Une analyse du rapport Mandiant

Daniel Ventre, CNRS (CESDIP/GERN),
Chaire Cyber Sécurité et Cyber défense (Saint-Cyr, Sogeti, Thales)

Juillet 2013 – article n°IV.1

Agences de renseignement, polices, industriels, chercheurs universitaires, se livrent à des enquêtes et à des analyses techniques, pour comprendre les modes opératoires des auteurs des cyberattaques mais aussi tenter d'apporter les preuves qui permettraient d'identifier ces derniers.
Certains investigateurs, étatiques en particulier, ne partageront jamais publiquement leurs résultats, ou se contenteront de quelques déclarations publiques désignant les menaces ; d'autres à l'image des chercheurs universitaires, de projets coopératifs internationaux ou d'industriels de la sécurité, publieront au contraire dans le détail les résultats de leurs enquêtes.
Le rapport produit par l'entreprise américaine Mandiant en février 2013 trouve place dans cette catégorie de travaux. Mais selon nous, son intérêt ne réside pas tant dans la nature des informations qu'il délivre sur la menace militaire chinoise que dans le regard qu'il nous permet de porter sur le processus de construction du discours sécuritaire (le rapport contribue-t-il à modifier ou non les perceptions de la réalité, la définition de la menace ? ; comment le rapport s'insère-t-il dans le contexte politique ou économique ?; quelle reconnaissance ou publicité confère-t-il aux « experts » qui le produisent ?)

I – Le contexte

Publié en février 2013, le rapport *APT1: Exposing One of China's Cyber Espionage Units*[1] affirme apporter les preuves de l'existence de groupes militaires chinois spécialisés dans les opérations de cyber espionnage visant tout particulièrement les Etats-Unis. L'enquête, analysant 150 incidents observés sur une période de 7 années, a permis de reconstruire le profil de l'unité 61398 dépendant du 2ème bureau de l'armée, 3ème Département, localisée près de Shanghai. Outre ce groupe, les auteurs du rapport prétendent en observer plusieurs dizaines d'autres répartis dans le monde, une vingtaine d'entre eux en Chine.

1.1. Un rapport… de plus ?

Le rapport, loin d'être un travail isolé, s'inscrit aussi dans le droit prolongement d'un ensemble de travaux sur la Chine publiés depuis les années 1990 aux Etats-Unis principalement. Ces publications portent essentiellement sur deux objets :

- Le monde des hackers : cyber espionnage, cyber criminalité, opérations d'origine militaire, hackers patriotes/nationalistes, hacktivistes qui sévissent sur les réseaux depuis les années 1990.
- L'armée chinoise et son intérêt manifeste pour la guerre de l'information, la maîtrise de l'espace informationnel (et du cyberespace), l'informatisation des forces (plus exactement la

[1] Mandiant, *APT1: Exposing One of China's Cyber Espionage Units*, 76 pages, février 2013, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

notion d'*informationization*, recouvrant l'informatisation des systèmes d'armes mais aussi la prise en compte des opérations dans le cyberespace)

Au rang des nombreuses publications anglo-saxonnes traitant de ces sujets, rappelons les plus significatives. Nous trouvons les travaux[2] de James Mulvenon (1999)[3], Toshi Yoshihara (2001)[4], Nina Hachigan (2001)[5], Timothy L. Thomas (2001[6], 2004[7], 2006[8], 2007[9], 2009[10]), Ken Dunham et Jim Melnick (2006)[11], Brian Mazanec (2008)[12], Ron Deibert et Rafal Rohozinski (2009)[13], Bryan Krekel et George Bakos[14], Jeffrey Carr (2009) [15], R. A. Clarke et R. Knake (2010) [16], Elisabette M. Marvel (2010) [17], Martin Libicki (2011)[18], Dmitri Alperovitch (2011)[19], Venusto Abellera (2011) [20], C. Paschal

---

[2] Il s'agit là d'une sélection (et non d'une liste exhaustive) d'ouvrages, rapports techniques d'analyses d'incidents, documents étatiques traitant de la « cybermenace » chinoise (cyberespionnage, hacktivisme, capacités militaires, stratégies militaires). Nous ne prenons pas en compte dans cet inventaire sommaire les travaux académiques publiés dans des revues scientifiques, les articles publiés dans les revues militaires, ni les rapports de mémoires de mastères ou thèses qui peuvent être produits dans les différentes institutions académiques et universités de défense.

