que la résilience est importante, mais il faut en assumer les conséquences, y compris financières.

Ensuite, il est important d'**observer**. Trop souvent, une fois que cela marche, on arrête de regarder. Il est paradoxal que l'Internet soit à la fois une infrastructure critique très importante pour tant d'activités, et qu'il y ait si peu d'observations de son fonctionnement et de connaissances sur son état, au niveau global. Quant au niveau d'une entreprise ou organisation, on constate que peu d'administrateurs réseau utilisent des systèmes de veille comme ceux d'alarme BGP [6]. Il y a un gros potentiel d'amélioration ici.

Il y a bien sûr aussi des améliorations techniques possibles, comme celle qui est largement en cours avec le déploiement de DNSSEC, pour s'assurer de l'authenticité des réponses DNS, ou bien comme le futur (?) déploiement de « BGPsec », dont les premiers RFC, approuvés à l'IETF, devraient paraître cet été. Mais ce n'est pas par hasard que j'ai peu parlé de ces techniques ici. D'abord, ajouter du logiciel ne renforce pas forcément la résilience, tout nouveau

6. Vu les conséquences de la bogue, qui affectait le routeur suivant, il n'aurait même pas été nécessaire que ce logiciel équipe 100 % des routeurs pour casser une grande partie de l'Internet.

7. Deux d'entre elles, récentes, et particulièrement spectaculaires, étaient CVE-2009-0696 et CVE-2011-1910.

8. Les serveurs DNS de .FR sont actuellement un mélange de BIND 9 et de NSD, chez plusieurs hébergeurs différents. Dans le futur, des logiciels comme BIND 10 ou comme le futur Knot, actuellement en cours de développement, pourront être utilisés. Pour encourager le maintien d'une variété des logiciels serveurs, l'AFNIC est un des financiers des NLnet Labs, les développeurs de NSD.

logiciel apportant de nouvelles bogues. Ensuite, rien ne dit que ces techniques seront largement utilisées. L'expérience de l'usage de l'Internet montrent que des techniques de sécurité perçues comme lourdes, contraignantes et peu pratiques sont souvent écartées au profit d'une prise de risques calculée [9]. C'est ainsi que PGP est toujours resté limité à un usage de niche et que IPsec ne sert que pour des tunnels internes à l'organisation qui le déploie.

Du point de vue technique, une approche sans doute meilleure est architecturale : garder un Internet simple et ne pas multiplier les composants qui peuvent planter, ou autoriser une entrée non prévue. C'est ainsi qu'une approche de filtrage central obligatoire, comme en Chine ou en France avec la loi LOPPSI, indépendemment de ses aspects politiques, est une très mauvaise idée pour la résilience. La panne du point de filtrage central peut bloquer tout l'Internet d'un pays, et sa compromission par un attaquant peut avoir des conséquences nationales. Un tel point central est la négation de la nature distribuée de l'Internet, qui assure une bonne partie de sa résilience [21].

Enfin, un autre point important pour l'étude de la résilience de l'Internet est celui de la « résilience humaine ». On l'a vu, la résistance à une panne ou une attaque dépend souvent de la réaction intelligente des êtres humains. Réduire leur initiative, durcir les procédures par manque de confiance dans les cerveaux humains, rigidifier le processus de réaction, ne permettra pas de faire face aux menaces futures [3], qui sont difficiles à prévoir.

5 Conclusion

On l'a vu, éteindre l'Internet n'est pas si simple que ça. Il est très probable que ce n'est pas un objectif réaliste pour trois gusses dans un garage et que le fantasme du petit génie qui réussit à tout faire sauter depuis son iPad connecté en WiFi est voué à rester un sujet pour Hollywood [10]. Mais est-ce impossible d'éteindre l'Internet ? Rien n'est complètement impossible. Disons simplement que cela nécessiterait une action massive d'un état puissant et que cela ne serait pas discret.

