La nécessaire ré-organisation de l'Internet autour d'un meilleur contrôle politique

Stéphane Bortzmeyer
AFNIC
bortzmeyer@nic.fr

La nécessaire ré-organisation de l'Internet autour d'un meilleur contrôle politique

Stéphane Bortzmeyer
AFNIC
bortzmeyer@nic.fr

afnic

Le contexte

Le contexte

- « un terrorisme en accès libre sur Internet » (B. Cazeneuve, 2014)

Le contexte

- « un terrorisme en accès libre sur Internet » (B. Cazeneuve, 2014)
- « une question centrale, celle de l'Internet civilisé » (N. Sarkozy, 2011)

Le contexte

- « un terrorisme en accès libre sur Internet » (B. Cazeneuve, 2014)
- « une question centrale, celle de l'Internet civilisé » (N. Sarkozy, 2011)
- « il ne peut pas y avoir de zone de non-droit dans l'espace numérique » (M. Valls, 2015)

Le contexte

- « un terrorisme en accès libre sur Internet » (B. Cazeneuve, 2014)
- « une question centrale, celle de l'Internet civilisé » (N. Sarkozy, 2011)
- « il ne peut pas y avoir de zone de non-droit dans l'espace numérique » (M. Valls, 2015)
- « Internet, la loi du Far West » « [la nécessité du] contrôle du cœur de la toile qu'est le système d'exploitation » (M. Boutih, 2015)

afnic

Le contexte

- « un terrorisme en accès libre sur Internet » (B. Cazeneuve, 2014)
- « une question centrale, celle de l'Internet civilisé » (N. Sarkozy, 2011)
- « il ne peut pas y avoir de zone de non-droit dans l'espace numérique » (M. Valls, 2015)
- « Internet, la loi du Far West » « [la nécessité du] contrôle du cœur de la toile qu'est le système d'exploitation » (M. Boutih, 2015)

Bref, il faut (r)établir la loi française sur l'Internet.

afnic

Le débat

1. Une partie politique :

Le débat

1. Une partie politique :
    1. Est-ce qu'on est d'accord avec les principes affichés (par exemple l'interdiction des discours racistes, ou bien du partage de la culture) ?

Le débat

1. Une partie politique :
    1. Est-ce qu'on est d'accord avec les principes affichés (par exemple l'interdiction des discours racistes, ou bien du partage de la culture) ?
    2. Si oui, est-ce une bonne idée de faire respecter ces principes par l'infrastructure, plutôt que par la punition des coupables ?

afnic

Le débat

1. Une partie politique :
   1. Est-ce qu'on est d'accord avec les principes affichés (par exemple l'interdiction des discours racistes, ou bien du partage de la culture) ?
   2. Si oui, est-ce une bonne idée de faire respecter ces principes par l'infrastructure, plutôt que par la punition des coupables ?
2. Une partie technique, qui a été largement absente des débats : quelles sont les conséquences pour l'Internet ?

afnic

Les mesures dirigées vers l'infrastructure

Les mesures dirigées vers l'infrastructure

- ARJEL (décret n° 2011-2122 du 30 décembre 2011),

Les mesures dirigées vers l'infrastructure

- ARJEL (décret n° 2011-2122 du 30 décembre 2011),
- LCEN+terrorisme (décret n° 2015-125 du 5 février 2015 et la Main Rouge...),

Les mesures dirigées vers l'infrastructure

- ARJEL (décret n° 2011-2122 du 30 décembre 2011),
- LCEN+terrorisme (décret n° 2015-125 du 5 février 2015 et la Main Rouge...),
- et bien sûr décisions judiciaires.

Exemple du DNS

Il y a plusieurs obligations légales qui mentionnent le DNS : ARJEL, la Main Rouge, jugements ThePirateBay ou AlloStreaming. . .

afnic

Exemple du DNS

Il y a plusieurs obligations légales qui mentionnent le DNS : ARJEL, la Main Rouge, jugements ThePirateBay ou AlloStreaming. . .

Au passage, excellente lecture, le rapport du Conseil Scientifique de l'AFNIC « Conséquences du filtrage Internet par le DNS »
`https://www.afnic.fr/fr/l-afnic-en-bref/actualites/actualites-generales/6573/show/le-conseil-scientifique-de-l-afnic-partage-sur-le-filtrage.html`

La censure via le DNS marche ?

La censure via le DNS marche ?

1. Décisions judiciaires servies à seulement certains FAI,

La censure via le DNS marche ?

1. Décisions judiciaires servies à seulement certains FAI,
2. Cyberrebelles utilisant un résolveur local,

La censure via le DNS marche ?

1. Décisions judiciaires servies à seulement certains FAI,
2. Cyberrebelles utilisant un résolveur local,
3. Américanophiles utilisant Google Public DNS ou Cisco Open DNS (excellent pour la souveraineté numérique !)

afnic

Mesure par les sondes Atlas en France

```
Measurement \#2420872 for thepiratebay.se/A uses 500 probes
[141.101.118.194 141.101.118.195] : 239 occurrences
[ERROR: NXDOMAIN] : 21 occurrences
[146.112.61.106] : 2 occurrences
[ERROR: SERVFAIL] : 31 occurrences
[127.0.0.1] : 184 occurrences
Test done at 2015-09-16T07:43:43Z
```

La première réponse est l'authentique.

afnic

Autre mesure avec les Atlas

```
Measurement \#2420874 for alloshare.com/A uses 500 probes
[52.0.7.30] : 384 occurrences
[ERROR: NXDOMAIN] : 35 occurrences
[127.0.0.1] : 58 occurrences
Test done at 2015-09-16T07:49:56Z
```

