

L'ABC du filtrage d'internet.

Filter internet, c'est simple et l'espionner tout autant. Il suffit de le vouloir. On raconte ici comment un gouvernement décidé peut, assez simplement, réaliser cela. Il s'agit d'une présentation, pas d'un tutoriel.

L'accès à internet est depuis longtemps filtré quand le réseau est utilisé par les enfants. A la maison, avec les logiciels de contrôle parental ; à l'école avec les logiciels installés sur des ordinateurs-relais dans les écoles et les académies. Dans les deux cas, il s'agit de protéger les jeunes internautes des contenus qui leur sont préjudiciables. Le filtrage est réalisé à l'initiative des parents et des professeurs.

Plus nouveau, l'accès internet devrait prochainement également être filtré, quand celui ci est utilisé par des grandes personnes/majeurs/adultes responsables. Le but n'est plus réellement de protéger les internautes, mais plutôt semble t'il de promouvoir de grandes et belles idées telles que, par exemple, « la moralité » « la création » ou « la civilisation ».

Cette 'kindergarten-isation' d'internet a déjà commencé dans des pays (autrefois) démocratiques tels que l'Australie, la Suède et, sur une base 'volontaire,' au Royaume Uni. Elle s'apprête à connaître un nouveau développement en France avec « la montée en puissance de la Hadopi » (dixit la ministre). Voilà une bonne occasion pour se poser la question : comment ~~papa et maman~~ nos gouvernements vont ils s'y prendre pour filtrer internet ?
(les sources et liens sont à la fin)

I : un pays imaginaire

- a) : les personnages
- b) : les différence entre internet et le téléphone

II : Quoi filtrer ?

- a) les sites web / les DNS
- b) les pages web / les url
- c) les adresses i.p.
- d) le peer to peer / les paquets

III : Où filtrer ?

- a) chez les F.A.I.
- b) chez l'autorité / le filtrage espionnage par un proxy
- c) chez l'habitant / sur les postes clients

IV : Les modes de filtrage retenus

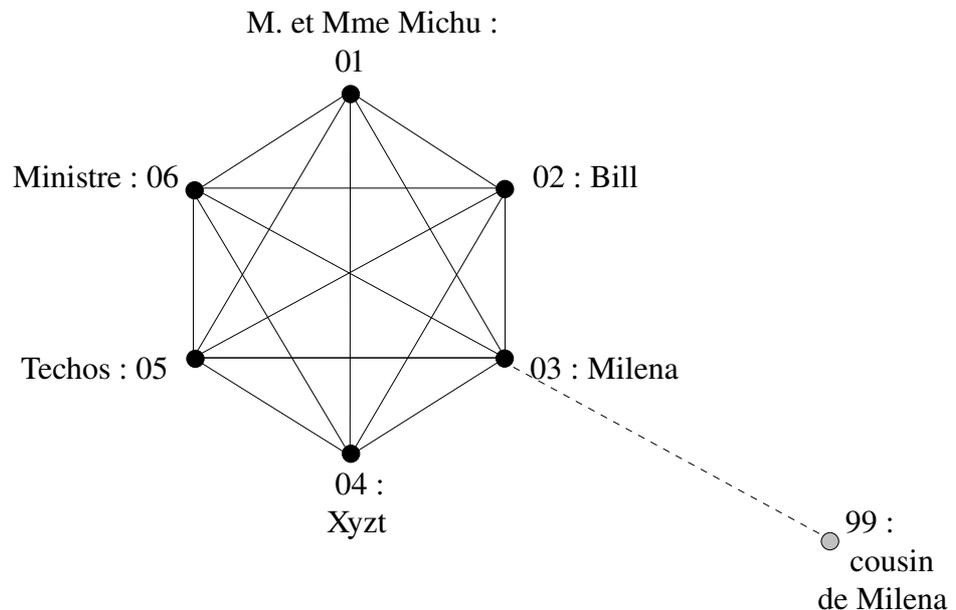
- a) un double filtrage par DNS et par i.p.
- b) un double filtrage chez l'autorité et chez l'habitant.

Conclusion : d'internet à hiérarchie.net

sources / liens

I : Un pays imaginaire.

