Institut für Strategie- Politik- Sicherheits- und Wirtschaftsberatung, Berlin

Hacktivism of Chinese Characteristics and the Google Inc. Cyber Attack Episode

by Dr. Sheo Nandan Pandey

Introduction

China's legions of hackers, known as *Hongke* (Red Guests), hit headlines across the world on Jan 12, 2010. David Drummond, the Senior Vice President, Corporate Development and Chief Legal Officer of Google Inc. revealed that a "sophisticated" cyber attack had taken place on its infrastructure.[1] Google Inc. engineers, as reported in *The Washington Post*, *The New York Times* and *Marketwatch*, had suspected where the attack had come from in Dec 2009 and identified the location of the attackers in the People's Republic of China (PRC).

According to U.S. Congressional sources, reported subsequently in U.S. print media, the Chinese cyber attacks had targeted at least 34 U.S. companies including Yahoo, Symantec, Adobe, Northrop Grumman and Dow Chemical. Eli Jellenc of VeriSign's iDefese Labs, who helped some firms to investigate the attacks, and stated that the Chinese hackers were after the 'source code' of the targeted U.S. companies. The attackers employed multiple types of malicious codes against multiple targets. Security experts in the field believe that the cyber attacks constitute part of China's 'concerted political and corporate espionage' against its adversaries.[2]

The attacks resulted in a retaliation from Google Inc. and a reaction from the U.S. administration and the PRC, which exceeded all the past acrimonious exchanges. The development is a substantial change in the US threat perception against Chinese 'hacktivism'.[3] Amidst China's denials and counter claims, several countries including India have since complained vigorously about Chinese hackers.[4]

---

[1] http://googleblog.blogspot.cpm/2010/01/new-approach-to-china.html
[2] http://www.washingtonpost.com/wp-dyn/content/article/2010/01/13/AR2010011300359.html
[3] "Hacktivism" is a portmanteau of 'hack' and 'activism'. It carries a positive as well as negative connotation. However in both case, it relates to electronic direct action, combining programming skills and critical thinking. It is more often than not synonymous to malicious and destructive acts that could undermine the security of internet a technical, economic and political platform. The term was coined by techno-culture writer Jason Sack in a piece about media artist Shu Lea Cheang, published in InfoNation in 1995 while the first act of 'Hacktivism, as documented by Julian Assang, relate to 1989 incident of 'anti-nuclear WANK worm penetrated log screen of American DOE, HEPNET, and SPAN (NASA) connected with VMS world wide. Chinese "Hacktivists" made slightly late but sure footed debut right in 1997 and have, of late, added substantial technological muscles to their capabilities.
[4] The computers in the Prime Minister Office (PMO) were hacked on Dec 15, 2009. As per the statement of the then Indian National Security Advisor (NSA) M. K Naryanan, the attack came in the form of e-mail with a PDF attachment, containing a Trojan virus, which allows a hacker to access and to control a computer remotely and down load or delete files. Chinese Foreign Ministry spokesman Ma Zhaoxu formally denied China's hands. This was not the first time the Chinese hackers attacked Indian computer networks. Computers of nine key Indian embassies, including offices in the US, UK and Germany were infected by the

According to a release of IT security firm Sophos on Feb 3, 2010, China ranked third with 11.2 % share after the U.S. (37.4 %) and Russia (12.8 %) among the top 10 malware hosting countries on the web across the world during Jan - Dec, 2009. There has been decline in China's share from 51.4 % in 2007 and 27.7 % in 2008. Inspite of official Chinese denials, the evidence of the role of China in the world of cyber warfare is quite clear.

The Google Inc. Cyber Attack Episode reveals both defensive and offensive character of China's computer network operations (CNO) against its targets. 'Self-Censorship' stipulation, which Google Inc. refused to comply with and threatened to leave China unless dropped and its Golden Shield (*jindungongcheng*) Project, some times referred as 'Great Firewall of China', operating directly under the command and controls of the Chinese intelligence organization the Ministry of Public Security (MPS), happened to be at the core of all organized defensive efforts.[5] Cyber force, entrusted with computer network operations (CNO) discernibly holds the character for offensive operations. There are also Psychological Operations (PSYOPS) troops, mobilized to provide propaganda covers, to play an offensive-defensive role with a difference.