Décision plus ancienne, certains ont gardé le nom dans leur config, d'autres l'ont supprimé.

afnic

Pour que la censure via le DNS marche

Pour que la censure via le DNS marche

1. Il faudrait bloquer le port 53 en sortie, et/ou faire du DPI comme en Chine,

Pour que la censure via le DNS marche

1. Il faudrait bloquer le port 53 en sortie, et/ou faire du DPI comme en Chine,
2. Les gens feront alors des tunnels (déjà mis en œuvre dans Unbound, sur le port 443),

afnic

Pour que la censure via le DNS marche

1. Il faudrait bloquer le port 53 en sortie, et/ou faire du DPI comme en Chine,
2. Les gens feront alors des tunnels (déjà mis en œuvre dans Unbound, sur le port 443),
3. Sans compter les projets du groupe de travail IETF DPRIVE (chiffrement du DNS).

afnic

Passage à l'échelle

Passage à l'échelle

- Réflechissez deux secondes si on vous demande quelque chose d'aussi simple que de filtrer le port 53 en sortie sur votre réseau.

afnic

Passage à l'échelle

- Réflechissez deux secondes si on vous demande quelque chose d'aussi simple que de filtrer le port 53 en sortie sur votre réseau.
  - Dans les routeurs de sortie ? Il faudra qu'ils soient rapides.

afnic

Passage à l'échelle

- Réflechissez deux secondes si on vous demande quelque chose d'aussi simple que de filtrer le port 53 en sortie sur votre réseau.
  - Dans les routeurs de sortie ? Il faudra qu'ils soient rapides.
  - Des boîtiers spécialisés (forcément en coupure donc critiques) ? Encoe du matos états-unien ou chinois en plus ?

afnic

Passage à l'échelle

- Réflechissez deux secondes si on vous demande quelque chose d'aussi simple que de filtrer le port 53 en sortie sur votre réseau.
  - Dans les routeurs de sortie ? Il faudra qu'ils soient rapides.
  - Des boîtiers spécialisés (forcément en coupure donc critiques) ? Encoe du matos états-unien ou chinois en plus ?
  - Dans les boxes ? Il faudra alors interdire les connexions avec d'autres CPE.

afnic

Passage à l'échelle

- Réflechissez deux secondes si on vous demande quelque chose d'aussi simple que de filtrer le port 53 en sortie sur votre réseau.
  - Dans les routeurs de sortie ? Il faudra qu'ils soient rapides.
  - Des boîtiers spécialisés (forcément en coupure donc critiques) ? Encoe du matos états-unien ou chinois en plus ?
  - Dans les boxes ? Il faudra alors interdire les connexions avec d'autres CPE.
- Tout est possible, mais a des conséquences (coût, fragilité).

afnic

Routage / IP

Il y a plusieurs façons de mettre en œuvre la censure au niveau routage ou IP (couche 3) :

1. Filtrage IP en sortie

Routage / IP

Il y a plusieurs façons de mettre en œuvre la censure au niveau routage ou IP (couche 3) :

1. Filtrage IP en sortie
2. Injection de fausses routes (cas turc contre Google Public DNS, cf. exposé à FRnog 22)

Routage / IP

Il y a plusieurs façons de mettre en œuvre la censure au niveau routage ou IP (couche 3) :

1. Filtrage IP en sortie
2. Injection de fausses routes (cas turc contre Google Public DNS, cf. exposé à FRnog 22)

Pas encore fait en France ?

afnic

Et ça marche ?

1. VPN

Et ça marche ?

1. VPN
2. Tor

Et ça marche ?

1. VPN
2. Tor

Interdire les VPN et Tor ?

Et les attaques actives ?

Exemple en Chine :

```
% dig @123.123.123.123 A www.france-ix.net
  ...
;; connection timed out; no servers could be reached

% dig @123.123.123.123 A www.facebook.com
  ...
;; ANSWER SECTION:
www.facebook.com. 2620 IN A 46.82.174.68
```

Et les attaques actives ?

Exemple en Chine :

```
% dig @123.123.123.123 A www.france-ix.net
  ...
;; connection timed out; no servers could be reached

% dig @123.123.123.123 A www.facebook.com
  ...
;; ANSWER SECTION:
www.facebook.com. 2620 IN A 46.82.174.68
```

Cette machine 123.123.123.123 n'existe pas. C'est le réseau qui répond (l'adresse IP est un mensonge).

Mais ça marche en Chine

Mais ça marche en Chine

- Oui, car le réseau a été entièrement architecturé pour le contrôle.

Mais ça marche en Chine

- Oui, car le réseau a été entièrement architecturé pour le contrôle.
- Quelles sont les priorités, contrôle ou résilience ? (« Rapport de l'observatoire de la résilience de l'Internet en France » `https://www.afnic.fr/fr/l-afnic-en-bref/actualites/actualites-generales/8302/show/l-observatoire-de-la-resilience-de-l-internet-publie-s` `html`)

Conclusion

Conclusion

- On ne fait pas d'omelette sans casser d'œufs.

Conclusion

- On ne fait pas d'omelette sans casser d'œufs.
- Censurer n'est pas seulement une question politique : cela nécessite un changement sérieux de l'infrastructure d'Internet.

afnic

Conclusion

- On ne fait pas d'omelette sans casser d'œufs.
- Censurer n'est pas seulement une question politique : cela nécessite un changement sérieux de l'infrastructure d'Internet.
- Ce changement va le rendre plus compliqué, plus fragile et favoriser les GAFA.

afnic

Merci !

www.afnic.fr
contact@afnic.fr