On imagine un réseau qui ne relie que 6 personnes. Sur ce réseau – au début en tout cas – chacun est égal. Chacune des 6 personnes connectées dispose d'une adresse i.p. et d'un site personnel / d'un nom de domaine. Son site est installé directement sur son ordinateur personnel (elle s'auto-héberge). Le réseau est un « réseau de pairs » et il a donc la forme d'une étoile dans un hexagone – une représentation empruntée à Williamson (1975). (fig.1)



a) les personnages

Monsieur et Madame Michu.

adresse i.p. 01 ; nom de domaine : chezmichu.net

Monsieur et Madame Michu sont d'honnêtes citoyens qui n'ont jamais eu la curiosité de soulever le capot de leur box et qui sont donc respectables.

Bill.

adresse i.p. 02 ; nom de domaine : chez bill.com

Bill est un gars astucieux qui bricole divers business dans son garage, généralement légaux.

Milena.

adresse i.p. 03 ; nom de domaine : chezmilena.net

Milena est une travailleuse immigrée qui vient d'un pays étranger et aux moeurs politiques troubles. Elle dispose d'une connexion avec un de ses cousins au pays.

Xyzt.

adresse i.p. 04 ; nom de domaine : pas de nom de domaine

Xyzt représente l'élément antisocial du réseau, celui qu'il convient de filtrer, espionner, taxer, emprisonner ... D'ailleurs, il y a fort à parier qu'Xyzt n'est qu'un pseudo.

Techos.

adresse i.p. 05 ; nom de domaine : techos.net

Techos est l'informaticien qui fournit la bande passante au réseau et qui va 'router' (faire passer) les messages qui y circulent. Techos fait tout ce qu'on lui demande, tant qu'il est payé.

Ministre de l'Internet.

adresse i.p. 06 ; nom de domaine : mininternet.gouv

Le Ministre de l'Internet est le ministre chargé par l'autorité suprême de nettoyer le réseau des pirates et autres indésirables. Son titre exact est « Ministre de la bienséance, de l'optimisme et du patriotisme économique sur internet »

b) les différences entre internet et le téléphone

Le réseau internet ressemble beaucoup au réseau téléphonique. Il y a cependant 2 différences importantes.

- les noms de domaine :

imaginons que le numéro de téléphone de monsieur et madame Michu soit le 01.02.03.04.05. Pour appeler les Michu, il faut composer ce numéro sur le clavier. Si on tape « m-o-n-s-i-e-u-r-e-t-m-a-d-a-m-e-m-i-c-h-u » sur le clavier d'un téléphone, on ne parviendra jamais à les joindre (sauf si on a mis leur nom en mémoire sur son propre téléphone).

Sur internet « ça marche ». Si on tape « 01 » sur la barre d'adresse du navigateur, on tombe sur le site des Michu. Et si on tape, comme tout le monde : « www.chezmichu.net », on tombe aussi chez les Michu..

La table de correspondance qui transforme les noms en numéros peut être stockée dans la mémoire de chaque ordinateur dans un fichier qui s'appelle 'HOSTS'. Aujourd'hui, ces tables sont stockées dans des ordinateurs qui ne servent qu'à cela : les serveurs DNS. La plupart sont la propriété des fournisseurs d'accès à internet.

On va supposer ici que le serveur DNS n'est autre que l'ordinateur de Techos.

- le routage.

Pour appeler les Michu en composant le 01.02.03.04.05, on ne passe pas par une autre ligne. Les plus anciens d'entre nous se rappellent encore qu'il fallait demander à la demoiselle du téléphone de raccorder notre ligne à la ligne des Michu pour pouvoir leur parler.

Sur internet, c'est différent. Tous les ordinateurs connectés en même temps (les 'hosts') peuvent se parler. Par exemple, si Milena veut se connecter au site des Michu, sa communication ne prendra pas forcément la 'route' (ligne) directe. Si, un jour, une météorite écrase la ligne qui relie l'ordinateur de Milena et celui des Michu, Techos peut 'router' les messages qu'ils s'envoient en passant, par exemple, par l'ordinateur de Bill.

II : Quoi filtrer ?

a) les sites web : le filtrage DNS

« Normalement », quand on veut accéder au site de Bill ou envoyer un e.mail à Bill, on tape « chezbill.com » et le serveur DNS de Techos 'traduit' « chezbill.com » par « 02 », ce qui permet d'afficher la page d'accueil de Bill.

