Overview of the publications on Chinese Cyberdefense [1]

Daniel Ventre, CNRS (CESDIP/GERN)[2],
Chairman of the Cyber Security and Cyberdefense Chaire (Saint-Cyr, Sogeti, Thales)

July 1st, 2013. Convention on « China: Cybersecurity and Cyberdefense policies and strategies»

July 2013 – article n°VI.1.a

The APT1 report: *Exposing One of China's Cyber Espionage Units*[3] is one of the most notorious recent American publications, dealing with China and its practices and policies in terms of cyberdefense. The report is one of many publications on China, since the 90s, in the United States, mostly focusing on two aspects:

- The hacker's world: cyber espionage, cyber crime, military-originating operations, patriotic/nationalistic hackers, hacktivists operating on networks since the 90s.
- The Chinese army, and its obvious interest in information warfare, command of informational space (and cyberspace), computerization of forces (more accurately the notion of *informationization* , which covers the computerization of weapon systems but also the assessment of operations within cyberspace).

Among the most significant Anglo-Saxon publications dealing with those subjects, the following stand out. We will find here the works[4] of James Mulvenon (1999)[5], Toshi Yoshihara (2001)[6],

---

[1] This text is an excerpt from: Daniel Ventre, *Une analyse du rapport Mandiant* », Revue *Sécurité Globale*, Paris, A paraître. 2013.

[2] ***This article cannot be reproduced, in part or in whole, partially or completely, without the written authorization of its author. Copyright : Daniel Ventre, 2013***

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

[4] This is a selection, and not a comprehensive list, or works, incident technical analysis reports, state documents dealing with the Chinese cyberthreat (cyberespionage, hacktivism, military capacities, military strategies). It is obvious that many more works have been produced in the past 20 years, namely in academic or specialized reviews. We send the reader, in that regard, towards reviews such as Foreign Affairs; Journal of Strategic Security; Journal of Defense Studies ; etc.

[5] 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-

Nina Hachigan (2001)[7], Timothy L. Thomas (2001[8], 2004[9], 2006[10], 2007[11], 2009[12]), Ken Dunham et Jim Melnick (2006)[13], Brian Mazanec (2008)[14], Ron Deibert et Rafal Rohozinski (2009)[15], Bryan Krekel et George Bakos[16], Jeffrey Carr (2009) [17], R. A. Clarke et R. Knake (2010) [18], Elisabette M. Marvel (2010) [19], Martin Libicki (2011)[20], Dmitri Alperovitch (2011)[21], Venusto Abellera (2011) [22], C. Paschal Eze (2011) [23], Mark A. Stokes, Jenny Lin et L.C. Russell Hsiao (2011)[24], William T. Hagestad (2012)[25], Dennis F. Poindexter (2013).

Unis, pp.175-186, minutes of the conference held in San Diego, Californie, 9-12 July 1998, http://www.rand.org/content/dam/rand/pubs/conf_proceedings/CF145/CF145.chap9.pdf ; http://www.rand.org/pubs/conf_proceedings/CF145.html

[6] 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

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

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

[9] 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

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

[11] 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

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

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

[14] 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, December of 2008

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

[16] - 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 October 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 March of 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

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

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

[19] Elisabette M. Marvel, *China's Cyberwarfare Capability*, 105 pages, Nova Science Pub Inc, 31st of October 2010

[20] Martin Libicki, *Chinese use if cyberwar as an anti-access strategy*, testimony brought before the U.S. China Economic and Security Review Commission, January 27th 2011, Publication Rand corporation, 6 pages, http://www.rand.org/content/dam/rand/pubs/testimonies/2011/RAND_CT355.pdf

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

[22] 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, September of 2011

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

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

[25] William T. Hagestad, *21st Century Chinese Cyberwarfare*, IT Governance Publishing, Cambridge, United Kingdom, 314 pages, March 1, 2012

Let us also point out the annual reports[26] of the American Department of Defense on the development of Chinese military power, which always give much attention to questions of information warfare and cyberspace (these reports have been published since the year 2000), the congressional reports of *US-China Economic and Security review* Commission (published annually since 2002)[27], the *United States House of representatives* report (2011)[29], the Office of *National Counterintelligence Executive* report (2011)[30], or even the American *National Intelligence Agency* report (classified report in 2013)[31].

