Des militaires chinois recherchés pour cyberespionnage économique

Daniel Ventre, Titulaire de la Chaire Cyberdéfense et Cybersécurité.

21 mai 2014. Article n° III.14

L'information n'a pas fait les grands titres en France, mais les Etats-Unis viennent de prendre une décision qui fera date dans l'histoire de l'évolution des relations avec la Chine, sur fond de lutte dans le cyberespace. Le 19 mai 2014 le FBI a ajouté à sa liste des personnes recherchées, photos à l'appui[1], les noms de 5 militaires chinois, officiers au sein de l'unité 61398, accusés d'opérations de cyberespionnage industriel contre des entreprises américaines menées depuis 2006.

Les militaires-hackers chinois désignés sont :

- Gu Chunhui (以及顾春晖, Gu Chun Hui, "KandyGoo", Gao Chunhui)[2]. Gu Chunhui aurait été identifié dès la fin des années 1990, et mentionné dans le livre de Scott Henderson (The Dark Visitor[3], 2007, p.12 et 49). Il aurait participé au groupe de hackers Red Hacker Alliance[4].
- Huang Zhenyu (黄镇宇, Huang Zhen Yu, "hzy_lhx")[5]
- Le capitaine Sun Kailiang (孙凯良, Sun Kai Liang, Jack Sun)[6]
- Wang Dong (王东, Jack Wang, "UglyGorilla")[7]. Wang Dong, qui aurait été identifié dès 2004, fut mentionné dans le rapport Mandiant publié en 2013.
- Wen Xinyu (文新宇, Wen Xin Yu, "WinXYHappy", "Win_XY", Lao Wen)[8].

Les six entreprises américaines victimes de ces opérations sont : Westinghouse Electric Co. ; SolarWorld AG ; United States Steel Corp. ; Allegheny Technologies Inc. ; the United Steel, Paper and Forestry, Rubber, Manufacturing, Energy, Allied Industrial and Service Workers International

[1] http://www.fbi.gov/news/news_blog, 19 mai 2014
[2] http://www.fbi.gov/wanted/cyber/gu-chunhui
[3] http://www.lulu.com/items/volume_62/2048000/2048958/4/print/2048958.pdf
[4] http://fmso.leavenworth.army.mil/documents/beijings-rising-hackers.pdf
[5] http://www.fbi.gov/wanted/cyber/huang-zhenyu
[6] http://www.fbi.gov/wanted/cyber/sun-kailiang
[7] http://www.fbi.gov/wanted/cyber/wang-dong
[8] http://www.fbi.gov/wanted/cyber/wen-xinyu

Union ; Alcoa, Inc. Pour une analyse des entreprises victimes, nous renvoyons à la lecture de l'article publié par Jeffrey Carr[9].

31 accusations pèsent sur chacun des 5 accusés (l'intégralité du rapport d'accusation est disponible sur le site du Département de la Justice américain[10]). Les crimes qui leur sont reprochés sont les suivants :

- Tentative de fraude (10 ans de prison) (18 U.S.C. § 1030(b))[11]
- Accès illicite dans des ordinateurs (5 ans de prison) (18 U.S.C. §§ 1030(a)(2)(C), 1030(c)(2)(B)(i)-(iii), and 2.)[12]
- Diffusion de malware (10 ans) (18 U.S.C. §§ 1030(a)(5)(A), 1030(c)(4)(B), and 2.)[13]
- Usurpation d'identité (2 ans) (18 U.S.C. §§ 1028A(a)(1), (b), (c)(4), and 2)[14]
- Espionnage économique (15 ans) (18 U.S.C. §§ 1831(a)(2), (a)(4), and 2.)[15]
- Vol de secret industriel (10 ans) (18 U.S.C. §§ 1832(a)(2), (a)(4), and 2.)[16]

(Pour une lecture analytique de ces textes de loi, voir l'ouvrage: *Prosecuting Computer Crimes*, Department of Justice, 2010, 213 pages)[17]

Les raisons, motivations et effets attendus d'une telle procédure, du point de vue américain, sont multiples.

- Lors d'une conférence de presse, le procureur Holder a estimé que les opérations menées par les hackers militaires chinois méritaient une réaction appropriée de la part de la justice américaine. Pour les Etats-Unis, la compétition internationale doit uniquement reposer sur les capacités d'innovation des entreprises et non s'appuyer sur la capacité des gouvernements à voler des secrets industriels. Selon James B. Comey, Directeur du FBI, le gouvernement chinois depuis trop longtemps pratique le cyberespionnage dans le but d'aider ses entreprises à obtenir un avantage économique.