Maintenant imaginons que Bill affiche quelque chose qui ne plait pas au ministre (par exemple, il fait de la publicité pour de l'alcool sur son site alors qu'il n'est pas producteur). Le ministre va demander à Techos de traduire 'chezbill.com' par '05' (l'adresse i.p. de techos). Désormais, tous ceux qui tapent « chezbill.com » tombent sur la page d'accueil de Techos. Le ministre peut alors demander à Techos d'afficher sur son site « le site de Bill est inaccessible », « accès interdit », « erreur », etc.

b) les pages web : le filtrage par url.

Bill est un effronté. Il va diviser son site en 2 pages web. Chacune de ces pages aura un nom (= une url) différent.

Par exemple Bill va créer la page : « www.chezbill.com/matos », pour son business ordinaire, et la

page « www.chezbill.com/whiskey » pour le côté 'bar' de son affaire. Il va ensuite se plaindre que le filtrage de son site ruine son commerce légal : « www.chezbill.com/matos ».

Si le ministre est faible et/ou si Bill est influent, le ministre va demander à Techos d'interdire l'accès à la page « www.chezbill.com/wiskey » et d'autoriser l'accès à la page « www.chezbill.com/matos ». Mais il y a un problème par ce que les deux pages correspondent à la même adresse i.p. , l'adresse i.p. de Bill, le 02.

Il va donc falloir procéder à un « filtrage hybride » en 2 temps.

1) diriger tous les appels au 02 (« www.chezbill.com », « www.chezbill.com/matos » et « www.chezbill.com/wiskey », vers un ordinateur spécial dit 'plate forme de filtrage'.

2) regarder sur cette plate forme quelles pages ont été demandées (si c'est possible) et rediriger ceux qui avaient tapé « www.chezbill.com/wiskey », vers le 05.

Le filtrage par url est coûteux, ou alors il demande beaucoup de personnel ; il est donc réservé aux pays riches et aux dictatures densément peuplées.

c) le filtrage des adresses i.p.

Tous les sites internet n'ont pas de nom. Par exemple, celui de Xyzt. Xyzt n'a pas voulu donner son nom et son adresse, donc il n'a pas pu acheter de nom de domaine. Pour accéder à la page web de Xyzt, on tape simplement son adresse i.p. , le 04.

Mais c'est là que le filtrage est le plus simple. Il suffit au Ministre de demander à Techos de ne pas 'router' (permettre l'envoi) les appels au 04, et Xyzt est inaccessible. Sauf mesure secondaire, cela revient à couper l'accès à internet d'Xyzt, car si il pouvait envoyer des messages, alors il pourrait en recevoir.

d) le filtrage du 'peer to peer' / le filtrage des paquets

Sur internet, on peut se transmettre autre chose que des pages au format html (des pages web). On peut se transmettre à 2 ou à plusieurs, du courrier électronique et aussi des textes, images, musiques et ds fichiers de toute nature. On appelle le plus souvent « peer to peer », la pratique consistant à envoyer des messages sur le réseau, les réceptionne qui veut.

Filtrer le 'peer to peer', c'est donc enlever du réseau, non plus des correspondants, mais du contenu. On peut comparer cela à la chasse aux marchandise de contrebande sur les autoroutes (une des tâches de la gendarmeries depuis que les douanes internes de l'U.E. ont été supprimées).

le marquage ou tatouage des fichiers:

Le but du ministre de l'internet qui veut supprimer certains messages du réseau (par exemple des chansons sous copyright, des films, des séries...) va être de reconnaître ces messages pour les faire enlever. La technique consiste à marquer les messages 'qui ne doivent pas circuler', ce qui permet de les suivre à la trace, comme les vaches avec leur cloche, autrefois.

Une fois qu'ils ont été repérés, on peut en profiter pour punir ceux qui les réceptionnent. C'est la tâche de la fameuse Hadopi.

le blocage des protocoles

Il y a un autre moyen de filtrer le peer to peer, c'est le 'filtrage des protocoles' des logiciels de peer to peer. Un 'protocole' est un échange de politesses que s'envoient deux ordinateurs quand ils correspondent. De même que l'on ne peut pas écrire à un cardinal sans dire 'votre éminence', ni à un ambassadeur sans dire 'votre excellence', on ne peut pas communiquer sur internet sans protocole. Les logiciels de peer to peer, comme les autres, ont leur protocoles.