Anglo-Saxon literature produced on China's cyberwarfare and information warfare capacities has been depicting, since the 90s, a worrying nation, aggressive and with unlimited resources at hand (because, when the subject of actual civil servants themselves is left aside, arises that of cybercriminals or even millions of citizens shifted into nationalistic hackers, forming as many threats for the rest of the globe, given their skills and motivations), a nation with obscure defense strategies[32], whose current tendancy to launch cybernetic attacks finds it roots in centuries of warring tradition (the Art of War of Sun Tzu, Mao's irregular war), would rely on the existence of techno-warrior forces formed since the Cold War[33], and would indicate China's will to impose itself as an alternative to America's hegemonic power, thus jeopardizing the World order which set at the end of the Cold War. Facing it, America and the rest of the industrialized world would find itself vulnerable, inferior (R. Clarke[34]; Joel Brenner[35]) given their dependence to cyberspace, the number of potential adversaries, their motivations, and would therefore have no choice but to prepare for confrontation whil trying to fill the gap in terms of capacities, both offensive and defensive[35]. This amounts to an alarming speech, which finds its roots in the forecasts of

---

[26] Department of Defense, USA, *Annual Report to Congress. Military Power of the People's Republic of China*, 2000 and following.

[27] Law of 2000. Last report in November of 2012.

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

[29] United States House of Representatives, *Communist Chinese Cyber-Attacks, Cyber-Espionage and Theft of American Technology*, USA, June 30th 2011, 91 pages, Kindle Edition available at : 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

[30] Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace*, October of 2011, 31 pages, United States, http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf

[31] The report would seem to confirm that China is the main source of cyberthreats. The existence of this document is mentioned in the press. Example : Stacy Curtin, China is America #1 Cyber Threat: U.S. Govt. Report, February 11th, 2013, http://finance.yahoo.com/blogs/daily-ticker/china-america-1-cyber-threat-u-govt-report-150621517.html

[32] - Richard Halloran, *The Opacity of China's Military*, The Washington Times (Washington, DC), March 10 2009 - Kristopher Harrison, *Why China's economic opacity is a serious problem*, Foreign Policy, July 10, 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,* June 10th, 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*, USA, 66 pages, p.I, http://www.defense.gov/pubs/pdfs/China_Military_Report_08.pdf

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

[34] R. A. Clarke, R. Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, Ecco Publisher, USA, April of 2010, 320 pages

[35] Joel Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*, The Penguin Press HC, USA, September of 2011, 320 pages. J. Brenner was a political advisor for questions of cybersecurity in the NSA (United States).

[36] 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, USA, January of 2013, 146 pages, http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf

The 1990-2000 decade announcing a Cyber Pearl Harbor and other cybernetic chaos, and has taken hold of the political class (the American Senator Mike Rogers has declared that the United States are losing the cyberwar against China)[37]. More moderate perspectives, enticing to a more constructive dialog and a cooperating attitude between China and the United States are put forward by entities such as the EastWest Institute[38]. A few publications also analyze the consequences this upheaval of cybernetic power could have on international relations (Françoise Mengin[39]).