[3] James Mulvenon, *The PLA and Information Warfare*, in James Mulvenon, Richard H. Yang (Eds.), *The People's Liberation Army in the Information Age*, 297 pages, 1999, RAND Corporation, Washington, Etats-Unis, pp.175-186, Actes de la conférence tenue à San Diego, Californie, 9-12 Juillet 1998, http://www.rand.org/content/dam/rand/pubs/conf_proceedings/CF145/CF145.chap9.pdf ; http://www.rand.org/pubs/conf_proceedings/CF145.html

[4] Toshi Yoshihara, *Chinese Information Warfare: a phantom menace or emerging threat?* Strategic Studies Institute, Novembre 2001, 41 pages, http://www.au.af.mil/au/awc/awcgate/ssi/chininfo.pdf

[5] Nina Hachigan, *China's Cyber-Strategy*, Foreign Affairs 80, n° 2, 2001, pp.118-133

[6] Timothy L. Thomas, *The Internet in China: Civilian and Military Uses*, Information & Security, An International Journal , Volume 7, 2001, pages 159-173

[7] Timothy L. Thomas, *Dragon Bytes: Chinese information war theory and practice*, Foreign Military Studies Office, 2004, 168 pages, Etats-Unis; http://www.ists.dartmouth.edu/events/abstract-TimThomas.html

[8] Timothy L. Thomas, *Cyber Silhouettes: Shadows Over Information Operations*, Foreign Military Studies Office, 334 pages, Etats-Unis

[9] Timothy L. Thomas, *Decoding The Virtual Dragon - Critical Evolutions In The Science And Philosophy Of China's Information Operations And Military Strategy - The Art Of War And IW*, Foreign Military Studies Office (FMSO), Etats-Unis, 2007

[10] Timothy L. Thomas, *Cyber Silhouettes: Shadows Over Information Operations*, Foreign Military Studies Office (FMSO), Fort Leavenworth, KS, Etats-Unis, 2009, 298 pages

[11] Ken Dunham, Jim Melnick, *'Wicked Rose' and the NCPH Hacking Group*, VeriSign iDefense, 2006

[12] Brian Mazanec, *Cyberwarfare as an Element of PRC National Power and its Implications for U.S. National Security*, Brian Mazanec Pub., Amazon Digital Services, 113 pages, décembre 2008

[13] Ron Deibert, Rafal Rohozinski, *Tracking GhostNet: Investigating a Cyber Espionage Network*, SecDev Group & University of Toronto, Munk Centre for International Studies, 29 mars 2009, Canada, 53 pages, http://www.nartv.org/mirror/ghostnet.pdf

[14] - Bryan Krekel, George Bakos, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, Northrop Grumman Corp, prepared for the US-China Economic and Security Review Commission, 9 Octobre 2009, 61 pages, Etats-Unis, http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf

- Bryan Krekel, Patton Adams, George Bakos, *Occupying the information high-ground; Chinese capabilities for computer network operations and cyber-espionage*, Prepared for the U.S.-China Economic and Security Review Commission by Northrop Grumman Corp, 7 mars 2012, 136 pages, Etats-Unis, http://origin.www.uscc.gov/sites/default/files/Research/USCC_Report_Chinese_Capabilities_for_Computer_Network_Operations_and_Cyber_%20Espionage.pdf

[15] Jeffrey Carr, *Inside Cyber Warfare : mapping the cyber underworld*, O'Reilly Media, Etats-Unis, décembre 2009, 240 pages

[16] R. A. Clarke, R. Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, Ecco Publisher, Etats-Unis, avril 2010, 320 pages