Par exemple ici, les requêtes envoyées par un serveur du logiciel Bittorrent :

```
~http://example.com/announce      -> ~http://example.com/scrape
~http://example.com/x/announce     -> ~http://example.com/x/scrape
~http://example.com/announce.php   -> ~http://example.com/scrape.php
```

Le 'filtrage protocolaire' déconnecte les ordinateurs qui lisent cela.

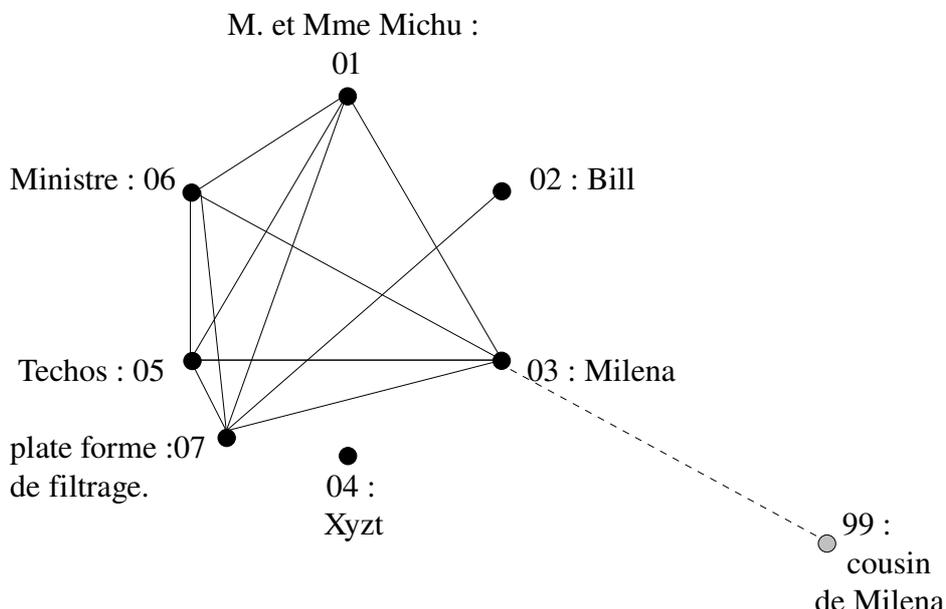
le blocage des 'ports' réseau

Et il y a encore un troisième moyen de filtrer les protocoles, c'est d'empêcher les ordinateurs d'ouvrir les 'ports' par où passent les fichiers échangés. Par exemple, le protocole Bittorrent passe par les ports 6881 à 6889. Si le F.A.I. ferme ces ports chez ses abonnés, il leur ferme les oreilles.

III : Où filtrer ?

a) : Le filtrage chez les F.A.I.

Les fournisseurs d'accès à internet font d'avantage que fournir la bande passante. Comme Techos, ils ont leurs propres serveurs DNS et ils 'routent' les messages des internautes. Ils ont donc le pouvoir technique. Le plus simple pour l'autorité – ici, pour le Ministre de l'Internet, est donc de transmettre ses desiderata aux F.A.I. (ici à Techos) pour qu'ils « nettoient » le réseau ici et là. Le réseau ainsi 'nettoyé' est un réseau forcément « bricolé ». Il se présente désormais plus ou moins ainsi : (fig.2)



b) Le filtrage chez l'autorité : le filtrage / espionnage par proxy.

Un ordinateur 'proxy' ou mandataire, est à l'origine un ordinateur qui envoie un message au nom de quelqu'un d'autre. Mais comme on va le voir, un 'proxy' peut tout aussi bien être un ordinateur que personne n'a mandaté et qui décide de son propre chef (celui de son propriétaire) de servir d'intermédiaire à un autre ou à tous les autres.

