WASHINGTON CHINOISE SUR LE CYBERESPACE

LE 11 OCTOBRE 2012 ***GUILLAUME DASQUIÉ***

Seuls les services secrets des États-Unis, et un peu d'Europe, auraient le droit de fricoter avec les géants du numérique qui gèrent l'Internet mondial. Pas les Chinois. C'est ce que préconisent deux parlementaires américains. Pas très *fair play* .

En début de semaine, le Congrès américain **frappait d'ostracisme les filiales américaines** des groupes chinois **Huawei** et **ZTE**, en convoquant une conférence de presse pour inviter l'industrie américaine à ne plus travailler avec ces entreprises spécialisées dans les infrastructures de télécommunications. Huawei et ZTE équipent des *data centers*, des fournisseurs d'accès à Internet (FAI) ou vendent des composants de la téléphonie mobile. Des technologies considérées comme autant de menaces potentielles par le Congrès.

À l'appui de cette attaque en règle, un rapport émanant de la Commission du renseignement de la Chambre des représentants. Dont les membres, depuis plusieurs mois, ne cachent pas **tout le mal qu'ils pensent de la présence** – encore modeste – de Huawei et ZTE sur le marché américain.

La version finale de leur document de 60 pages – que nous avons lu, **ici en PDF** – multiplie les affirmations quant à l'opacité de ces deux géants chinois des télécoms et du numérique, à la fois fabricants et prestataires de service. Sans toutefois apporter de preuves matérielles convaincantes.

Une absence regrettable dans la mesure où ces attaques contre Huawei et ZTE interviennent sur fonds de tensions économiques sur le marché des télécoms américains, en raison de la concurrence que ces groupes représentent. Peu après la conférence de presse du Congrès, la direction de Huawei **a d'ailleurs répondu** en laissant entendre qu'il s'agirait d'un mauvais procès motivé par la course vers de juteuses parts de marché.

Opérations militaires

Sur un plan matériel, le document s'appuie le plus souvent sur des informations déjà publiées dans la presse, même si une note de bas de page mentionne l'existence d'annexes classifiées, portant sur le travail des services américains de renseignement quant à la réalité de ce risque.

Le rapport a été rédigé par deux élus suivant régulièrement *"la communauté du renseignement"* et ses enjeux, Dutch Ruppersberger et Mike Rogers.

Alors que ce dernier a fait **une partie de sa carrière au FBI**, Ruppersberger, pour sa part, passe pour un

parlementaire très attentif aux questions de souveraineté nationale. Au Congrès, depuis plusieurs législatures, il représente le second district du Maryland, **la circonscription où campe la National Security Agency** (NSA), à Fort Meade, ainsi que la plupart des commandements américains impliqués dans les opérations militaires sur les réseaux numériques. En particulier **le US Cyber Command**. Dans ce second district du Maryland on compte ainsi près de 38 000 personnes travaillant pour l'appareil sécuritaire du gouvernement.

[CARTE INTERACTIVE] LA CHINE INVESTIT L'EUROPE

En pleine crise financière, les liquidités chinoises font craindre des vagues d'acquisitions en Europe. OWNI a recueilli et ...

Et plusieurs dizaines de milliers d'autres employées dans des sociétés privées sous-traitantes. Tout un monde qui vit – à tort ou à raison – sur la base d'une économie du soupçon ciblant les acteurs chinois dans des technologies de l'information.

À défaut de preuves irréfutables à l'encontre de ces entreprises chinoises, la démarche des parlementaires américains peut paraître un rien étonnante. En effet, le géant américain Cisco semble entretenir les mêmes ambiguïtés que celles reprochées à Huawei et ZTE – contrats avec les militaires de leur pays d'origine et partenariats avec des agences de renseignement.

Espionnage

Avec des conséquences tout aussi préoccupantes pour le citoyen. Depuis le début des années 2000, à travers le monde, Internet se développe **grâce à des routeurs** fournis par Cisco ou par les cinq autres sociétés américaines ou franco-américaine (Alcatel-Lucent) qui maîtrisent ces technologies et travaillent parallèlement avec le complexe militaire de leur pays – jusqu'à l'arrivée d'Huawei qui les concurrence.

