Le Conseil Atlantique sur la cybersécurité : la collaboration contre les menaces peut être la clé de la prospérité

Publié le vendredi 20 juin 2014
Voir en ligne : https://www.france-science.org/Le-Conseil-Atlantique-sur-la.html

Ce lundi 9 juin, une discussion entre experts dans le domaine de la cybersécurité s'est tenue au Conseil Atlantique, un *think tank* influent de Washington, DC. Le forum ouvert au public faisait partie de la *Cyber Statecraft Initiative*, une série de d'événements sur la coopération, la concurrence, et les conflits internationaux dans le cyber-espace.

Crédits : Yellowj

Le Conseil Atlantique a été fondé en 1961 pour fournir un forum sur l'évolution des forces politiques et économiques du monde moderne. Il développe des actions d'éducation et d'animation menées par un réseau de dirigeants importants et non partisans, dans les domaines variés, notamment la politique et les affaires internationales. Aujourd'hui, ses divers centres et programmes couvrent de nombreuses régions et des sujets contemporains. [1]

L'événement s'est passé au *Brent Snowcraft Center on International Security* au siège du Conseil Atlantique, au centre de Washington DC. Le sujet de discussion était, sans surprise, l'évolution de la cybersécurité à la suite des révélations d'Edward Snowden l'année dernière. La divulgation des vastes programmes de collecte des données gérés par la NSA (*National Security Agency*) et le développement des techniques appliquées aux Big Data, ont soulevé des questions sur la surveillance électronique et l'environnement mondial du cyber-espace. Les experts ont identifié les les grandes questions et les solutions générales relatives à la cybersécurité. Le consensus ? Dans un monde où la sécurité numérique et la vie privée se réduisent constamment, la collaboration est la meilleure défense.

Jason Healey, directeur de la *Cyber Security Initiative*, a modéré la discussion entre trois membres éminents de la communauté de la cybersécurité. Tous étaient ouverts aux commentaires et questions d'un public représentatif des agences gouvernementales, universités, ambassades et entreprises. David Ignatius, rédacteur adjoint et chroniqueur, a pris une part importante dans cette discussion, en se référant à son livre publié cette année, *The Director*, un roman d'espionnage qui comporte des attaques cybernétiques. Cheri McGuire, vice-présidente des affaires gouvernementales et de la politique de cybersécurité à Symantec, et Jeff Moss, membre de la *Cyber Security Initiative*, complétaient les intervenants.

Avec une série de questions, les panélistes ont abordé les problèmes posés par le piratage informatique, une menace qui est de plus en plus liée à la sécurité nationale. M. Ignatius considère que rien n'est vraiment secret, parce que la protection de la vie privée est réduite chaque jour. Selon les experts, il faut faire face à une nouvelle réalité, entre la surveillance du gouvernement, exposée par M. Snowden, et le pouvoir montant de la piraterie criminelle. Ils ont abordé aussi la menace économique posée par les cyber-attaques ; les consommateurs perdent confiance dans les entreprises quand ils sentent que leurs informations ne sont pas sécurisées. L'année dernière, des pirates ont volé les informations personnelles d'au moins 800 millions de personnes. En dépit de ce chiffre, des entreprises américaines ne dépensent pas plus de 2% de leur budget technologique sur la sécurité [2]. M. Moss a critiqué certaines entreprises pour le manque de protection ou d'informations insuffisantes données aux consommateurs, ces faiblesses nuisant à l'économie comme à la sécurité nationale.

Mme McGuire décrit la lutte contre les attaquants comme une course aux armements. Il faut développer des défenses plus rapidement que les pirates ne développent leurs attaques : un vrai défi étant donné que les attaquants disposent d'un accès libre aux données de millions de personnes dans le monde, selon M. Ignatius. Les panélistes ont conclu que cette tâche ne peut être accomplie sans coopération à plusieurs niveaux : les individus, les entreprises, et les agences gouvernementales. La technologie antivirus n'arrêterait que 45% des attaques, un chiffre qui montre le besoin d'utiliser d'autres approches. De plus, les experts ont rappelé au public international qu'il faudra une collaboration entre les pays pour lutter contre cette menace.

Sources :

- [1] "Renewing the Atlantic Community for Global Challenges" - Atlantic Council - 2014 - http://www.atlanticcouncil.org/about
- [2] "US retailers face pressure to raise cybersecurity spending." - Reuters - Dhanya Skariachan & Phil Wahba - 5/2/2014 - http://www.reuters.com/article/2014/02/05/us-usa-retailers-cybersecurity-idUSBREA1409H20140205

Pour en savoir plus, contacts :

- Site Internet du Conseil Atlantique : http://www.atlanticcouncil.org/
- Article anglais sur la discussion sur le Site Internet du Conseil Atlantique : http://www.atlanticcouncil.org/events/past-events/national-security-and-digital-prosperity-after-snowden-a-discussion-with-david-ignatius
- Site Internet de la Cyber Statecraft Initiative : http://www.atlanticcouncil.org/programs/brent-scowcroft-center/cyber-statecraft

Code brève
ADIT : 76202

Rédacteurs :

- Ellen Zamsky (stagiaire-ntics@ambascience-usa.org) ;

- Suivre le secteur Nouvelles Technologie de l'Information, Communication, Sécurité sur twitter @MST_USA_NTICS ;
- Retrouvez toutes nos activités sur http://france-science.org.