The paper is aimed at understanding the 'distinctive character' of 'Chinese Hacktivism', both in terms of institutional and individual activities and operations. There is essentially a 'pre-event hard side' and 'post-event soft side' of the operations. Leaving aside the specific 'pre-event hard side' of the Google Inc. episode, the paper will look into and focus on the basics of the Chinese cyber warfare infrastructure including the doctrine, responsible in part or entirely for the growth and development Chinese hacker organisations.

'Post-event soft side' of the Google Inc. episode has shown Chinese media, academic circle and the government machinery speaking as with one voice, characteristic of Chinese political governance. It lends credence to the explicit and/or implicit culpability of the Chinese state in the development of the Chinese hacker community. In turn, it arouses academic concern to understand whether the Chinese state could declare a cyber war against its potent adversaries with capability to disguise the origin of a so called distribution denial of service' (DDOS) attacks such as Russian government reportedly conducted in the case of the Baltic state of Estonia in April 2007 and Georgia in July 2008.[6]

The study has thus been organized to focus on: the Pool Size and Antecedents of Hacktivists; State Leverage and Synergy; and, Sources and Methods of Attacks. Postulates include: the Chinese hacktivism has grown in the past as a weapon of future war; the state and non-state hacktivists enjoy favourable policy and technical support for future growth and development. Even under permanent observation and with hi-tech security mechanism in place, China's competitors and adversaries, including India, face the prospect of continued cyber attacks.

---

mysterious GhostNet, A China based cyber espionage network. In the past three years, the GhostNet has infected Indian Informatics Centre (NIC) several times.

[5] PRC carries out internet censorship under a wide variety of laws and administrative regulations, which included Article 12, Article 14 and article 15 of the State Council Order No. 292, issued in September 2000 that makes it incumbent upon IIS provider to censor information as per the wishes of the Chinese government. Golden Shield project, launched in 1998 involved altogether 30,000 experts. The first part of the project lasted eight years and could be completed only in 2006. The work on the second part began in 2006 and completed in 2008. according to the CCTV, the project has cost China 6.4 billion YUAN (US$800 million)

[6] In May 2007, Urmas Paet, the Estonian Foreign Minister, accused the Kremlin of direct involvement in the attack of Estonian government sites and telephone networks in retaliation to the decision of the Estonian government to shift the Bronze Soldier Statue from the centre of the capital city Tallinn to a suburb, which the Russians considered disrespect.

Pool Size and Antecedents of Hacktivists

Chinese hacktivists tend to multiply fast both in number and skills. They constitute many layers of interest groups: malware tool developers, security researchers, and those in training. Since 1997, the notoriety of the Chinese hacktivists has come to encompass quite a large area of global cyber warfare activity.

James Mulvenon of the Center for Intelligence Research and Analysis, a consultant to U.S. intelligence agencies, put the number of trained Chinese military hackers at around 50,000 in 2008.[7] The U.S. Federal Bureau of Investigation had earlier put their number at 30,000 in 2003.[8] They have benefited from professional training at People's Liberation Army (PLA) Communication Command Academy, Wuhan, Hubei Province, National University of Defence Technology (NUDT), Changsha, Hunan Province, PLA University of Science and Engineering, Nanjing, Jiangsu Province, PLA Information Engineering University, Zhengzhou, Henan Province, to name only a few. China's People's Armed Police Force (PAPF), entrusted, inter alia, with the task of 'preservation of public order and security', hold 'several tens of thousands of cyber cops', who can at will switch from policing the Chinese web space to cyber warfare.[9]

There are some non-state hacktivist groups, operating across China. Scott J. Henderson has listed as many as 189 hacker groups in his seminal work, the Dark Visitor: Inside the World of Chinese Hackers, on the basis of their websites. Other estimates put the number Chinese non-state hacktivists at 250 groups. One of the prominent groups, China Red Hacker Alliance (*zhongguo hongke lianmeng*), has staggering over 400,000 individual hackers as its member.[10]

Some of the top Chinese hacker groups known for their proficiency, collaborate with the Alliance included Xfocus, Black Eagle Honker Base, NSFOCUS, Venus Technology, Evil Octal, and others. Further prominent Chinese hacker groups making their presence felt in the game include Goodwell, Lonely Swordsman, Glacier, Leaf, Flyingfox, Coolswallow, China Eagle Group, Wicked Rose, the NCPH Hacking Group, and Hacksa.cn. These and hundreds of Chinese hacker groups use, one way or the other, a large pool of 384 millions internet users, sharing some of the 232,446 million IP (Internet Protocol) addresses, 16,818 million domain names and 3,232 million websites.[11]