À ce titre, pour les observateurs américains, les accointances entre Cisco et la NSA sont légions. Selon l'enquêteur James Bamford, **auteur de plusieurs livres qui font autorité sur la NSA** et les technologies d'espionnage, cette proximité relève de l'essence même de la NSA, au regard de ses missions de surveillance globale des réseaux. Lors d'un **entretien avec des journalistes de la chaîne PBS** Bamford affirmait :

> ***L'une des choses que la NSA fait c'est de recruter beaucoup de gens venant de l'industrie des télécoms, donc de gens qui connaissent comment Internet fonctionne, qui savent comment certains systèmes à l'intérieur d'Internet sont construits. Par exemple, ils pourraient recruter des gens de Cisco qui construisent divers routeurs, et les intégrer dans la NSA pour ensuite déconstruire le fonctionnement des routeurs.***

Les enjeux financiers provoqués par le gonflement des budgets militaires après le 2001 ont accentué cette dynamique. De nos jours, le groupe Cisco, via un département spécialisé – dénommé *Federal Intel Area* -, propose des services de surveillance et de traitement du renseignement sur-mesure à l'ensemble des services secrets américains ; comme le montre **cette brochure commerciale** [pdf]. Une relation qui semble parfaitement assumée ; nous avons retrouvé sur LinkedIn **le CV détaillé** de l'un des responsables de ce programme actuellement en poste chez Cisco.

LES ROUTEURS DE LA DISCORDE

Européens et Américains sont d'accord : les équipements chinois sont materia non grata, en particulier les routeurs - ...

Finalement, ces relations entre entrepreneurs du numérique et appareil sécuritaire s'inscrivent dans la tendance naturelle de tous les États à contrôler et surveiller tous les réseaux de communication – depuis le télégraphe jusqu'à Internet. Le 14 août dernier près de Baltimore, lors d'une conférence réunissant des agences du département américain de la Défense impliquées dans le renseignement électronique, Keith Alexander, patron de la NSA, a rappelé cette évidence **lors d'une intervention de près de 40 minutes** consacrée aux opérations de la NSA dans le cyberespace.

S'exprimant sur quelques détails des missions de son agence sur le numérique, il a évoqué **les 18 câbles sous-marins reliant les États-Unis au continent européen** et permettant aux connexions Internet de traverser l'Atlantique grâce à de multiples relais technologiques… Et les partenariats avec des pays comme la Grande-Bretagne ou la France permettant de surveiller l'ensemble.

Ces acteurs technologiques étant les clients des appareils sécuritaires de leur pays d'origine, il est difficile des les imaginer ne bâtissant pas ces ponts qui facilitent leur tâche – au nom de l'idée qu'ils se font de leur propre sécurité nationale, et des intérêts qu'ils partagent.

Festival of lights, Photo CC by Rene Mensen I **365 Day 256**, Photo CC by Collin Harvey.

ITI
le 11 octobre 2012 - 10:51 • SIGNALER UN ABUS - PERMALINK

Bjr.

"…grâce à des routeurs fournis par Cisco ou par les cinq autres sociétés américaines ou franco-américaine (Alcatel-Lucent) qui maîtrisent ces technologies et travaillent parallèlement avec le complexe militaire de leur pays"

Et où ceux-ci font-ils concevoir (tout ou partie) leurs routeurs, leurs chips ? Et qui en fait l'assemblage ???? ZTE et Huawei sont certes plus visibles, mais tant qu'on persistera à faire fabriquer/sous-traiter des parties entières de routeurs en Chine, le problème persistera.

ITI

VOUS AIMEZ 1 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

GUILLAUMEDASQUIE
le 11 octobre 2012 - 11:29 • SIGNALER UN ABUS - PERMALINK

Absolument ! Bien vu.
Et sur cette problématique – de l'interdépendance – je vous conseille l'excellent papier de nos confrères de Rue 89 :

http://www.rue89.com/2012/10/10/telecoms-energie-les-geants-chinois-face-au-soupcon-securitaire-236057

VOUS AIMEZ 1 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

1 ping

Washington chinoise sur le cyberespace « le 11 octobre 2012 - 20:45

[...] on owni.fr Share this:TwitterFacebookJ'aime ceci:J'aimeSoyez le premier à aimer [...]