[17] Elisabette M. Marvel, *China's Cyberwarfare Capability*, 105 pages, Nova Science Pub Inc, 31 octobre 2010

[18] Martin Libicki, *Chinese use if cyberwar as an anti-access strategy*, Témoignage présenté devant l' U.S. China Economic and Security Review Commission, 27 janvier 2011, Publication Rand corporation, 6 pages, http://www.rand.org/content/dam/rand/pubs/testimonies/2011/RAND_CT355.pdf

Eze (2011) [21], Mark A. Stokes, Jenny Lin et L.C. Russell Hsiao (2011)[22], William T. Hagestad (2012)[23], Dennis F. Poindexter (2013). Rappelons également l'existence des rapports annuels[24] du Département de la défense américain sur le développement de la puissance militaire chinoise, qui accordent toujours une place aux questions de la guerre de l'information et du cyberespace (rapports publiés depuis l'année 2000), des rapports au Congrès de *l'U.S.-China Economic and Security Review* Commission (publiées annuellement depuis juillet 2002)[25], des travaux de *l'USCC Research Staff* (2011) [26], de la *United States House of Representatives* (2011)[27], de l'Office of the *National Counterintelligence Executive* (2011)[28] ou encore de la *National Intelligence Agency* américaine (rapport classifié 2013)[29].

Une troisième approche s'intéresse plus particulièrement aux transformations sociales, politiques, économiques, induites par l'introduction des réseaux en Chine: capacités d'expression citoyenne, influence étrangère, surveillance et contrôle étatique sur les populations, utilisation des réseaux sociaux (Xu Wu 2007[30] ; Yongnian Zheng 2007[31] ; Rebecca Fannin 2008[32] ; Sherman So et J. Christopher Westland 2009[33] ; Wang Jun 2011[34] ; Guobin Yang 2011[35] ; Lennon Yao-chung Chang 2013[36]…)

---

[19] Dmitri Alperovitch, *Revealed: Operation Shady RAT*, McAfee, 2011, http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf.

[20] Venusto Abellera, *Exploring China's Use of Known Cyber Capabilities in the Intrusions of United States Public Sector Networks*, ProQuest, UMI Dissertation Publishing, 124 pages, septembre 2011

[21] C. Paschal Eze, *Cyber Coexistence Code: Whither U.S.-China Cyber Cold War?*, Global Mark Makers, 29 pages, octobre 2011

[22] Mark A. Stokes, Jenny Lin and L.C. Russell Hsiao, *The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure*, Project2049, 11 novembre 2011, 32 pages, http://project2049.net/documents/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf

[23] William T. Hagestad, *21st Century Chinese Cyberwarfare*, IT Governance Publishing, Cambridge, Royaume-Uni, 314 pages, 1° mars 2012

[24] Department of Defense, Etats-Unis, *Annual Report to Congress. Military Power of the People's Republic of China*, 2000 et suiv.

[25] Loi de l'année 2000. Dernier rapport en date de novembre 2012

[26] USCC Research Staff, *The National Security Implications of Investments and Products from the People's Republic of China in the Telecommunications Sector*, 104 pages, janvier 2011, CreateSpace Independent Publishing Platform

[27] United States House of Representatives, *Communist Chinese Cyber-Attacks, Cyber-Espionage and Theft of American Technology*, Etats-Unis, 30 juin 2011, 91 pages, Kindle Edition disponible à l'adresse: http://www.amazon.com/Communist-Cyber-Attacks-Cyber-Espionage-Technology-ebook/dp/B005966LG2/ref=sr_1_7?s=books&ie=UTF8&qid=1364229259&sr=1-7&keywords=cyber+china

[28] Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace*, Octobre 2011, 31 pages, Etats-Unis, http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf

[29] Le rapport confirmerait que la Chine est la principale cybermenace. L'existence du document est évoquée dans des articles de presse. Exemple : Stacy Curtin, China is America #1 Cyber Threat: U.S. Govt. Report, 11 février 2013, http://finance.yahoo.com/blogs/daily-ticker/china-america-1-cyber-threat-u-govt-report-150621517.html

