Cyber Incidents Attributed to China

Laura Saporito and James A. Lewis
Center for Strategic and International Studies

Many times in discussion of cybersecurity one hears the charge that there is no evidence that China and Chinese hackers are responsible for the many incidents attributed to them. CSIS did a review of open source literature identifying China as the source of hacking and cyber espionage incidents. This is an initial list, as we know of other major cyber incidents attributed to China by officials in Australia, Canada, France, Germany, India, Japan, the UK, and other countries not discussed here. We have broken our list into two parts. The first section lists reports that identify specific individuals and entities; the second section refers to incident ascribed generally to China. These reports identify six groups and fourteen individuals, all but one connected to the Chinese government and most with connections to the PLA, as responsible for cyber espionage.

Specific Attribution to China

"APT1: Exposing One of China's Cyber Espionage Units," Mandiant Intelligence Center Report (2013). http://intelreport.mandiant.com/

> Mandiant's Intelligence Report identifies APT1 as a persistent Chinese cyber threat actor with operations that are likely government-sponsored. APT1 is believed to be the 2nd Bureau of the People's Liberation Army (PLA) General Staff Department's (GSD) 3rd Department, commonly known as Unit 61398. Activity has been traced to Shanghai. Also known as 'Comment Crew' and 'Byzantine Candor,' operations can be traced back to beginning in 2006. There are 141 known victims across multiple industries, with targets including the information technology, aerospace, public administration, satellites and telecommunications, scientific research and consulting, energy, transportation, construction and manufacturing, international organizations, engineering services, high-tech electronics, legal services, media, advertising and entertainment, navigation, chemicals, financial services, food and agriculture, metals and mining, healthcare, and education industries. In an effort to stress the human agency behind cyberattacks, the report identifies three online personas: 'Ugly Gorilla,' a screen name attributed to Wang Dong, 'DOTA,' and 'SuperHard,' attributed to Mei Qiang. All three individuals have connections to the Chinese military.

Lawrence, Dune and Michael Riley. "A Chinese Hacker's Identity Unmasked," Bloomberg Businessweek, 14 February 2013: http://www.businessweek.com/articles/2013-02-14/a-chinese-hackers-identity-unmasked.

> Bloomberg's investigation into a hacker targeting government ministries in Vietnam, Brunei, and Myanmar, as well as oil companies, a newspaper, a nuclear safety agency, an embassy in mainland China, and personal computers in Taiwan and Philippines was traced to a QQ (QQ is popular instant-messaging software in China) and email address belonging to Zhang Changhe. Located in Zhengzhou, Zhang is a teacher at PLA Information Engineering University where professors train junior officers to serve in operations throughout China. Zhang is also affiliated with the Beijing Group, consisting

of programmers, the people handling the infrastructure of command centers, and translators of stolen data.

"Luckycat Redux: Inside an APT Campaign with Multiple Targets in India and Japan," Trend Micro Research Paper (2012). http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_luckycat_redux.pdf

Trend Micro's Report released findings regarding their tracking of the Luckycat campaign. The Luckycat campaign attacked diverse targets including aerospace, energy, engineering, shipping, and military research industries as well as Tibetan activists and organizations in Japan and India using a variety of malware, some of which have been linked to other cyber-espionage campaigns. Using open source research, Trend Micro mapped an email address back to its QQ number and linked the number to a hacker in the Chinese underground community. Although the Trend Micro report does not link the attacks directly to government-employed hackers, the techniques and victims targeted point to a state-sponsored campaign. From his nickname and the hacker's published posts, The New York Times (http://www.nytimes.com/2012/03/30/technology/hacking-in-asia-is-linked-to-chinese-ex-graduate-student.html?pagewanted=all) traced the alias to Gu Kaiyuan. Located in Chengdu, Gu was a former student at Sichuan University, which receives funding for computer network defense research and indicates the Chinese government sponsorship of hackers.

O'Gorman, Gavin and Geoff McDonald. "The Elderwood Project," Symantec Corporation (2012).