- La décision prise de poursuivre des généraux chinois repose donc officiellement sur cette distinction entre pratiques acceptables (l'espionnage politique, étatique, militaire, l'espionnage légitime et licite comme celui qui a pour objectif officiel la lutte contre le terrorisme par exemple) et non-acceptables (le cyberespionnage économique qui déséquilibre la compétition économique mondiale). Il n'est pas question de l'identité des cibles de l'espionnage, mais bien de le distinguer en fonction de ses finalités. Pour les américains l'espionnage des entreprises reste donc possible, tant qu'il n'est pas motivé par une finalité économique.

- Il est évident que la procédure, sur le plan juridique, a peu voire aucune chance d'aboutir[18] à la remise aux autorités américaines des militaires recherchés, et donc à plus forte raison à leur jugement. Il est également évident que cette procédure a peu de chances de limiter, concrètement, les pratiques chinoises (les pratiques reprochées à la NSA ont-elles d'ailleurs cessé, face à leur dénonciation par plusieurs gouvernements suite aux révélations d'E. Snowden?).

[9] http://jeffreycarr.blogspot.fr/2014/05/analysis-of-victim-companies-in-pla.html
[10] http://www.justice.gov/iso/opa/resources/5122014519132358461949.pdf
[11] http://www.law.cornell.edu/uscode/text/18/1030
[12] http://www.law.cornell.edu/uscode/text/18/1030
[13] http://www.law.cornell.edu/uscode/text/18/1030
[14] http://www.law.cornell.edu/uscode/text/18/1028A
[15] http://www.law.cornell.edu/uscode/text/18/1831
[16] http://www.law.cornell.edu/uscode/text/18/1832
[17] http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf
[18] http://www.lawfareblog.com/2014/05/why-did-doj-indict-the-chinese-military-officers/

- La justice américaine étant saisie, les cyberattaques relèvent du droit pénal, de la criminalité ordinaire dirions-nous. Il n'est pas question de "cyberguerre", d'usage de la force, ni d'espionnage militaire. Les Etats-Unis semblent dire "à méthodes de voyous, traitement de voyous" et cela peu importe que les coupables identifiés soient des militaires agissant dans le cadre de leurs fonctions, ou de simples citoyens. Voici donc l'image de ces militaires placardée sur les pages du FBI au même rang que des criminels en col blanc, des assassins, des terroristes. Il y a dans cette démarche la volonté évidente d'affecter l'image de ces militaires, et au-delà bien sûr de la Chine. Mais ce choix est-il le meilleur, le plus efficace? Pourquoi n'avoir pas plutôt choisi de porter l'affaire devant les juridictions de l'Organisation Mondiale du Commerce[19] (en invoquant plus spécialement les TRIPS Agreement (Trade Related-Aspects of Intellectual Property Rights) qui proposent des recours spécifiques pour le vol de propriété intellectuelle ? Pourquoi les Etats-Unis n'ont-ils jamais adressé une requête auprès de l'OMC alors qu'ils dénoncent depuis plusieurs années ces atteintes à la propriété intellectuelle et les agissements spécifiques de la Chine (voir par exemple le rapport Cox[20] de 1999 relatif au commerce avec la Chine et les enjeux de sécurité nationale)?

- Les Etats-Unis démontrent qu'ils disposent de capacités de renseignement autorisant une identification très précise des auteurs des cyber-opérations. L'attribution est possible. Le FBI a publié des détails sur les méthodes utilisées par les hackers, ce qui pour certains est une révélation de nature à dissuader ces attaquants: *"This will scare the PLA hackers, at least for a few months, while they try to find out how they were detected."*[21]

- C'est la première fois que l'on met un visage sur la cybermenace chinoise. Jusque-là elle était dans le discours, à la fois concrète (pour ceux qui l'affrontent sur les réseaux) et abstraite. Forts de cette capacité d'attribution, d'identification, les Etats-Unis démontrent qu'ils ont à la fois les moyens et la volonté de remonter la trace de leurs agresseurs.