[30] Xu Wu, *Chinese Cyber Nationalism: Evolution, Characteristics, and Implications*, Lexington Books, Etats-Unis, 2007, 280 pages

[31] Yongnian Zheng, *Technological Empowerment: The Internet, State, and Society in China*, Stanford University Press, Etats-Unis, Novembre 2007, 272 pages

[32] Rebecca Fannin, *Silicon Dragon: How China Is Winning the Tech Race*, McGraw-Hill, janvier 2008, 300 pages

[33] Sherman So, J. Christopher Westland, *Red Wired: China's Internet Revolution*, Marshall Cavendish Limited, Novembre 2009, 256 pages

[34] Wang Jun, *Cyber Nationalism and China's Foreign Affairs*, China Social Sciences Press, janvier 2011, 299 pages

[35] Guobin Yang, *The Power of the Internet in China: Citizen Activism Online*, Columbia University Press, 320 pages, 2011

[36] Lennon Yao-chung Chang, *Cybercrime in the Greater China Region: Regulatory Responses and Crime Prevention Across the Taiwan Strait*, Edward Elgar Pub, janvier 2013, 272 pages

Toute la littérature produite sur les capacités de cyberguerre et guerre de l'information chinoise dresse depuis les années 1990 le portrait d'une nation inquiétante, agressive, disposant de capacités inépuisables (car lorsqu'il ne s'agit pas des menaces que représentent les acteurs étatiques eux-mêmes, il est question des cybercriminels ou encore des millions de citoyens mus en hackers nationalistes, constituant autant de menaces pour le reste de la planète en raison de leurs compétences et de leurs motivations), d'une nation aux stratégies de défense opaques[37], dont la démarche actuelle d'attaques dans l'espace informationnel trouverait racine dans une pratique guerrière séculaire (l'art de la guerre de Sun Tzu, la guerre irrégulière de Mao), s'appuierait sur l'existence de forces de techno-guerriers constituées dès la guerre froide[38] et traduirait la volonté de la Chine de s'imposer comme une alternative à la puissance hégémonique américaine, remettant ainsi en cause l'ordre international établi à la fin de la guerre froide. Face à elle l'Amérique et l'ensemble du monde industrialisé se trouveraient en état de vulnérabilité, d'infériorité (R. Clarke[39]; Joel Brenner[40]) en raison de leur dépendance au cyberespace, du nombre d'adversaires potentiels, de la motivation de ces derniers, et n'auraient alors d'autre solution que de se préparer à la confrontation en cherchant à rattraper leur retard en termes de capacités, défensives et offensives[41]. Un discours alarmiste, qui prend racine dans les prédictions de la décennie 1990-2000 annonçant un Cyber Pearl Harbor et autres chaos cybernétiques, a pris place au sein de la classe politique (le sénateur républicain américain Mike Rogers déclare ainsi que les Etats-Unis sont en train de perdre la cyberguerre contre la Chine)[42].

1.3. Le discours des militaires

Soulignons d'autre part que le thème de la cybermenace chinoise est souvent traité par les militaires, ou d'anciens militaires : Thimothy L. Thomas[43], Scott J. Henderson[44], Rich Barger[45], Mark. A. Stokes[46], William T. Hagestad[47] sont de ceux-là[48]. En raison du profil d'une partie de ses dirigeants, on

---

[37] - Richard Halloran, *The Opacity of China's Military*, The Washington Times (Washington, DC), 10 mars 2009
- Kristopher Harrison, *Why China's economic opacity is a serious problem*, Foreign Policy, 10 juillet 2012, http://shadow.foreignpolicy.com/posts/2012/07/10/why_chinas_economic_opacity_is_a_serious_problem
- Kerry B. Collison, *Opacity the heart of China's PLA strategy,* 10 juin 2010, http://kerrycollison.blogspot.fr/2010/06/opacity-heart-of-chinas-pla-strategy.html
- Office of the Secretary of Defense, *Annual Report to Congress, Military Power of the People's Republic of China, 2008*, Etats-Unis, 66 pages, p.I, http://www.defense.gov/pubs/pdfs/China_Military_Report_08.pdf

