Peut-on éteindre l'Internet ?

Stéphane Bortzmeyer
AFNIC
bortzmeyer@nic.fr

SSTIC, Rennes, 9 juin 2011

Nous allons tous mourir !

Tous les jours, une annonce catastrophiste : « Il n'est plus exagéré de considérer possible de mettre un État à genoux sans tirer un coup de feu » (Michael Rake, président de British Telecom)

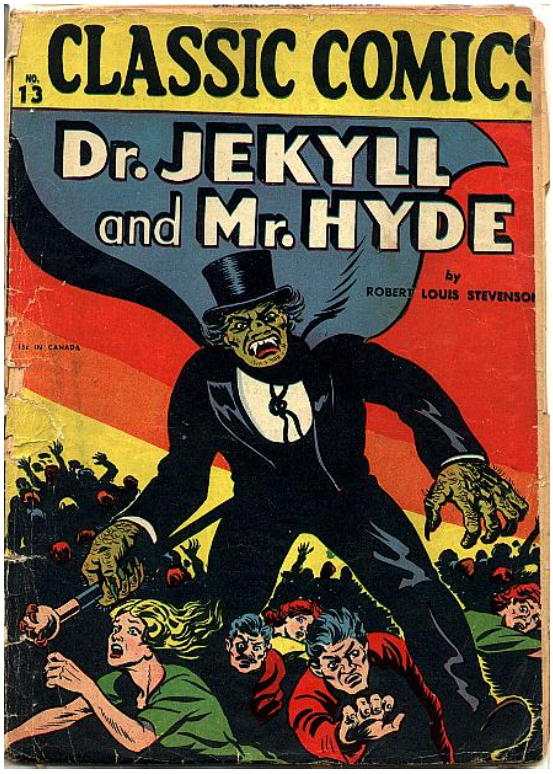
1. Trois russes dans un garage stoppent tout l'Internet,
2. Deux lycéens iraniens font sauter une centrale nucléaire à distance, via l'Internet,
3. Une bogue dans Cisco IOS et toute la civilisation occidentale (Twitter, YouTube et Facebook) stoppe,
4. L'armée chinoise arrête les réseaux puis les parachutistes débarquent,

Posons le problème

Peut-on arrêter l'Internet ?

Si oui, qui et comment ?

Expérience de pensée



Supposons que nous soyons un groupe de Génies du Mal, et que nous voulions stopper l'Internet. . .

. . . Tout va dépendre de notre budget (les Génies du Mal sont

Premier essai

(Photo de _GaLaK_)

Couper les câbles, détruire les *data centers*

Dans certains pays, peu de liens internationaux. Couper est facile. Arrêter AMS-IX et le Linx va certainement perturber l'Internet européen

Deuxième essai

Trouver une vulnérabilité zéro-jour, par exemple dans le code d'IOS

Il faudrait en fait plusieurs vulnérabilités pour tout couvrir. Propager l'attaque impose de ne pas couper l'Internet (syndrôme d'Ebola : tuer le porteur n'est pas une bonne stratégie pour le virus).

Cela dépend aussi de la rapidité des analystes et des patcheurs. Si la faille est dans un protocole, et pas un logiciel, le Génie du Mal aura un avantage.

Troisième essai

Une classique dDoS

Attention, on veut planter tout l'Internet, pas juste france.fr. Viser un point central ? Si Facebook s'arrête, l'Internet est en panne. Ou bien la racine du DNS ?

Le problème est que les objectifs les plus intéressants sont aussi les mieux défendus (racine du DNS). Et si l'attaque dure plus d'une heure, des tas de mesures de défense seront prises. Le Génie du Mal peut toutefois compter sur les difficultés de coordination.

Quatrième essai

(Photo de _R. D. Ward_)

Et si je suis déjà Président à Vie d'un pays civilisé ?

C'est plus facile : quelques coups de téléphone de menace et tout

Autres idées bienvenues...

Être Génie du Mal est amusant mais frustrant : il est facile de semer le désordre localement, bien plus dur d'éteindre réellement l'Internet.

Et les perturbations ne durent pas assez longtemps pour faire beaucoup de Mal.