State Leverage and Synergy

The state leverage of Chinese hacktivists, both within and beyond the government is discernible at various levels and forms. The same holds true where it relates inter-group synergy. The PRC is however making a clear cut distinction between cyber crimes and cyber

[7] http://www.chinapost.com.tw/commentary/reuters/2010/01/22/241862/p2/Google-hacked.htm
[8] http:// www.chinapost.com.tw/commentary/reuters/2010/01/22/241861/p2/US-fears.htm
[9] The evidence is borne of a statement of the Chinese Minister of Public Security Meng Jainzhu in the presence of several senior police officers while touring Anhui Province in Nov 2009. As reported in Chinese media (People's Daily, November 1, 2009; Ming Bao, November 2, 2009), Meng had then called upon 'several tens of thousands of cyber cops' to boost cooperation with companies in electronics and IT fields for the job in the presence of se
[10] Wendel Minnick, "Is Beijing behind Cyber Attacks on Pentagon", *DefenseNews*, June 2, 2008 http://www. defensenews. Com/story. php?i=3576373
[11] http://www.marketreportchina.com/market/article/content/3376/201001/217340.html

war, the former to safeguard its interests and the latter to impinge on the interests of the adversaries.[12]

China's non-state cyber groups have constantly attacked adversaries on issues that stand in the way of state policy. They have, accordingly, come to earn the honorific title of "patriotic hackers", whom China's military or state security departments turn to for their operations.[13] Elements of the present day China Red Hacker Alliance while part of Honker Union engaged U.S. hackers over the Hainan Island Incident, which related to a mid-air collision of U.S. Navy EP-3E Aries II signals surveillance aircraft with PLA Navy J-811 Interceptor fighter jet on April 1, 2001. They altered the page of the U.S. government website.[14]

They also altered the page of the U.S. Department of Labour and Department of Health and Human Services to display a picture of Wang Wei, the Chinese pilot who died in the collision. The page was titled "China hack!", and read in English: "The whole country is sorry for losing the best son of China - Wang Wei for ever. We will miss you until the day". Chinese hackers, masquerading under pseudonym of "Chinese Honker Team", quite possibly affiliated to China Red Hacker Alliance showed up and attacked Iranian websites in retaliation to Iranian hackers, pseudonym Iranian Cyber Army, venturing to take over China's search engine Baidu on Jan 12, 2010.[15] There are many such stories from Taiwan, Japan and other countries including India, involving one or the other Chinese hacker entities.

Notwithstanding, there is a move in China for the state and non-state hacktivist groups to evolve and work in a public private partnership (PPP) model, in particular where it relates to Research and Development (R&D). This is evident from China's preferential policies, extended to commercial computer and electronic enterprises, who share their resources and data with relevant units in the PLA, the Para-military People's Armed Police Force (PPF), the Ministry of State Security (MSS), and the Ministry of Public Security (MPS) and others. [16]

The First Research Institute of the MPS was of late in the forefront of recruiting Chinese graduates in areas including computers, engineering, mathematics and foreign languages. The same hold true about research units with the MSS. The advertisements are placed on government and private websites. The recruitment of such hackers is carried out under the guise of software engineers and Net-related security experts. The symbiotic relationship of the Chinese state with the Chinese hacktivists is equally evident in their training programmes, be it formal as part of information warfare (IW) or informal hacking training outfits.[17]

The Chinese hackers quite often hold seminars and run magazines with names such as Hacker X Files, Hacker Defense and the like and provide tips on how to break into computers and/or

[12] As China turned a virtual haven for internet crimes, China introduced three new articles to its criminal code, which has provision of seven years of imprisonment. Further, China has also broadened its definition of crimes committed on computers.
[13] New York Times, February 3; China News Service, January 25; Cnjz.cn [Beijing], November 1, 2009; Guofang.info [Beijing], September 17, 2009.
[14] http://www.china.org.cn/english/12150.htm
[15] The hack of Baidu.com has been authenticated by the Chinese print media, in particular the People's Daily, which published a screen grab showing a message reading: "This site has been hacked by the "Iranian Cyber Army", along side a picture of the Iranian flag. In a statement the company said, "Services on Baidu main website www.baidu.com were interrupted due to external manipulation of its DNS (Domain Name Server) in the US. Baidu has been resolving this issue and majority of services have been restored". Iranian hackers had reportedly retaliated Chinese Twitter users who used #CN4Iran hash tag to express support for opposition candidate promising reforms.
[16] China.com.cn, November 3, 2009; Apple Daily [Hong Kong], January 29, 2010; Asiasentinel.com [Hong Kong], January 22, 2010.
[17] China shut down Black Hawk Safety Net (3800cc.com), a group that sold training materials and malicious codes for illegal hacking in Feb 2010. Established in 2005, the group had 12000 paid and 170,000 members. There are yet tens of academies operating through out China. Some of the important non-state hacker training facilities, making news in the Chinese media for different reasons included Yinhe Info and Tech Academy and Beida Qingniao. The Chinese government entities known for turning out a larger number of hackers included Shanghai Jiaotong University and Lanxiang vocational school. Among Chinese military outfits, the China Academy of Military Sciences has earned equal notoriety.

