Que devient le thème de la « cybermenace chinoise » ?

14/01/2014 à 07h00 Mis à jour le 14/01/2014 à 13h17

En 2014, les entreprises chinoises resteront au coeur de l'actualité avec la nécessaire maîtrise des risques liés à l'acquisition de matériels d'origine étrangère et à l'accès aux marchés nationaux d'entreprises étrangères.

L'actualité de la cybersécurité s'est très largement fait l'écho tout au long de ces dernières années de nombreuses cyberattaques attribuées à la Chine. Mais nous constatons aussi que depuis quelques mois le thème de la « cybermenace chinoise » est moins mis en avant dans les discours sur la cybersécurité. En effet, les dernières actualités à avoir fait l'objet d'une forte publicité remontent à la première moitié de l'année 2013 : publication du rapport Mandiant affirmant avoir localisé les unités de cyberespionnage étatique chinois, puis au mois de juin, rencontre des présidents américain et chinois pour amorcer un dialogue sur les enjeux et les pratiques dans le cyberespace. Mais depuis, il semblerait que l'on parle moins de la Chine…

Pourquoi parle-t-on moins de la cybermenace chinoise ?

A cela plusieurs raisons sans doute :

- Au début de l'année 2013 certains observateurs crurent déceler une accalmie dans l'activité d'origine chinoise (http://www.theverge.com/2013/5/20/4347482/chinese-cyberattacks-on-us-resume-after-post-report-lull). Un rapport de l'US-China Economic and Security Commission (http://www.reuters.com/article/2013/11/06/net-us-usa-

china-hacking-id[illegible]9A51AN20131106?feedType=RSS&[illegible]me=politicsNews&utm_source=dlvr.it&utm_medium=twitter&dlvrit=574655) publié en novembre 2013 attribue cette accalmie à l'impact du rapport Mandiant. La Chine, prise la main dans le sac, se serait faite plus prudente…

- Les principaux promoteurs du discours sur la cybermenace chinoise doivent gérer le scandale international provoqué par les révélations sur les pratiques de cybersurveillance américaines. Ces révélations rappellent que la Chine n'est pas seule, loin de là, à exploiter le cyberespace pour assurer sa sécurité et maintenir ou accroître sa puissance.

- Depuis juin 2013, le monde accorderait plus d'attention aux pratiques de la NSA qu'à celles des services de renseignement, à l'armée et aux cybercriminels chinois. Pour Mike Rogers (http://www.zdnet.fr/actualites/espionnage-chinois-accusations-ridicules-et-tentatives-de-diversion-des-us-39796542.htm), membre de la Commission américaine du renseignement, l'espionnage chinois serait le grand gagnant de cette situation.

- De nouveaux acteurs de la cybermenace prennent place dans le paysage mondial. L'Iran est le principal. Mais on rappelle aussi que la menace n'est pas figée : en octobre 2013, un rapport de la société américaine Akamai indiquait que, pour la première fois, la Chine ne serait plus la première source d'attaques, détrônée par l'Indonésie (http://www.abc.net.au/news/2013-10-18/an-indonesia-overtakes-china-as-top-source-of-cyber-attack-traf/5032428).

- Un nouveau thème apparaît : celui de la Chine victime des cyberattaques. Les documents de Snowden indiqueraient que la NSA a déjà mené des cyberattaques contre la Chine (http://hackersnewsbulletin.com/2013/08/latest-snowden-leak-reveals-us-hit-231-cyber-attacks-russia-iran-china.html). En août 2013, l'Internet chinois fut victime de la plus importante attaque DDoS (http://www.nextgov.com/cybersecurity/2013/08/who-hacked-chinas-internet-yesterday/69374/) qu'il eut à subir. Plus récemment, en décembre, la banque chinoise Coal Bank (http://www.ehackingnews.com/2013/12/china-coal-bank-website-hacked.html) aurait été piratée par des hackers japonais. Les exemples d'atteintes au cyberespace chinois se multiplient, et la Chine n'hésite pas à s'en faire l'écho.

La Chine n'en reste pas moins omniprésente dans l'actualité de la cybersécurité et de la cyberdéfense

Un examen attentif de l'actualité montre cependant que la Chine est toujours au centre de préoccupations de cybersécurité et cyberdéfense :

- En août 2013, des hackers chinois, peut-être liées à APT1, tombent dans le pot de miel posé par Trend Micro fin 2012 (un faux système de contrôle de distribution d'eau (http://thehackernews.com/2013/08/Chinese-hackers-APT1-honeypot-water-control-system.html)).

- En septembre 2013, est identifié un groupe de hackers chinois, surnommé « Hidden Lynx » (http://in.reuters.com/article/2013/09/17/cyber-attacks-china-idINDEE98G0CN20130917) par la société Symantec. Ce groupe, d'une cinquantaine d'individus, serait lié aux auteurs de l'opération Aurora de 2010.

- Pendant le shutdown américain d'octobre 2013 (le gouvernement américain ayant alors fermé certains de ses services administratifs (http://www.lemonde.fr/ameriques/article/2013/10/01/le-shutdown-americain-a-qui-profite-la-crise_3488045_3222.html)), une cyberattaque attribuée à la

Chine a touc site de la Commission Electorale Fédérale (http://www.breitbart.com/Big-Peace/2013/12/17/Report-Chinese-Hackers-Attacked-FEC-Website) (FEC – Federal Electoral Commission).

- Un rapport de FireEye (décembre 2013) révèle que des hackers chinois auraient espionné la diplomatie européenne au cours des derniers mois, au travers d'une série d'attaques très ciblées contre des ministères. Les chercheurs nomment cette opération « Ke3Chang » (http://www.nytimes.com/2013/12/10/world/asia/china-is-tied-to-spying-on-european-diplomats.html?_r=0). La Chine a démenti (http://news.xinhuanet.com/english/china/2013-12/10/c_132957229.htm) les accusations.

Mais l'un des sujets qui occupera encore partie de l'actualité cyber en 2014, sera celui de la maîtrise des risques que peuvent faire courir pour la sécurité et la défense nationale l'acquisition de matériels d'origine étrangère et l'accès aux marchés nationaux d'entreprises étrangères. Les entreprises chinoises sont au cœur de ces problématiques. Les Etats hésitent dans le traitement de ces défis, entre accès libre aux marchés nationaux, contrôle étroit (voir la décision du Royaume-Uni (http://econflicts.blogspot.fr/2013/12/news-report-on-huawei-cyber-security.html)), limitations, régulation, et interdiction (voir décision australienne (http://www.theregister.co.uk/2013/11/01/australian_confirms_huawei_ban/)) de commerce pour tout ce qui toucherait de près ou de loin aux intérêts, infrastructures (les cœurs de réseau par exemple), services vitaux de la nation. Les Etats hésitent d'autant plus que, si leur posture est légitime, ils ne peuvent trop fermer leurs marchés sous peine de se voir fermés, en retour, l'immense marché chinois.

Daniel Ventre

Daniel Ventre est ingénieur au CNRS (Centre de recherches sociologiques sur le droit et les institutions pénales - CESDIP), titulaire de la Chaire Cybersécurité & Cyberdéfense (Ecoles de Saint-Cyr Coëtquidan - Sogeti - Thales), chargé de cours à Télécom ParisTech. Ses travaux et publications traitent des conflits dans le cyberespace (guerre de l'information, cyberguerre). Il est également directeur de la collection Cyberconflits et cybercriminalité, aux éditions Hermès-Lavoisier.

Auteurs de plusieurs ouvrages sur la question, Daniel Ventre tient également un blog (http://econflicts.blogspot.com).

Daniel Ventre