Dubbed 'Operation Aurora' for the use of the Hydraq (Aurora) Trojan horse, Symantec monitored this group's activity and their utilization of the 'Elderwood platform,' so named for a source code variable (originates from China). The targeted industry sectors include defense, various defense supply chain manufacturers, human rights and NGOs, and IT service providers, with Google, Adobe Systems, Juniper Networks, Yahoo, Symantec, Northrop Grumman, Morgan Stanley, and Dow Chemical all documenting attacks. The scale of the attacks (both number of targets and duration) as well as the resources required to gather intelligence and intellectual property indicate that a large criminal organization, attackers supported by a nation state, or a nation state itself were responsible. The New York Times (http://www.nytimes.com/2010/02/19/technology/19china.html?_r=0) reported from a source involved in the investigation that Jiaotong University in Shanghai and Lanxiang Vocational School in the Shandong Province were traced back to the attacks.

Stokes, Mark A. and L.C. Russell Hsiao. "Countering Chinese Cyber Operations: Opportunities and Challenges for US Interests," Project 2049 Institute (2012).

The report identifies the GSD Third Department Beijing North Computing Center (BNCC) as one of the most capable in Chinese cyber operations. Also referred to as the GSD 418th Research Institute or by its military cover designation of Unit 61539, BNCC is located in the Jiaoziying suburb of Beijing. BNCC has targeted US government and

private networks. The report also identifies senior BNCC authorities: Geng Xiaohe, Jia Yenghe, Zhu Zhaoming, Fu Shengxin, Li Xiaohui, Yao Zingsong, Kong Tiesheng, Ma Hang, and Yang Baoming.

Chien, Eric and Gavin O'Gorman. "The Nitro Attacks: Stealing Secrets from the Chemical Industry," Symantec Corporation (2011).

A targeted attack campaign primarily directed at private companies involved in the research, development and manufacture of chemicals and advanced materials occurred in 2011. A total of 29 companies in the chemical industry saw the longest sustained attacks, but another 19 companies is various other sectors (primarily defense) were affected as well. Symantec traced the attacks back to a computer system that was a virtual private server (VPS) located in the United States, but the system was owned by a 20-something male living in the Hebei region in China. The cost of the VPS (RMB200 a month) as well as its US location is suggestive, but Symantec was unable to determine if the hacker was operating as part of a larger organization.

"Global Energy Cyberattacks: 'Night Dragon,'" McAfee (2011): http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf.

McAfee documents a coordinated and targeted cyber campaign starting in November 2009, dubbed 'Night Dragon,' conducted against global oil, energy, and petrochemical companies. After identifying the tools, techniques, and network activities used in the attacks, McAfee asserts that the attacks originated primarily in China. Although many actors are believed to have participated in the attacks, McAfee also identified one individual who provided C and C infrastructure to the attackers as someone based in Heze City, Shandong Province, China. Furthermore, all of the identified data exfiltration occurred from Beijing-based IP addresses on weekdays during 9 am to 5 pm Beijing-time. The attackers also used hacking tools of Chinese origin that are prevalent on Chinese underground hacking forums.

Stokes, Mark A., Jenny Lin and L.C. Russell Hsiao. "The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure," Project 2049 Institute (2011).

The report identifies the PLA's Chengdu Military Region, First Technical Reconnaissance Bureau (TRB), military cover designation Unit 78006 as involved in computer network exploitation operations. Revealed in a Reuters report (http://www.reuters.com/article/2011/04/14/us-china-usa-cyberespionage-idUSTRE73D24220110414), classified State Department cables from 2009 that leaked in 2011 identify this unit's involvement in operations dubbed 'Byzantine Hades' and 'GhostNet'. These attacks targeted networks of US and foreign governments as well as those of cleared defense contractors. The cables also identify Chen Xingpeng and his link to the TRB.

"Honker Union of China to launch network attacks against Japan is a rumor," ChinaHush, 15 September 2010, http://www.chinahush.com/2010/09/15/honker-union-of-china-to-launch-network-attack-against-japan-is-a-rumor/.

This report identifies the Honker Union and lists their known attacks from 1998 to 2005. Operating from mainland China, the Honker Union has launched network attacks against Indonesia, Taiwan, and the United States and targeted Japanese central and local governments, banks, universities, and companies, as well as a Tibetan political dissident. These targets suggest that the Honker Union may be a proxy force of the Chinese government.

The SecDev Group. "Tracking GhostNet: Investigating a Cyber Espionage Network," Information Warfare Monitor (2009). http://www.infowar-monitor.net/ghostnet.