Changement de perspective

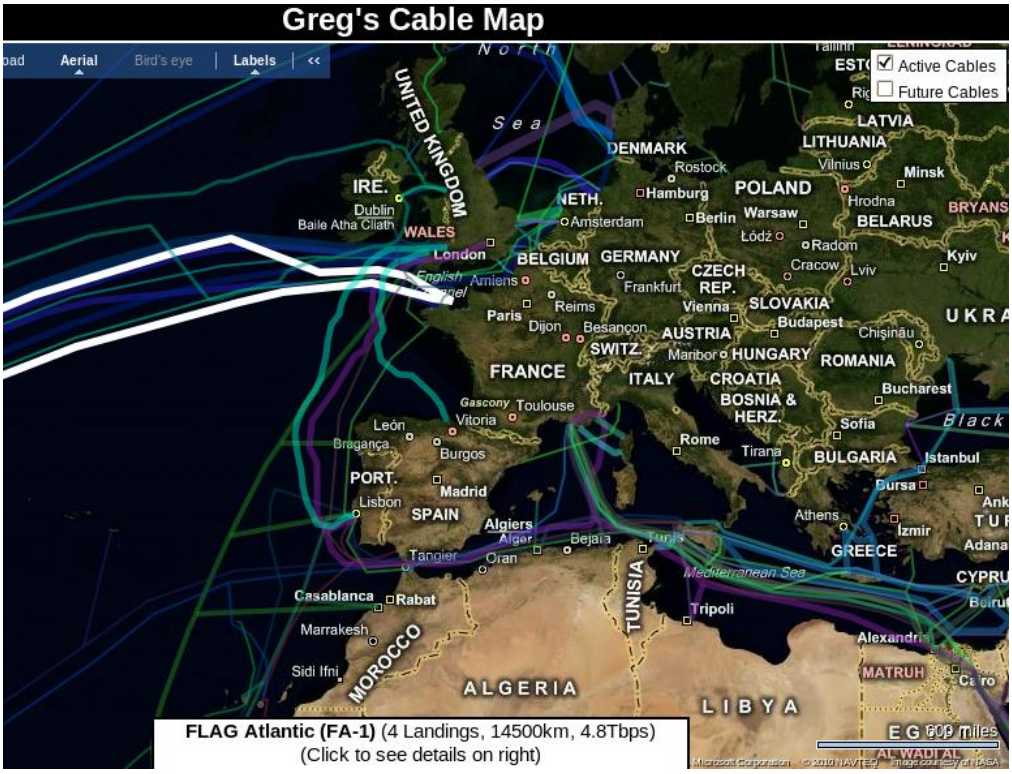
Au lieu d'être Génie du Mal, je suis gentil.

Comment puis-je améliorer la résilience de l'Internet ?

D'abord, les mauvaises idées

1. Refaire l'Internet en partant de zéro. Les vulnérabilités de l'Internet sont celles de tous les systèmes complexes. Le nouveau réseau aura les mêmes problèmes.
2. Civiliser le réseau avec plus de centralisation, plus de monopoles, plus de contrôles, plus de procédures, . . . Cela lui enlèverait justement ce qui fait sa résilience.

Redondance physique



`http://www.cablemap.info/`)

1. Éviter les SPOF,
2. Attention aux SPOF cachés (plusieurs *data centers* mais tous

Écrire des logiciels sans bogues

1. Plus facile à dire qu'à faire,
2. Meilleurs langages, programmeurs plus qualifiés, moins de course aux fonctions,
3. Examen croisé du code source : accès au source indispensable.

Coordination des acteurs

1. Certainement une des plus grosses faiblesses de l'Internet aujourd'hui,
2. Lu sur NANOG : ≪ Quelqu'un sait comment joindre un être humain du niveau 2 chez [gros opérateur] ? ≫
3. En France, pas de canaux officiels de communication entre, par exemple, l'AFNIC et les gérants de serveurs récursifs (heureusement qu'il y a Twitter). Travaux de coordination actuellement en cours.

Politique

1. Les actions qui peuvent censurer ou couper l'Internet viennent souvent du gouvernement officiel,
2. Il n'y a donc pas que les ingénieurs qui ont du travail, les citoyens aussi.