Let us underline that the topic of Chinese cyberthreat is often tackled by the military, or the ex-military: Thimothy L. Thomas[40], Scott J. Henderson[41], Rich Barger[42], Mark. A. Stokes[43], William T. Hagestad[44] , among others[45]. Given the profile of some of its leaders, Kevin Mandiant worked within the 7th Communication Group (Pentagon), as a special agent, at the AFOSI (U.S. Air Force Office of Special Investigations). Travis Reese and Dave Merkel, both members of the company CEO, are also members of the AFOSI. Richard Bejtlich, also a member of Mandiant's CEO, author of the Tao Security website[46], was an intelligence officer within the US Air Force CERT as well as in the Air Force Information warfare center (AFIWC) and the Air Intelligence Agency.

Finally, a third approach focuses more on social, political and economic transformations, induced by the very introduction of networks within China : citizen's freedom of speech, foreign influence, state control and surveillance over populations, social networks use (Xu Wu 2007[47] ; Yongnian Zheng 2007[48] ; Rebecca Fannin 2008[49] ;

---

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

[38] Greg Austin, Franz-Stefan Gady, Cyber Detente between the United States and China, EasWest Institute, New York, United States, 28 pages, 2012, http://www.ewi.info/system/files/detente.pdf

[39] Françoise Mengin, *Cyber China: Reshaping National Identities in the Age of Information*, CERI Series in International Relations and Political Economy (Paris, France), Palgrave Macmillan, 288 pages, November of 2004

[40] Lieutenant-colonel Thimothy L. Thomas was an analyst at the FMSO (Foreign Military Studies Office), in Fort Leavenworth (Kansas, USA), director of the USARI - Soviet Studies - United States Army Russian Institute (USARI), in Gamisch - Germany.

[41] Scott J. Henderson, ex-US army officer (analyst),who wrote the book "the Dark Visitor" and ran the famous eponym website, and who focused on Chinese hackers' activities.

[42] Rich Barger, in charge of intelligence matters at Cyber Squared , worked within the U.S. Army (1st Information Operations Command). On the Cyber Squared website, Several APT groups are mentioned as being under scrutiny of the company http://www.cybersquared.com/just-the-tip-of-the-iceberg/

[43] Member of Project 2049, co-author of the 2049 report, *The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure*, M. A. Stokes served in the U.S. Air Force for 20 years.

[44] U.S. Marine Lieutenant-colonel

[45] In China, officers are also the greatest source of works, which has profoundly shaped Western perception's of the country's ambitions and intentions during the 2000 decade : the notorious Unrestricted Warfare, from colonels Liang Qiao et Wang Xiangsui. This publication has probably way more marked western minds than others works, albeit just as important, on information warfare, published by other Chinese officers (Wang Baocun, Dai Qingmin ou Wang Pufeng) since the beginning of the 90s, but which have remained more confidential, because of their more conceptual or theoretical and of the language barrier. Liang Qiao, Wang Xiangsui, *Unrestricted Warfare*, Beijing: PLA Literature and Arts Publishing House, February of1999, 228 pages, http://www.cryptome.org/cuw.htm

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

[47] Xu Wu, *Chinese Cyber Nationalism: Evolution, Characteristics, and Implications*, Lexington Books, United States, 2007, 280 pages

[48] Yongnian Zheng, *Technological Empowerment: The Internet, State, and Society in China*, Stanford University Press, United States, November 2007, 272 pages

Sherman So et J. Christopher Westland 2009[50] ; Daniel Ventre 2010[51], Wang Jun 2011[52] ; Guobin Yang 2011[53] ; Severine Arsene 2011[54] ; Lennon Yao-chung Chang 2013[55].

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

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

[51] Daniel Ventre, *Emeutes au Xinjiang et guerre de l'information chinoise*, dans Daniel Ventre (Dir.), "Cyberguerre et guerre de l'information. Stratégies, règles, enjeux", 2010, Hermès Lavoisier, 320 pages, ISBN 978-2-7462-3004-0

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

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

[54] Séverine Arsène**,** *Internet et politique en Chine. Les contours normatifs de la contestation*, Paris, Karthala, coll. « Recherches internationales », 2011, 420 p., ISBN : 978-2-8111-0580-8.

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