The SecDev Group documents a cyber espionage campaign targeting over 1,295 computers in 103 countries, with targets ranging from ministries of foreign affairs, embassies, international organizations, news media, and NGOs. Many of these targets are clearly linked to Chinese foreign and defense policy, particularly in South and Southeast Asia. The most common evidence consists of log files or malware that trace back to the Lingshui signals intelligence facility and the Third Technical Department of the People's Liberation Army on Hainan Island.

Henderson, Scott. "Javaphile, Buddhism, and…The Public Security Bureau?" The Dark Visitor (2007): http://www.thedarkvisitor.com/2007/12/javaphile-buddhism-andthe-public-security-bureau/

The founding member of the influential Chinese hacker group, Javaphile, has a formal consulting relationship with the Shanghai Public Security Bureau and researcher credentials at the Jiatong University's Information Security Engineering Institute in Shanghai. Henderson, an independent analyst, identified Yinan Peng and traced his involvement to 'Byzantine Anchor,' which targeted the Pentagon, State Department, Google, and other US corporations as detailed in the 2011 Wikileaks of classified State Department cables from 2009. This information is also cited in the US-China Economic and Security Review Commission 2009 report ("Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation").

Dunham, Ken and Jim Melnick. "'Wicked Rose' and the NCPH Hacking Group," VeriSign iDefense (2006).

The authors document repeated zero-day attacks, which utilized exploit code for Microsoft Word and Excel, and trace the attacks back to the Network Crack Program Hacker (NCPH) group located in Zigong in the Sichuan Province. During 2006, the group specifically targeted the Defense Department. The group is believed to be comprised of students from the Sichuan University of Science and Engineering, led by Tan Dailin who uses the pseudonym 'Wicked Rose,' with KuNgBiM, Rodag, and

Charles as members. The authors also identify WHG as a close affiliate, whose real name may be Zhao Jibing and is believed to be employed in the Sichuan province.

China Digital Times, translated from Chinese, 13 May 2004.

CDT advertised that Unit 61398 of the People's Liberation Army, located in Pudong District, Shanghai, seeks to recruit computer science graduate students. Students who sign the contract are rewarded with a significant National Defense Scholarship (5,000 yuan per year) and an offer to work in the unit. Interested candidates from Zhejiang University are encouraged to contact Teacher Peng in the Graduate Division.

Thornburgh, Nathan, "The Invasion of the Chinese cyber Spies," Time Magazine, (2005), http://www.time.com/time/magazine/article/0,9171,1098961,00.html#ixzz2NKPE40Da

Thornburgh reports on a Chinese espionage effort given the Code Name "Titan Rain," which were traced to the Chinese province of Guangdong and three Chinese routers that acted as the first connection point from a local network to the Internet.

General Attribution to China

Lewis, James "Hidden Arena: Cyber Competition and Conflict in Indo-Pacific Asia Prepared for the Lowy Institute MacArthur Asia Security Project
http://csis.org/files/publication/130307_cyber_Lowy.pdf

This report discusses the regional implications of Chinese cyber activities and discusses Chinese military and intelligence strategies in the context of Asian security relations

"Chinese Time Bomb," Seculert, 5 March 2013: http://blog.seculert.com/2013/03/the-chinese-time-bomb.html

After the release of the Mandiant report, Seculert discovered spear-phishing attacks, which were using emails purporting to contain the Mandiant report to target Japanese journalists. Seculert found that the server was intended to trace to Korea. However, using Seculert traces the IP address to a server located in Jinan, the capitol of the Shandong province of China. This region has also been linked to the Operation Aurora and Shady RAT attacks.

Inkster, Nigel. "Chinese Intelligence in the Cyber Age," Survival: Global Politics and Strategy 55, no.1 (2013): 45-66.

The PLA focuses on integrated network electronic warfare and is pursuing an ambitious cyber warfare agenda that aims to link all service branches via a common ICT platform capable of being accessed at multiple levels of command. While establishing evidence beyond all reasonable doubt is difficult in all cases, many attacks have been traced back to servers located in China.

Vergano, Dan. "China's universities linked to cyber-spying," USAToday.com, 28 February 2013.

Research fellow Russell Hsiao of the Project 2049 Institute comments that recruitment efforts at universities publishing analyses of hacking software, such as Shanghai Jiao Tong University, "lend credence to the assertion that some Chinese military units are involved and at the very least are cognizant of some of these known intrusions of U.S-based entities."

