QUAND LE WEB SE MILITARISE

LE 30 OCTOBRE 2010 ***SUSAN CRAWFORD (TRADUCTION OLIVIER TESQUET)***

Alors que les autorités américaines ont manifesté leur volonté de renforcer la surveillance d'Internet, Susan Crawford, ancienne conseillère de Barack Obama, s'inquiète de cette évolution.

Professeur de droit à Yale, ***Susan Crawford*** *a été la conseillère en innovation de Barack Obama jusqu'en décembre 2009.*

—

Je crois qu'il faut que quelqu'un se penche sur toutes ces histoires de surveillance d'Internet, stratégiquement placées en Une du New York Times. Il y a ici une piste à suivre. Voici quelques repères chiffrés:

1. Les cyberattaques – Il semble y avoir un profond intérêt pour la capacité à déclarer la guerre en ligne, comme l'ont mis en évidence les recherches en matière de cybersécurité et les discours publics d'Herbert Lin, un acteur clé qui a travaillé sur de nombreux rapports pour le **National Research Council**. Ethan Zuckerman **a synthétisé une présentation de Lin**, qui paraphrase ses remarques de la façon suivante:

> ***Si nous voulons préempter les cyberattaques, il faut être dans les réseaux de celui d'en face. Mais cela peut impliquer de s'introduire dans l'ordinateur familial de citoyens américains. Aussi loin que le cloud computing dépasse les frontières, nous attaquons peut-être des ordinateurs dans de multiples juridictions. Lin se demande si un Internet mieux authentifié permettrait d'anticiper les attaques. Et ils nous rappelle que le commandement stratégique américain a émis des autorisations pour mener "des actions de neutralisation des menaces actives" – s'introduire dans une machine pour stopper une attaque en cours, par exemple…***
>
> ***Le Dr Lin note que les actions de renseignement à l'étranger ne violent pas les lois internationales. Il est possible de s'engager dans des actions clandestines réglementées par la législation américaine. Et en réponse à une cyberattaque, les Etats-Unis pourraient lancer une grande variété de ripostes (Lin précise qu'il ne préconise aucun de ces exemples) – ils pourraient attaquer les défenses aériennes de l'ennemi, pirater leurs machines de vote pour influencer une élection, mener des campagnes de "cyberexploitation" pour espionner ces nations. Dans ces conditions, les Etats ne doivent-elles pas craindre les conséquences d'un Internet "libre et ouvert"? Pourraient-ils raisonnablement choisir de renforcer leur contrôle sur le web?***

2. Un *"Internet mieux authentifié"* impliquerait évidemment l'usage de leviers fournis par les opérateurs de télécommunications, pour permettre aux seules machines autorisées, identifiées, de se connecter. La possibilité de déconnecter à distance des machines ou des appareils jusqu'à ce qu'ils soient *"nettoyés"* est désormais **à portée des réseaux fédéraux** – et cette capacité va inévitablement s'étendre aux connexions privées.

3. Un *"Internet mieux authentifié"* signifierait aussi des applications et des machines plus facilement exploitables. C'est ce dont parle le directeur du FBI, Robert Mueller, **à 3:29 de cette vidéo**.

4. Il doit y avoir beaucoup de stress au sein du gouvernement américain vis-à-vis de la position publique de l'administration sur l'amélioration de la surveillance, sur l'authentification, et sur la capacité à déclarer la guerre en ligne. **Le discours d'Hillary Clinton sur la "liberté d'Internet"** en janvier 2010 a montré que la libre circulation de l'information sur le web était une composante importante de la diplomatie.

Internet n'est pas le téléphone

5. Eu égard à ce stress, les agences qui sont les plus intéressées par les cyberattaques, la surveillance, l'existence de trappes d'accès dans les communications cryptées et tout l'attirail d'un *"Internet mieux authentifié"* ont un intérêt à présenter leur vision du web comme un processus inévitable. Logiquement, une partie de cette campagne de persuasion réside dans leur capacité à porter cette version de l'histoire dans les grands médias.

6. Donc, nous y voilà – une nouvelle histoire **en première page du Times d'hier**, 19 octobre: *"L'administration pousse pour renforcer la loi sur les écoutes"* . C'est une question extrêmement controversée. La loi devrait-elle forcer l'ensemble des technologies en ligne à disposer de "trappes", permettant aux autorités de réclamer (pour l'essentiel) que l'information leur soit restituée comme au temps de **l'autocommutateur téléphonique privé**?

7. Internet est différent du réseau téléphonique. C'est un accord décentralisé qui permet d'acheminer des paquets d'informations à des adresses définies. Il a rendu possible une innovation sans précédent, il a aidé la liberté d'expression et l'amélioration de vies humaines autour du monde. Le brider pour l'adapter aux besoins "d'authentification" d'une loi d'application (ou de la sécurité nationale) serait un énorme pas en arrière.

Mais cela nous aiderait sûrement à faire la guerre en ligne.

Ce billet a initialement été publié sur le blog de Susan Crawford

—

Crédits photo: Flickr CC ***jurvetson***, ***randy.troppmann***

2 pings

Quand les gouvernements se feront prendre par derrière » Article » OWNI, Digital Journalism le 16 novembre 2010 - 18:10

[...] A lire également sur le sujet: Quand le web se militarise [...]

De la cyberguerre à la surveillance » Article » OWNI, Digital Journalism le 6 janvier 2011 - 13:28

[...] Un durcissement impitoyable des politiques de sécurisation de la Toile, par le biais législatif, technique et policier, [...]