build a Trojan horse step by step. In the 'pre-event hard side' of the game, as per Willy Lam, senior cadres, such as Dr Jiang Mianheng, the eldest son of former Chinese President Jiang Zemin and the Vice Principal of the Chinese Academy of Sciences play a major role.[18] The process is bound to gather momentum as the 12th Five Year Plan (2011 - 2015) of the PLA on net-based combat systems, including cyber espionage and counter-espionage, is put in place.

In the 'post-event soft side' of the game, the Chinese hacking community draws on national support, far exceeding the symbiotic relations evident in the course of 'pre-event hard side'. It is a battle where the Chinese media, academia and officials come out in total denial and try to find even scape-goat whenever at all possible.

The Google Inc. Cyber Attack Episode stands as a clear testimony to the role of the Chinese media in Cyber Warfare. Using studied rhetoric, it sought to convince the world that Google Inc. was working on behalf of the U.S. administration to 'impose its values on other cultures in the name of democracy'. *Global Times*, a tabloid owned by *People's Daily*, the mouthpiece of the communist Party of China (CPC), ran a number of articles including an editorial with the headline: "The world does not welcome the White House's Google".[19]

It sought to justify both Chinese censorship of internet content and cyber attacks as such with a difference. In a calculated defensive offensive, the *Global Times* named the U.S. as the very first country in the world to have created 'cyber army of 80,000 people equipped with over 2,000 computer viruses. Even where if true, a supposedly unscrupulous act of 'X' can not legally justify an unscrupulous act of 'Y'.

Chinese officials and experts stood behind the media offensive. In a statement, Zhou Yonglin, the Deputy Operations Director of the National Computer Network Emergency Response Centre (NCNERC), said: "Everyone with technical knowledge of computers knows that just because a hacker used an internet protocol (IP) address in China, the attack was not necessarily launched by a Chinese hacker." iDefense Labs among other security firms have testified that the IP addresses of attack on Google Inc. and other targets corresponded to 'single foreign entity consisting of either of agents of Chinese state or proxies there off'. Chinese Foreign Ministry spokesman Ma Zhaoxu justified the sordid game with a difference. He found gagging of internet contents as being necessary, in tandem with China's 'national conditions and cultural traditions'. As for the offensives of the Chinese hacktivists, Ma cited exiting legal stipulations that renders hacking a punishable crime in China.[20]

Going a step forward, Chinese academia in the field has been busy finding a scape-goat. Peter Lee, for example, found it expedient to suggest that the Google Inc. episode was a help to India, the 'U.S. ally' and 'China's emerging rival' and borne of two hard realities: U.S. business tycoon Google Inc. not 'doing well in China' and U.S. President Barrack Obama not 'doing well in United States'.

In the 'high profile confrontation with China',[21] Wang Yizhou, deputy chief of the Institute of World Politics and Economy at the Chinese Academy of Social Sciences characteristically tried to turn the table against the U.S. and said: "In the U.S., a country that boasts its Internet freedom, governmental supervision virtually infiltrates across the nation, and its influence further extends to worldwide servers. Information-searching via Google and online chatting

[18] Willy Lam, "Beijing Bones up its Cyber Warfare Capacity", *China Brief*, Volume:10 Issue:3, February 4, 2010.
[19] Chinadigitaltimes.net/china-news/main/world
[20] Chinese official response to Google Inc. threat to pull out of China unless China allowed Google search engine to run uncensored came characteristically 11 days later on 24th Jan 2010 in almost premeditated way in the course of two interviews.
[21] Peter Lee, "Winner of Google-China Feud is India", *Asia Times*, Jan 28, 2010.

through Windows Live Messenger are all under stringent surveillance, and the relevant agencies are tasked with compiling backups." Even if true, it can not justify China's actions.