"Eurofighter Maker EADS Attacked – Chinese Hackers Blamed," techweekeurope.co.uk, 26 February 2013: http://www.techweekeurope.co.uk/news/chinese-hackers-eads-eurofighte-108651

Der Spiegel cited sources from EADS and ThyssenKrupp that indicate that both companies were targeted by cyberattacks originating from China. Although the ThyssenKrupp attack occurred locally in the United States, the attacks were both linked to internet addresses in China. Although China denies the attacks, the information targeted is consistent with Chinese interests and could have potentially damaging military and civilian consequences.

"Digital Spying Burdens German-Chinese Relations," SpiegelOnline, 25 February 2013: http://www.spiegel.de/international/world/digital-spying-burdens-german-relations-with-beijing-a-885444.html

Germany's domestic intelligence agency reported close to 1,100 digital attacks on the German government by foreign intelligence agencies. German officials traced two significant attacks on EADS and ThyssenKrupp to China. The head of the department in charge of cybersecurity at the German Interior Ministry commented: "the overwhelming number of attacks on government agencies that are detected in Germany stem from Chinese sources." Officials have traced the attacks to three major Chinese cities: Beijing, Shanghai, and Guangzhou.

"EADS, ThyssenKrupp attacked by Chinese hackers: report," Reuters, 24 February 2013: http://www.reuters.com/article/2013/02/24/net-us-eads-thyssenkrupp-hacking-idUSBRE91N07M20130224

EADS and ThyssenKrupp reported major attacks by Chinese hackers in 2012. A ThyssenKrupp spokesman provided more details on the attack, stating that it took place in the United States from a Chinese internet address. Both EADS and ThyssenKrupp fit the type of companies targeted by Chinese hackers.

Nakashima, Ellen. "US said to be target of massive cyber-espionage campaign," The Washington Post, 10 February 2013. http://articles.washingtonpost.com/2013-02-10/world/37026024_1_cyber-espionage-national-counterintelligence-executive-trade-secrets.

A recent National Intelligence Estimate is reported to have identified China as the country most aggressively targeting US computer networks.

"Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2012," Office of the Secretary of Defense, Department of Defense (2012).

The report documents that the PRC is pursuing a long-term, comprehensive military modernization program designed to improve the ability of China's armed forces to fight and win high-intensity, information-centric military operations. This focus on 'informatization' also contributed to the PLA's improved military cyberspace capabilities to enable anti-access/area-denial (A2/AD) missions.

Dilanian, Ken. "US Spy Agencies to Detail Cyber Attacks from Abroad," Los Angeles Times, 8 December 2012: http://articles.latimes.com/2012/dec/06/nation/la-na-cyber-intel-20121207.

Cites an intelligence agency official involved in investigating cyberespionage as saying: "we have traced attacks back to a desk in a [People's Liberation Army] office building."

Dobbins, James. "War with China," Survival: Global Politics and Strategy 54, no.4 (2012): 7-24.

Dobbins asserts that the PLA has conducted repeated intrusions into US networks to access sensitive data. While these activities have so far been conducted without American reprisal, repeated attacks could escalate into a cycle of retaliations (cyberwar).

Krekel, Bryan, Patton Adams and George Bakos. "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," report prepared by the Northrop Grumman Corporation for the US-China Economic and Security Review Commission (2012).

PLA leaders have embraced the idea that advantages are accorded to those with the ability to exert control over an adversary's information and information systems, often preemptively. Several computer network operations that have targeted US systems have been attributed to this Chinese strategy.

Lai, Robert and Syed (Shawon) Rahman. "Analytic of China Cyberattack," The International Journal of Multimedia and Its Applications 4, no.3 (2012).

The authors identify China as the most active nation state with cyber espionage activities using a "grain of sands" approach: steal as much data as possible, then infer valuable information from the stolen data. Experts believe that China can be traced back to targeted attacks, including Titan Rain, State Department's East Asia Bureau, Offices of Rep. Frank Wolf, Commerce Department, Naval War College, Commerce Secretary Carlos Gutierrez and the 2003 blackout, McCain and Obama presidential campaigns, Office of Sen. Bill Nelson, GhostNet, Lockheed Martin's F-35 program, and many more. The authors also note that China has an adaptive advantage with its rapid advancement of malicious code, known for advanced persistent threat (APT) campaigns.