- Cette procédure prend les autorités chinoises au pied de la lettre, à savoir leur apporter les preuves de l'implication de l'armée dans les opérations de cyberespionnage : « In the past, when we brought concerns such as these to Chinese government officials, they responded by publicly challenging us to provide hard evidence of their hacking that could stand up in court. »[22]

La Chine réagit et avance ses arguments

- Au travers du porte-parole du Ministère des affaires étrangères[23], estimant que les accusations sont montées de toutes pièces ; qualifiant la procédure américaine de violation des normes élémentaires des relations internationales ; déplorant la dégradation des relations sino-américaines et le coup porté à la confiance ; réitérant la détermination de la Chine à lutter contre les menaces à la cybersécurité ; et réaffirmant que jamais la Chine ne s'est livrée à de l'espionnage industriel et économique ;

- Du point de vue chinois, on rappelle que, depuis les révélations d'E. Snowden, il est notoire que ce sont les Etats-Unis qui espionnent les puissances étrangères. Les Etats-Unis ont espionné la Chine en s'introduisant dans les réseaux de ses administrations, armées, entreprises. La Chine a demandé des explications à Washington et l'arrêt de ces pratiques.

[19] http://www.defenceiq.com/cyber-defence/articles/china-cyber-charges-take-beijing-to-the-wto-instea/
[20] http://www.house.gov/coxreport/
[21] http://fortunascorner.com/2014/05/21/indictment-of-china-military-hackers-reveals-new-details-of-cyber-attack-methods/
[22] http://www.justice.gov/nsd/opa/pr/speeches/2014/nsd-speech-140519.html
[23] http://news.takungpao.com/world/exclusive/2014-05/2484977.html

- Face à ce qu'elle considère comme un manque de sincérité dans le dialogue amorcé avec les Etats-Unis sur la cybersécurité, la Chine a décidé de suspendre les activités du groupe de travail (Sino-US Network Working Group) qui avait été mis en place pour dialoguer sur les enjeux de cybersécurité.

- Des mesures sont possibles contre les entreprises américaines présentes sur le territoire chinois ou commerçant avec la Chine, et peut-être à commencer par les 6 entreprises américaines citées dans la procédure.

Plus largement, ce sont les relations diplomatiques, économiques, politiques, culturelles sino-américaines qui s'en trouveront perturbées. Imaginons qu'un Etat prenne l'initiative d'engager des poursuites pénales contre le directeur de la CIA ou la patron de la NSA et de ses agents et affiche sur l'un de ses sites officiels un avis de recherche similaire. Quelle seraient les réactions de l'Amérique: les relations s'en trouveraient-elles améliorées? Le comportement des autorités américaines serait-il encouragé à changer? Probablement non.

Dans cet engagement politique entre les Etats-Unis et la Chine, quelle peut être, quelle doit être, la posture des pays tiers: doit-on considérer cela comme un duel strictement sino-américain (qui ne se terminera pas avec ce bras de fer judiciaro-politique), duquel il serait préférable de rester éloigné, ou bien faut-il prendre position pour l'un ou l'autre?

L'efficacité de l'accusation portée par l'Amérique est largement diminuée depuis les révélations d'E. Snowden. Il est plus difficile d'accuser les autres, quand on pratique de même. La distinction que tentent d'établir les Etats-Unis entre le cyberespionnage acceptable et celui qui ne l'est pas, ne leurre personne. La puissance du discours américain souffre donc à la fois des révélations d'E. Snowden et des pratiques de l'Etat dans le cyberespace; quant aux entreprises américaines, elles continueront de souffrir du cyberespionnage étranger, contre lequel les institutions américaines ne peuvent plus lutter efficacement, et éventuellement des mesures de représailles qui seront prises par Pékin à leur encontre suite à cette récente mise en accusation.

Rappelons enfin que la Chine connaît actuellement une campagne de lutte anti-corruption, qui se traduit par la mise en accusation et le jugement de hauts dirigeants politiques, industriels... (dernière condamnation en date, celle de l'homme d'affaires Liu Han)[24]. Les citoyens chinois sont aujourd'hui familiers de ce processus de criminalisation des agissements de leurs élites. La différence est de taille dans ce cas précis, car la mise au pilori de membres de leurs élites émane de l'étranger. On ne peut exclure une relation étroite entre cyberespionnage économique et corruption. Profitons également de cette analyse pour rappeler que la Chine ne construit pas son rattrapage économique à seuls coups de vols de données sensibles et de secrets; elle le fait en s'appuyant sur son propre potentiel d'ingénieurs, de créateurs, d'innovateurs, d'entrepreneurs. Et à la limite cela est encore plus inquiétant pour la compétitivité des entreprises occidentales, américaines ou autres, car il n'y a guère de parade pour freiner ce développement-là.

[24] https://fr.news.yahoo.com/un-proche-lex-chef-la-s%C3%A9curit%C3%A9-condamn%C3%A9-%C3%A0-055727655.html