[38] Evan Feigenbaum, *China's Techno-Warriors: National Security and Strategic Competition from the Nuclear to the Information Age*, Stanford University Press, Stanford, Etats-Unis, avril 2003, 360 pages

[39] R. A. Clarke, R. Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, Ecco Publisher, Etats-Unis, avril 2010, 320 pages

[40] Joel Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*, The Penguin Press HC, Etats-Unis, septembre 2011, 320 pages. J. Brenner fut conseiller juridique pour les questions de cybersécurité au sein de la NSA (Etats-Unis).

[41] Defense Science Board, *Resilient Military Systems and the advanced cyber threat*, Department of Defense, Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, Washington DC, 20301-3140, Etats-Unis, janvier 2013, 146 pages, http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf

[42] Mike Rogers, *America is losing the cyber war vs. China*, 8 février 2013, http://www.detroitnews.com/article/20130208/OPINION01/302080328/1007/OPINION/Rogers-America-losing-cyber-war-vs-China

[43] Le lieutenant colonel Thimothy L. Thomas, fut analyste au FMSO (Foreign Military Studies Office), à Fort Leavenworth (Kansas, Etats-Unis), directeur de l'USARI, Soviet Studies - United States Army Russian Institute (USARI), à Garmisch en Allemagne.

[44] Scott J. Henderson, ancien officier (analyste) de l'U.S. Army, qui a écrit le livre The Dark Visitor et alimenté le célèbre site internet éponyme, qui se focalisait sur les activités des hackers chinois.

[45] Rich Barger, responsable des questions de renseignement à Cyber Squared, a exercé au sein de l'U.S. Army (1st Information Operations Command). Sur le site de Cyber Squared, mention est faite de l'existence de plusieurs groupes APT qui font l'objet d'une analyse de la part de l'entreprise. http://www.cybersquared.com/just-the-tip-of-the-iceberg/

[46] Membre du Project2049, co-auteur du rapport *The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure*, M. A. Stokes a servi pendant 20 ans dans l'U.S. Air Force.

[47] U.S. Marine Lieutenant colonel

peut considérer que les publications de l'entreprise Mandiant s'inscrivent dans cette catégorie. En effet, avant de fonder l'entreprise en 2004, Kevin Mandia exerça au sein du 7th Communication Group (Pentagone), travailla comme agent spécial à l'AFOSI (U.S. Air Force Office of Special Investigations). Travis Reese et Dave Merkel, tous deux membres du CEO de l'entreprise, sont eux aussi d'anciens membres de l'AFOSI. Richard Bejtlich, également membre du CEO de Mandiant, auteur du site Tao Security[49], fut quant à lui officier de renseignement au sein de l'U.S. Air Force CERT ainsi que de l'Air Force Information Warfare Center (AFIWC) et de l'Air Intelligence Agency (AIA).

1.4. Le contexte politique

Le rapport est publié alors que les autorités américaines sont engagées dans une politique de durcissement de leurs positions en matière de cyberdéfense : annonce du renforcement des effectifs du CyberCommand[50], discours du secrétaire à la défense américain sur la nécessité de protéger la nation contre les cyberattaques[51], *executive order on cybersecurity* du Président B. Obama[52], dialogues au plus haut niveau entre les Etats-Unis et la Chine sur la question de la cybersécurité[53], durcissement du cadre juridique de la cyberguerre[54].