Références

1. AFNIC : Peut-on éteindre l'Internet ? `http://lecercle.lesechos.fr/entreprises-marches/high-tech-medias/221134033/peut-on-eteindre-internet` (2011)
2. Bayart, B., Berbon, L. : « En Égypte, la coupure d'Internet prend quelques minutes ». `http://www.publicsenat.fr/lcp/politique/egypte-coupure-d-internet-prend-quelques-minutes-71386` (2011)
3. Bortzmeyer, S. : La sécurité de BGP et l'importance des réactions rapides. `http://www.bortzmeyer.org/securite-bgp-et-reaction-rapide.html` (2008)

9. Enfin, dont on espère qu'elle est calculée.
10. Si cela se produit quand même dans les prochaines années, je m'engage à twitter que je me suis grossièrement trompé ☺

4. Bortzmeyer, S. : Le Pakistan pirate YouTube. http://www.bortzmeyer.org/pakistan-pirate-youtube.html (2008)
5. Bortzmeyer, S. : La grande panne DNS de Chine de mai 2009. http://www.bortzmeyer.org/panne-dns-chine.html (2009)
6. Bortzmeyer, S. : Surveiller ses annonces BGP avec les systèmes d'alarme. http://www.bortzmeyer.org/alarmes-as.html (2009)
7. Bortzmeyer, S. : BGP et le désormais célèbre attribut 99. http://www.bortzmeyer.org/bgp-attribut-99.html (2010)
8. Bortzmeyer, S. : Allez, encore une attaque par déni de service contre la racine du DNS ? http://www.bortzmeyer.org/racine-6avril.html (2011)
9. Col, P. : SuperMamie coupe l'Internet en Arménie ! http://www.zdnet.fr/blogs/infra-net/supermamie-coupe-l-internet-en-armenie-39759777.htm (2011)
10. Col, P. : Une pelleteuse coupe le site web du ministère de la Défense... et beaucoup d'autres ! http://www.zdnet.fr/blogs/infra-net/une-pelleteuse-coupe-le-site-web-du-ministere-de-la-defense-et-beaucoup-d-autres-39760750.htm (2011)
11. Cowie, J. : China's 18-Minute Mystery. http://www.renesys.com/blog/2010/11/chinas-18-minute-mystery.shtml (2010)
12. Cowie, J. : Egypt Leaves the Internet. http://www.renesys.com/blog/2011/01/egypt-leaves-the-internet.shtml (2011)
13. ENISA : The Internet Interconnection 'ecosystem' - new report identifies top risks for resilient interconnection of IT networks . http://www.enisa.europa.eu/media/press-releases/the-internet-interconnection-2018ecosystem2019-new-report-identifies-top-risks-for-resilient-inte (2011)
14. Hopkins, C. : The Cost of Egypt's Internet Blackout : $110 Million+. http://www.readwriteweb.com/archives/the_cost_of_egypts_internet_blackout_110_million.php (2011)
15. Miller, J.R. : Internet Traffic from U.S. Government Websites Was Redirected Via Chinese Networks. http://www.foxnews.com/politics/2010/11/16/internet-traffic-reportedly-routed-chinese-servers/ (2010)
16. RIPE-NCC : YouTube Hijacking : A RIPE NCC RIS case study. http://www.ripe.net/internet-coordination/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study (2008)
17. Romijn, E. : RIPE NCC and Duke University BGP Experiment. https://labs.ripe.net/Members/erik/ripe-ncc-and-duke-university-bgp-experiment/ (2010)
18. Schuchard, M., Mohaisen, A., Vasserman, E.Y., Kune, D.F., Hopper, N., Kim, Y. : Losing Control of the Internet : Using the Data Plane to Attack the Control Plane. http://www-users.cs.umn.edu/~mohaisen/doc/lci-ccs10-abs.pdf (2011)
19. Tonk, A. : Chinese BGP hijack, putting things into perspective. http://bgpmon.net/blog/?p=323 (2010)
20. Tonk, A. : Internet in Egypt offline. http://bgpmon.net/blog/?p=450 (2011)
21. Weill, M., Poncet, G. : L'Afnic s'inquiète pour l'avenir d'Internet. http://www.lepoint.fr/high-tech-internet/l-afnic-s-inquiete-pour-l-avenir-d-internet-14-02-2011-1295076_47.php (2011)

22. Zmijewski, E. : Mediterranean Cable Break. http://www.renesys.com/blog/2008/01/mediterranean_cable_break.shtml (2008)