# MICHAEL CHERTOFF

## Ancien Secrétaire à la Sécurité intérieure des Etats-Unis

**Steven Erlanger, Chef du Bureau de Paris du *New York Times***

Il me semble évident qu'Internet pose un défi énorme à la souveraineté. Nous essayons de parler de gouvernance alors qu'Internet sape la gouvernance. Si nous examinons l'autre grand sujet de cette conférence, à savoir la crise financière, nous constatons très rapidement que les gouvernements sont des outils d'une grande lenteur. Ils ne réagissent pas promptement ; au final, ils ne vont pas aussi vite que les marchés. Les meilleurs éléments ne passent pas toujours par nos instances de régulation.

Nous sommes confrontés ici au même problème. Il y a, comme on l'a appris hier soir, 900 millions d'internautes en Chine mais qui n'ont pas accès à ce qu'ils veulent voir. Nous savons que la Chine vend des logiciels de filtrage à l'Iran. Les gouvernements ont du mal à maîtriser ce qui existe. Nous savons qu'Al-Qaïda communique avec ses cellules par le biais d'Internet, grâce à Hotmail, Google Mail et des messages codés. Comment contrôler cela ?

Il me semble que nous avons réellement besoin d'agir en termes de gouvernance et de gouvernements. Je m'exprime peut-être ici en tant qu'Américain. Nous devons davantage réfléchir à notre vulnérabilité et aux questions de cyberguerre et de cybersécurité. Nous l'avons vu en Estonie ; nous l'avons vu pour la Géorgie. Nous sommes très vulnérables ; les choses peuvent s'interrompre très rapidement.

Je pense aussi que nous avons beaucoup de chance ; nous avons parmi nous l'ancien secrétaire américain à la Sécurité intérieure, Michael Chertoff. Il a évidemment passé un temps considérable à se préoccuper de ces questions. Avant de prendre les questions, j'espère que vous ne verrez pas d'inconvénient à ce qu'il nous parle pendant quelques minutes de ses propres inquiétudes et de ses propres expériences.

**Michael Chertoff**

Merci à vous tous de me permettre d'intervenir. Comme vous le savez, nous examinons la question de la cybersécurité aux Etats-Unis depuis de nombreuses années. A compter de 2007-2008, une stratégie complète de cybersécurité a été élaborée, sous les auspices de l'administration précédente, et se poursuit sous l'administration actuelle.

Globalement, il existe trois défis liés à la sécurité auxquels Internet doit faire face. L'un des problèmes est la cybercriminalité ; les gens ont parfaitement conscience de son existence. Ses dimensions sont écrasantes ; des vols de dizaines de millions de numéros de cartes de crédit ont eu lieu, avec des répercussions énormes sur les utilisateurs. A part ça, il y a l'espionnage industriel et l'espionnage d'Etat. Des quantités énormes de données sont volées. Tout le monde a entendu parler de l'attaque contre Google perpétrée plus tôt dans l'année, qui ne représente qu'un exemple parmi d'autres du type d'impact économique de ce phénomène sur le commerce et nos gouvernements.

Le troisième problème, lequel à mon sens est le plus dérangeant, est celui abordé par Steve, à savoir la question des cyberattaques et des cyberconflits. En 2007, l'Estonie a essuyé une attaque de déni de service. Il y a eu des cyberattaques autour des événements en Géorgie en 2008. Il y a récemment eu des articles dans les journaux à propos d'un ver qui semble attaquer les systèmes de contrôle de certains types d'appareils Siemens. Cela souligne le

danger d'une attaque qui non seulement submergerait un réseau, mais le détruirait entièrement. Un réseau qui gère potentiellement une infrastructure essentielle.

Nous sommes face à une conjoncture dans laquelle Internet permet aux personnes d'avoir potentiellement un effet catastrophique et destructeur. Cela ne concerne pas uniquement Internet en soi, mais aussi les systèmes réels qui dépendent d'Internet. Tel est le défi. Je pense que Craig avait raison de parler d'asymétrie. Il faisait référence au fait que le type de destruction qui était auparavant réservée à un Etat-nation peut désormais être exécutée par un groupe, voire un individu disposant de la capacités suffisantes.

Cependant, le même principe crée également un problème d'attribution. En d'autres termes, nous ne savons pas forcément qui mène une attaque. Souvent, une attaque est lancée par l'intermédiaire de tierces personnes, grâce à des serveurs piratés par des gens pour leur propre usage. Dans certains cas, on soupçonne un gouvernement d'avoir lancé une attaque, mais ce gouvernement nie l'accusation. Ils disent qu'il s'agit d'un groupe de jeunes ou de personnes qui agissent pour leur propre compte.

Cela ne facilite pas la mise en place du type de régime de gouvernance auquel nous sommes habitués. Par exemple, dans les domaines de l'armement ou de l'espace, au bon vieux temps de la guerre froide, nous connaissions les protagonistes en mesure de lancer une attaque nucléaire. Nous avons élaboré une doctrine et une série de règles internationales pour gouverner le domaine de l'armement nucléaire avec pour résultat un environnement stable. Le problème, à cause de l'asymétrie, est que nous ne pouvons pas procéder aussi facilement avec le cyberespace.

Ma question au panel est la suivante. Certaines personnes doutent que l'on parvienne à un quelconque accord international sur le cyberconflit. Ils sont convaincus qu'il serait impossible de le controler et qu'un pays pourrait très bien signer un accord et pourrait aussi bien nier être en train de le violer. Certaines personnes, en raison de la fréquence de l'espionnage sur Internet, pensent que ce ne sera pas utile.

D'autres encore pensent que nous pouvons trouver un accord dans certains domaines que tous les pays considéreraient comme interdits à la cyberguerre. Je me situe dans cette catégorie. Les exemples comprennent la destruction du système financier mondial, qui porterait préjudice à tout le monde. De nouveau la question se pose : comment contrôler ? Qui doit s'assurer que les serveurs de son propre pays ne servent pas à des attaques ? Que faire si un pays est incapable de gérer son propre domaine ? D'autres pays peuvent-ils intervenir pour assurer cette défense ? Les questions complexes sont nombreuses. La question que je soumets au panel est la suivante : quel avenir voyez-vous pour ce type de régime de contrôle des armes dans le contexte du cyberespace ?