1.5. Le contexte économique

Enfin, le rapport trouve place dans un contexte économique particulier, extrêmement favorable au marché de la cybersécurité (le chiffre d'affaire de Mandiant pour l'année 2012, dépassant les 100 millions de $ US, aurait cru de 76% par rapport à l'année précédente)[55]. L'initiative masquerait mal la démarche commerciale de l'entreprise : « voyez l'entreprise qui tire profits du piratage chinois »[56]. Les conclusions que propose le rapport pourraient alors ne pas être aussi objectives qu'il n'y paraît, ne décriraient pas la réalité, mais seulement un versant de la réalité, la perspective choisie l'étant dans un but commercial voire politique. Ces remarques nous amènent à considérer l'ensemble des critiques qui ont été formulées à l'encontre du rapport et les enseignements que l'on peut en tirer.

---

[48] En Chine, c'est aussi de militaires qu'émane la publication majeure qui a profondément marqué la perception occidentale des ambitions et intentions de ce pays au cours des années 2000 : le fameux Unrestricted Warfare, des colonels Liang Qiao et Wang Xiangsui. Cette publication a probablement bien davantage marqué les esprits occidentaux que les travaux pourtant tout aussi essentiels sur la guerre de l'information produits par d'autres militaires chinois (Wang Baocun, Dai Qingmin ou Wang Pufeng) dès les années 1990, mais demeurés plus confidentiels en raison de leur nature plus conceptuelle-théorique et de la barrière linguistique. Liang Qiao, Wang Xiangsui, *Unrestricted Warfare*, Beijing: PLA Literature and Arts Publishing House, février 1999, 228 pages, http://www.cryptome.org/cuw.htm

[49] http://taosecurity.blogspot.fr/

[50] Elisabeth Bumiller, *Pentagon Expanding Cybersecurity Force to Protect Networks Against Attacks*, The New York Times, 27 janvier 2013, http://www.nytimes.com/2013/01/28/us/pentagon-to-beef-up-cybersecurity-force-to-counter-attacks.html?_r=0

[51] Leon A. Panetta, *Defending the Nation from Cyber Attack*, Discours du secrétaire à la défense, New York, Etats-Unis, 12 octobre 2012, http://www.defense.gov/speeches/speech.aspx?speechid=1728

[52] White House, *Executive order on cybersecurity*, Etats-Unis, 12 février 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[53] Steve Holland, *Obama, China's Xi discuss cybersecurity dispute in phone call*, 14 mars 2013, Reuters, http://www.reuters.com/article/2013/03/14/us-usa-china-obama-call-idUSBRE92D11G20130314

[54] Michael N. Schmitt (US Naval War College), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, avril 2013, 300 pages

[55] Brad Stone, Michael Riley, *Mandiant, the Go-To Security Firm for Cyber-Espionage Attac*k, BloomberBusinessWeek, 7 février 2013, http://www.businessweek.com/articles/2013-02-07/mandiant-the-go-to-security-firm-for-cyber-espionage-attacks#p2

[56] Matthew Yglesias, *Meet the Company That's Profiting From Chinese Hacking*, 19 février 2013, Slate.com, http://www.slate.com/blogs/moneybox/2013/02/19/mandiant_is_the_big_winner_from_increased_anxiety_about_chinese_hacking.html

II – Critiques et enseignements à tirer du rapport

2.1. Les critiques

Les critiques sont venues de la Chine, sur la base d'arguments bien rodés. Le porte parole du ministère des affaires étrangères s'est exprimé, pointant du doigt la manière dont les Etats-Unis accusent de manière récurrente leur pays, estimant qu'une telle approche n'aidera pas à solutionner le problème de la cybercriminalité ; que seule la coopération internationale en matière de lutte anti cybercriminalité devrait être envisagée ; que la Chine est elle aussi l'une des principales victimes des cyberattaques ; que les Etats-Unis sont la source n°1 de ces attaques si l'on se fie uniquement à l'analyse des adresses IP; que la législation, renforcée ces dernières années, et la politique chinoise sont hostiles à de telles pratiques ; que sur la scène internationale la Chine, conjointement avec la Russie et quelques autres pays, a proposé un code de bonne conduite jusqu'alors refusé par les Etats-Unis ; enfin le porte-parole s'étonne qu'il soit possible techniquement d'attribuer et localiser de manière aussi précise des agresseurs, car l'on sait bien que ces derniers ont l'habitude d'anonymiser leurs opérations.[57]