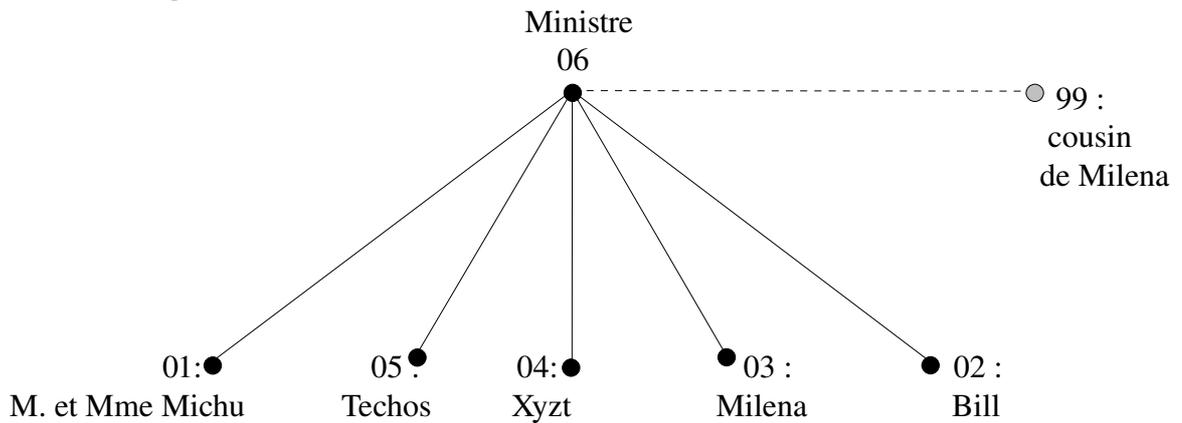
Si le ministre a connaissance de cette géniale possibilité, il peut demander à Techos de transformer son ordinateur (celui du ministre, le 06) en « proxy » pour tous les messages. Toutes les communications sont donc 'routées' vers le ministre, et seulement ensuite vers leur destinataire. Toutes les autres lignes sont inutiles. L'utilité est double:

1) Le ministre intercepte toutes les communications (web et peer to peer) et donc il peut les espionner. Il peut, par exemple, acheter autant d'écrans d'ordinateur que d'internautes et regarder en simultané les écrans des ordinateurs des Michu, de Bill, de Milena, de Xyzt, et même de Techos, comme autant de programmes de télévision. (des infos plus rigoureuses sont sur le site de David Monniaux)

2) le ministre peut, en temps réel, interrompre toute communication qui ne lui plaît pas, en débranchant simplement un câble.

Le cousin de Milena n'échappe pas à la règle : toutes les communications avec l'étranger passent par l'ordinateur du ministre.

Evidemment, l'« architecture » du réseau a beaucoup beaucoup changé. L'ancien réseau de pairs est devenu une « hiérarchie simple ». Cette forme de communication est représentée ainsi par Williamson (1975) (fig.3)



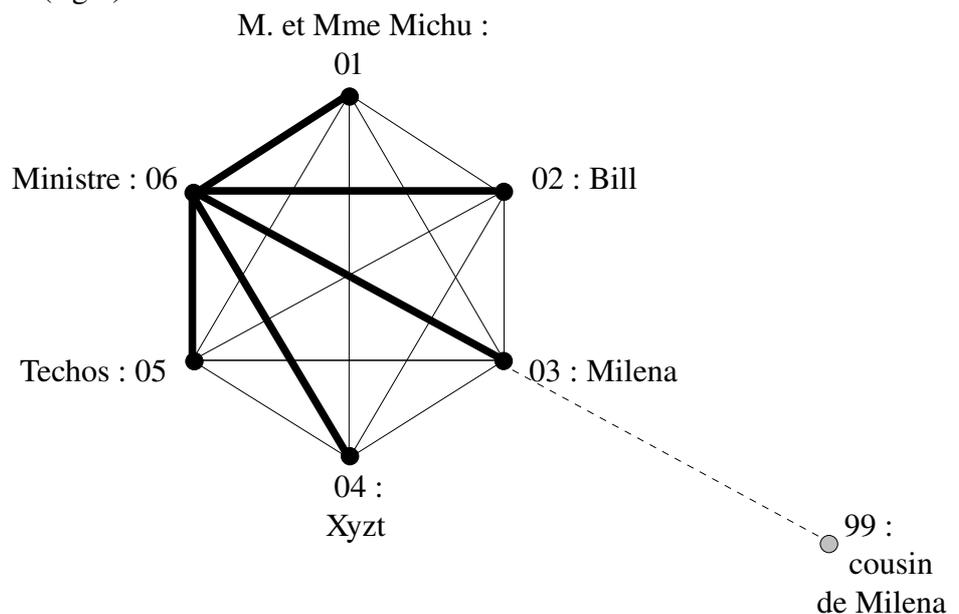
Il n'y a plus que deux sortes de communications, celles qui entrent dans l'ordinateur du ministre et celles qui en sortent. Tout passe désormais par lui, même si il peut faire en sorte que personne ne s'en aperçoive. Et, vis à vis de l'étranger, le réseau national se présente comme un intranet / comme un réseau NATé dont la seule i.p. publique serait celle du ministre.