In fact, Chinese hacktivism of the kind finds justification as being non-kinetic and are in tandem with China's two strategic doctrines: first, 'Gaining Information Dominance' (*zhi xinxi quan*) against potential adversaries; and secondly, adhering to 'Three Warfare' (*san zhong zhanfa*). [22] It is then in tandem with one of the 36 strategies of China's age old wisdom to 'kill with a borrowed sword'.[23]

Sources and Methods of Attacks

While not yet conclusive, Shanghai Jiaotong University and the Lanxiang Vocational School working closely together in the Google Inc. Cyber Attack Episode.[24] In the break-in, as Joe Stewart, a malware specialist with Atlanta based computer security firm SecureWorks, says, the hacktivists, in question, used a programme, based on an unusual algorithm, once discovered in a Chinese technical paper, published exclusively on Chinese language websites. The malware was a "Trojan Horse", capable of opening a backdoor of a computer on the Internet.

Beginning May 1999 when the Chinese hacktivists attacked U.S. government sites in retaliation to the accidental bombing of China's Embassy in Serbia, Belgrade, and through many of the 35 well known incidents, until the Jan 12, 2010 Google Inc. Cyber Attack Episode, and also including attacks in the U.S., Taiwan, Japan, New Zealand, Australia, South Korea, France, Germany and India, the methods, brought to bear upon for the purpose by the state and/or non-state Chinese hackers community fall into three major categories: the first is the use of e-mails for planting viruses; then phishing and lastly, the introduction of 'intelligent trojans' and 'vacuum trojans'. Tools employed, thus far, range from robotic and simple to brainy and sophisticated. For instance, Chinese hackers have quite frequently used a 'vacuum Trojan' to extract information from a pen drive automatically when connected to a USB port. It is also believed that the next step could be planting the targeted sites with the more difficult to detect fake data or partially fake data.

China's cyber weapon capabilities have come to be considered quite advanced, assessed to be so far the fifth in ranking and making all out efforts to rival the U.S., the technological leader in the world of IW capabilities. The arsenal, in order of threats, encompasses and included: large, advanced BotNet for DDos and espionage, electromagnetic non-nuclear pulse weapons; compromised counterfeit computer hardware; compromised peripheral devices; compromised counterfeit computer software; zero-day exploitation development framework; advanced dynamic exploitation capabilities; wireless data communication jammers; computer virus and worms; cyber data collection exploits; computer and networks reconnaissance tools; embedded Trojan time bombs; and, compromised micro-processors and other chips.

---

[22] "Three Warfare" doctrine combines psychological, media and legal warfare. Psychological warfare relates to use of propaganda, deception, threats, and coercion to degrade the ability of China's adversary to understand the objective situation and to make appropriate and effective decisions; media warfare pertains to dissemination of information to sway public opinion and obtain support from domestic and foreign audiences for China's forward actions; and, legal warfare stretches forth to use available domestic and international laws to substantiate legality of its operations.

[23] Sun Zi' s The Art of War lists 36 strategies, each of them expressed as proverbs and a story borne of on ground experiences through out the ages. "Kill with Borrowed Sword" is the third in sequence after 'Fool the Emperor to Cross the Sea' and 'Besiege Wei to Rescue Zhao'.

[24] Xinhua News Agency carried a rebuttal of the report in *New York Times* about the involvements of the two elite Chinese schools having close relation with the PLA. Quoting unnamed representative, the report said:"The report of the *New York Times* was based on an IP address. Given the highly developed network technology today, such a report is neither objective nor balanced".

Chinese media reports suggests that the Chinese IW units have been accessing, if not out sourcing R&D for developing viruses to attack the computer systems and networks of the adversaries, and tactics to protect friendly computer systems and networks. In Nanjing, the PLA has developed more than 250 trojans and similar tools. The Chinese Academy of Sciences, which provides suggestions about national information security policy and law, has established the State Lab for Information Security with 'National Attack Project' as one of its research programmes. Recently held military exercises bear out that the PLA has since increased the role of CNO and has been concentrating on offensive operations, primarily as first strikes against the networks of adversaries. The state and non-state Chinese hacktivist thus constitute a real threat to their adversaries until they are technologically matched and surpassed both in defensive and offensive operations.

***

Remarks: Opinions expressed in this contribution are those of the author.

Dr. Sheo Nandan Pandey, born Jan 14, 1947, served both institutions of higher learnings and the bureaucratic set up as member of Civil Services in India. He speaks several languages including Chinese mandarine. In area studies, China is his first love.

Berlin, Germany
www.ispsw.de