Mais d'autres critiques sont venues des Etats-Unis[58], notamment de l'expert Jeffrey Carr, reprochant tout d'abord les nombreuses erreurs qui jalonnent le dossier, puis une méthodologie insatisfaisante. Ainsi souligne-t-il :

- Les erreurs faites dans les noms de lieux, dans la localisation des acteurs identifiés, la principale faute consistant à localiser le district de Hebei à Shanghai.
- Le parti pris des auteurs. Il semblerait que ces derniers refusent de voir d'autres coupables possibles que les chinois et plus spécifiquement encore que les espions de l'unité 61398. A cet égard, Jeffrey Carr reproche à l'entreprise de n'avoir pas validé son hypothèse (l'origine chinoise des attaques ; l'identité militaire des agresseurs ; implication de l'unité 61398) en envisageant suffisamment de scénarios alternatifs. Il eut suffit pour cela d'appliquer par exemple les méthodes utilisées par les agences de renseignement américaines (ACH - Analysis of Competing Hypotheses). Ne l'avoir pas fait fragilise les conclusions, les exposant à la critique. L'entreprise aura succombé à la facilité, cherchant à satisfaire ses convictions, ses intuitions, quitte à manquer d'objectivité.
- L'absence de définitions précises (qu'est-ce qu'une APT dans la perspective du rapport : s'agit-il d'un processus, ou de l'identité des agresseurs)

Ces critiques remettent en question la qualité même du document, la validité des conclusions, l'impartialité des auteurs.

Une autre critique porte sur l'inutile prise de risque. Avoir révélé des informations sur les capacités d'enquête déployées va inévitablement entraîner les agresseurs à modifier leurs comportements, ce qui est de nature à fragiliser temporairement du moins la sécurité[59]. L'entreprise fait d'ailleurs son autocritique à ce sujet en expliquant son choix dans les pages mêmes du rapport : la divulgation de la vérité méritait cette prise de risque…

2.2. Les enseignements

---

[57] *China opposes hacking allegations: FM spokesman*, XinhuaNet, 19 février 2013, http://news.xinhuanet.com/english/china/2013-02/19/c_132178666.htm

[58] - Jeffrey Carr, *Mandiant APT1 Report Has Critical Analytic Flaws*, 19 février 2013, http://jeffreycarr.blogspot.fr/2013/02/mandiant-apt1-report-has-critical.html#!/2013/02/mandiant-apt1-report-has-critical.html

- Jeffrey Carr, *More on Mandiant's APT1 Report: Guilt by Proximity and Wright Patterson AFB* , 22 février 2013, http://jeffreycarr.blogspot.fr/2013/02/mandiant-apt1-report-has-critical.html#!/2013/02/more-on-mandiants-apt1-report-guilt-by.html

[59] Ellyne Phneah, Embarassing China with reports won't aid security, ZDnet, 27 février 2013, http://www.zdnet.com/cn/embarrassing-china-with-reports-wont-aid-security-7000011886/?s_cid=e305

S'il n'apporte pas véritablement d'information nouvelle[60], échouant à prouver l'identité des agresseurs, **le rapport contribue néanmoins à sa manière au discours alarmiste**, conforte la ligne de pensée développée depuis plus de 15 ans: il insiste sur la dangerosité des opérations menées par l'unité de renseignement chinoise, confirme l'existence d'unités de techno-guerriers (des espions high-tech à l'image de ceux dont dispose l'Amérique), met en exergue la vulnérabilité des acteurs américains (en rappelant le nombre d'incidents recensés et la relative aisance avec laquelle les agresseurs mènent leurs opérations d'espionnage). Les « experts » que sont les membres de l'entreprise véhiculent le même discours anxiogène, preuves à l'appui. Et bien sûr, ils proposent (tel est leur commerce) les solutions pour se prémunir de ces menaces.