c) le filtrage chez l'habitant / le filtrage sur les postes clients

Jusqu'ici, on a supposé que, pour filtrer internet, il fallait détourner le trafic vers un ordinateur (serveur) qui servira de filtre, d'une manière ou d'une autre. Il y a une autre solution.

Le ministre va installer des logiciels sur les ordinateurs des internautes, de la même manière que les parents installent des logiciels de contrôle parental sur les ordinateurs de leurs enfants. Cette solution est préconisée par le CGTI à propos de la fameuse Hadopi. Cette solution n'est efficace que si les logiciels sont mis à jour – comme les anti-virus. Elle nécessite donc que chaque ordinateur soit connecté en permanence à l'ordinateur du ministre.

Le réseau peut, cette fois-ci rester dans sa forme originale, mais les connexions avec l'ordinateur du ministre (route directe) sont obligatoires 7/7 et 24/24 (traits gras), pour les mises à jour des logiciels de contrôle gouvernemental. (fig.4)



IV : Le mode de filtrage retenu.

On se demande maintenant : sachant tout celà, que va choisir le Ministre de l'Internet pour filtrer le réseau :

a) un double filtrage des domaines et des i.p.

Le filtrage par URL ou filtrage hybride, est coûteux et compliqué. En plus, il est très facile pour des malins (ici pour Bill), d'invertir les noms de leurs pages web et leurs contenus (voir l'interview de M.Free à Pcinpact). Le seul avantage du filtrage par URL est politique : il permet au ministre de dire : « je vais filtrer les contenus illégaux et seulement ceux là, je le jure ».

Dans la pratique, une seule méthode est efficace pour empêcher Bill de vendre des biens prohibés et pour d'empêcher Xyzt d'exister, c'est le double filtrage par noms de domaines et par i.p.

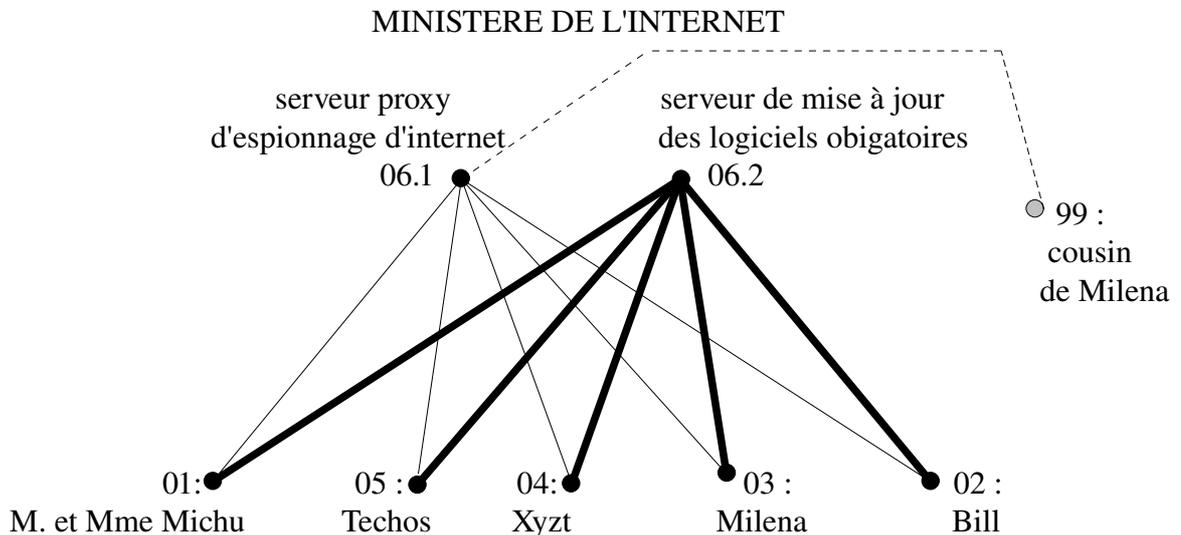
b) un double filtrage, chez l'autorité et chez l'habitant

