# NATHALIE KOSCIUSKO-MORIZET

## Secrétaire d'Etat chargée de la Prospective et du Développement de l'économie numérique

**Ulysse Gosset, Journaliste, France Télévisions**

Merci Monsieur Chertoff. On va peut-être donner la parole à la ministre française. Comment vous voyez l'avenir de la cybersécurité et qui doit assurer la sécurité des réseaux Internet à travers le monde ?

**Nathalie Kosciusko-Morizet**

D'abord, je voudrais à nouveau insister sur le fait que ce n'est pas le seul problème. La protection des données personnelles, par exemple, fait peser des menaces sur les individus et d'une certaine manière, sur les sociétés, qui sont tout à fait considérables et qu'il faut prendre en compte. C'est presque une facilité de foncer sur le sujet de la cybersécurité parce qu'on l'entend bien, parce que ça parle de guerre, parce que ça parle de quelques exemples qu'on a eus dans les années passées, dans l'actualité. Je pense que ce sera, d'une certaine manière, le sujet le plus facile à résoudre ou en tout cas le sujet le plus facile à concevoir intellectuellement. Peut-être pas à résoudre, mais au moins à concevoir intellectuellement. Maintenant, si on reste néanmoins dessus, qu'est-ce qu'on peut faire ? D'abord, il y a deux types de problèmes. C'est vrai que c'est très asymétrique. Ce sont des menaces très asymétriques et ce sont des menaces dans lesquelles plus encore que dans le monde réel, le cyber terrorisme se confond avec la cyber guerre parce qu'en fait, parfois, on peut très difficilement savoir qui est derrière l'attaque.

En fait, les méthodes de cyber guerre, même quand elles sont menées par des Etats, utilisent des pratiques qui sont celles du terrorisme. Ça consiste à prendre en main à travers des botnets des réseaux entiers d'ordinateurs que l'on a infectés pour les utiliser pour pouvoir attaquer massivement des parties entières du réseau. Ça peut être un Etat qui le fait, mais on entend bien que ce n'est pas très propre. Il y a deux types de méthodes : soit infecter des ordinateurs et à un moment les lancer tous sur une partie du système ou alors sur un site particulier. En général, c'est un site officiel, et créer à travers ce problème ce qu'on appelle un déni de service. Faire tomber le réseau comme ça. Il y a un autre moyen qui est l'utilisation de virus plus subtils et peut-être plus dangereux, d'ailleurs moins visibles. La première parade, me semble-t-il, c'est la coopération. La coopération pour partager les informations que l'on a sur les failles des réseaux et pouvoir les résoudre ensemble.

La coopération aussi, parce qu'Internet est un réseau profondément décentralisé et il trouvera sa sécurité en assumant ce caractère extrêmement décentralisé et pas en voulant recentraliser les systèmes, y compris les systèmes de protection. Je prends un exemple. Internet souffre de toutes sortes de fragilités, je partage là-dessus le point de vue de Monsieur Barrault, et en même temps, de moins de fragilités, d'une certaine manière, qu'il y a un ou deux ans, à cause de la réplication des serveurs racines. Dans le temps, il y avait une dizaine ou une douzaine de serveurs racines qui étaient essentiellement aux Etats-Unis et ils n'étaient que là-bas. Maintenant, on les a répliqués. On les a virtualisés un peu partout. Ce ne sont que des répliques et donc, ça ne résout pas l'ensemble du problème. Mais le fait de les avoir répliqués et virtualisés permet de résister à une attaque ou à un problème, plus facilement, plus longtemps en tout cas. Le caractère décentralisé du réseau est en soi protecteur et il me semble que ce qu'on devrait trouver au niveau mondial, c'est ça. Parer un certain nombre d'attaques dans le respect du caractère décentralisé du réseau et plus que dans le respect, en utilisant le caractère décentralisé du réseau en vrai bon réseau neuronal qu'est Internet.