Le processus de sécuritisation[61] consiste à désigner la menace (la Chine, ses actions via le cyberespace) ; nommer les objets référents (les infrastructures critiques, les entreprises, la stabilité de l'Etat-nation, la civilisation occidentale, la démocratie, le libéralisme, le cyberespace) ; vient alors la sécurisation, qui propose les solutions (des politiques de cyberdéfense, l'accroissement des moyens défensifs et agressifs, des règles de surveillance et de contrôle accru, des solutions commerciales).
Dans ce processus, l'entreprise de cybersécurité s'inscrit comme l'un des acteurs, aux côtés de l'Etat, susceptible non seulement de fournir des solutions aux problèmes identifiés (assurer la protection contre la menace) mais aussi de désigner et décrire la menace. **Sa responsabilité est grande dans le processus de définition de la menace**. Le rapport et les critiques dont il fait l'objet démontrent une fois de plus que, malgré les effets d'annonce, il est toujours possible de remettre en cause les résultats, proposer d'autres hypothèses tout aussi crédibles. La problématique de l'attribution n'est pas résolue. Toutefois, partant de résultats incertains et de conclusions discutables, la démarche n'en participe pas moins de la définition d'une menace et de la (re)construction d'une réalité, qui peuvent avoir un impact non seulement d'un point de vue marchand (ouvrir de nouveaux marchés de l'(in)sécurité) mais aussi politique (influencer la perception du monde que peuvent avoir les décideurs politiques.

Conclusion

On voit donc s'élever aux Etats-Unis quelques rares voix critiques, les unes appelant à plus d'objectivité et de discernement dans l'analyse des menaces (J. Carr et les divers commentateurs de son blog à propos du rapport Mandiant ; Eric C. Anderson au travers de son analyse du discours sinophobe[62]), les autres à plus de retenue dans l'expression des enjeux des politiques de cybersécurité (Martin Libicki dénonçant la rhétorique guerrière américaine qui fait courir le risque d'une escalade non maîtrisable de la violence internationale[63]). Mais on peut s'interroger sur le contrepoids que peuvent effectivement exercer des regards critiques et des appels à la prudence, face à un discours alarmiste qui trouve son ancrage dans près de deux décennies de fabrique de l'image de l'adversaire majeur.

---

[60] L'existence de l'unité 61398 n'est pas révélée par le rapport Mandiant. Un article de la presse chinoise (China Digital Times) évoquait visiblement déjà son existence en mai 2004. Le China Digital Times du 13 mai 2004 informe que l'unité 31398 de l'armée chinoise, localisée dans le district de Pudong, à Shanghai, recrute des informaticiens, et offre des bourses d'études universitaires. Laura Saporito and James A. Lewis, *Cyber Incidents attributed to China*, CSIS, Washington, Etats-Unis, 14 pages, 5 mars 2013, http://csis.org/files/publication/130311_Chinese_hacking.pdf. Le rapport du Projet2049 publiait également des informations précises sur cette unité dans son rapport de novembre 2011. Mark A. Stokes, Jenny Lin and L.C. Russell Hsiao, *The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure*, 11 novembre 2011, 32 pages,
http://project2049.net/documents/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf

[61] Théories de l'école de Copenhague, études de sécurité.

[62] Eric C. Anderson, *Sinophobia: the Huawei Story*, janvier 2013, CreateSpace Independent Publishing Platform, 400 pages, janvier 2013

[63] Kim Zetter, *Tone Down the Cyberwarfare Rhetoric, Expert Urges Congress*, Wired, 20 mars 2013, http://www.wired.com/threatlevel/2013/03/tone-down-cyberwar-rhetoric/?utm_source=dlvr.it&utm_medium=twitter

Fondation Saint-Cyr, Ecole militaire, 1 place Joffre, 75007 Paris
Téléphone: 01-45-55-43-56 - courriel: contact@chaire-cyber.fr; SIRET N° 497 802 645 000 18

La chaire remercie ses partenaires