On a vu que les F.A.I. pouvaient pratiquer le filtrage des noms de domaine et le filtrage des adresses i.p. Mais peut on faire confiance aux F.A.I.? Bien évidemment, non (voir dans le rapport du Forum des Droits sur Internet comment les autorités ont tellement confiance dans les F.A.I. qu'elles hésitent à leur fournir la liste des sites à filtrer).

Donc tout le trafic va être (dé)routé vers les serveurs proxy de l'autorité / vers l'ordinateur du ministre. Mais ce n'est pas suffisant pour filtrer le peer to peer (style, des internautes se transmettent des copies illégales de la chanson « Sergent Pepper », dans un fichier appelé « Hymne à la patrie ».

Donc en plus, il ca falloir installer des logiciels de filtrages dans les ordinateurs de chaque internaute, ce qui, techniquement ne pose aucun problème. Ce double filtrage est la solution recommandée par le fantastique rapport du CGTI.

Le réseau filtré va donc, au final, ressembler à quelque chose comme ceci : (fig.5)



Conclusion : d'internet à hiérarchie.net

Le réseau internet a été conçu pour la recherche, à une époque où les chercheurs étaient payés pour former une grande famille et pour partager leurs découvertes. Internet est donc un réseau de pairs et il ressemble, dans sa construction, à une communauté hippie quand le gourou est en vacances (il suffit de voir Richard Stallman ndlc). Il est égalitaire et ouvert. Il pousse à l'abandon des droits de propriété intellectuelle. Le CERN avait même mis les protocoles du Web dans le domaine public.
internet -----> circulation rapide des découvertes -----> logiciels libres, art libre, domaine public

Depuis, la politique scientifique et culturelle des Etats a connu un virage à 180 degrés. Aujourd'hui, les chercheurs sont payés pour déposer des brevets avant la fac concurrente. Aujourd'hui, l'INA fait payer l'accès aux images prises avec l'argent du contribuable.

Mener une telle politique de brevets et de copyright avec un réseau internet ouvert = impossible.
Un copyright, un brevet, sont faits pour mettre des barrières à la diffusion des connaissances.
Internet avait été conçu pour enlever ces barrières.

La seule solution, c'est donc de filtrer internet au point qu'il n'aura plus d'internet que le nom. Ce sera devenu un hiérarchie.net

hiérarchie.net <----- barrières à la diffusion <----- politique de brevets et de copyright

Et pour les mêmes raisons qu'internet conduisait au piratage, hiérarchie.net conduira à Big Brother.

sources de cette présentation

sur internet

Le 'blog d'un enseignant' sur le filtrage à l'école primaire
<http://kentel.blogspot.com/2006/04/filtrage-internet-lcole.html>

La présentation du filtrage d'internet par David Monniaux sur son blog
<http://david.monniaux.free.fr/dotclear/index.php/2008/12/09/330-le-point-sur-le-filtrage-internet>

Note de « la quadrature du net » sur le filtrage hybride.
<http://www.laquadrature.net/files/note-quadrature-filtrage-hybride.pdf>

Forum des droits sur internet : recommandation : les enfants du net III :
<http://www.foruminternet.org/specialistes/concertation/recommandations/recommandation-du-forum-des-droits-sur-l-internet-les-enfants-du-net-iii-conditions-necessaires-a-la-mise-en-place-du-filtrage-des-sites-pedopornographiques-par-les-fai-2791.html>

La news de PCinact sur le filtrage du « peer to peer » en Australie:
<http://www.pcinact.com/actu/news/48048-filtrage-p2p-protocole-bittorrent-austraie.htm>

sur papier :

Le livre d'Oliver Williamson : « Markets and Hierarchies » (1975) , chap.3 : peer groups and simples hierarchies.