Lewis, James A. "China's Economic Espionage: Why It Worked in the Past But It Won't in the Future," Foreign Affairs (2012).

Lewis identifies China as the most aggressive country to use economic espionage, remarking upon the nation's long-running, state-sponsored espionage program to acquire advanced technology and accelerate the growth of China's civil and military industries. He also notes that China combines official collection programs with the efforts of individuals, companies, and civil agencies.

Lieberthal, Kenneth and Peter W. Singer. "Cybersecurity and US-China Relations," Brookings Institution (2012).

The authors discuss the growing perception in America that the multi-faceted Chinese cyber threat has a large government-sponsored component. Rather than random attacks or attacks to solely provide the hacker with economic gain, many attacks target specific strategic objectives. These objectives include: inputs into decisions concerning China, monitoring and threatening dissidents who live abroad, proprietary technology of special strategic interest, and military-oriented planning and reconnaissance.

Riley, Michael and Dune Lawrence. "Hackers Linked to China's Army Seen From EU to DC," Bloomberg, 26 July 2012: http://www.bloomberg.com/news/2012-07-26/china-hackers-hit-eu-point-man-and-d-c-with-byzantine-candor.html.

Authors state that 'Byzantine Candor' is linked to China's military, the PLA, according to a 2008 diplomatic cable released by WikiLeaks. Two former intelligence officials verified the content in the document. The identified victims of the attacks also implicate China as many of them are organizations whose information and IP could give China an advantage. The targets also included lawyers pursuing trade claims against China's exporters and an energy company preparing to drill in waters that China considers under its sovereignty.

Segal, Adam. "Chinese Computer Games: Keeping Safe in Cyberspace," Foreign Affairs (2012).

Segal notes that U.S. intelligence officials claim that 20 groups associated with the People's Liberation Army and several Chinese universities are responsible for the majority of the attacks on Google, RSA, and other U.S. targets. Overall, cyberattacks originating from China can be classified as government-sponsored and tolerated as China views cyber operations as a way to gain an economic and military advantage.

Valeriano, Brandon and Ryan Maness. "The Fog of Cyberwar: Why the Threat Doesn't Live Up to the Hype," Foreign Affairs (2012).

Of the ongoing inter-state rivalries in the authors' study, China and the United States were the most active, with China attacking US assets 18 times and the US responding twice.

Alperovitch, Dmitri. "Revealed: Operation Shady RAT," McAfee (2011): http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf.

> McAfee details a targeted intrusion campaign that affected at least 71 victims in 14 geographic locations over a five year period, including US and other governments, defense contractors, energy, computer security, and communications technology companies, and non-profit organizations. The report identifies 'one state actor' behind the attacks, and other security experts verify that the evidence implicates China.

"Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2011," Office of the Secretary of Defense, Department of Defense (2011).

> The report notes that China's military has made steady progress to develop offensive cyber warfare capabilities. The PLA is integrating complex platforms, adopting modern operational concepts, and focusing on network-centric warfare. Developing capabilities for cyberwarfare is consistent with authoritative PLA military doctrines, 'Science of Strategy' and 'Science of Campaigns,' which identify information warfare as essential to achieving information superiority and defeating a stronger foe.

Ball, Desmond. "China's Cyber Warfare Capabilities," Security Challenges 7, no.2 (2011): 81-103.

> Ball identifies China as having the most extensive and practiced cyber-warfare capabilities in Asia. He also notes that the Chinese military and intelligence agencies are able to utilize the corporate sector, state-owned carriers as well as 'private' companies. Ball also discusses PLA information warfare units who have developed and field-tested procedures. He cites simulated cyber-attack exercises executed in Hubei province, Xian, and Datong. The PLA has also established at least twelve training facilities for integrated network electronic warfare (INEW). Ball locates the lead facility at Zhurihe in the Beijing Military Region, which features 'informationalized Blue Force' for 'opposed force' exercises.

Cliff, Roger, John F. Fei, Jeff Hagen, Elizabeth Hague, Eric Heginbotham, and John Stillion. "Shaking the Heavens and Splitting the Earth: Chinese Air Force Employment Concepts in the 21st Century," RAND Corporation (2011).

> Although the authors focus primarily on the PLAAF, they also depict the Chinese military's general ideology that focuses on information superiority. The Chinese frequently engage in network attacks to weaken the functionality of their enemy computer network systems. They also focus on information defense by blocking cyberattacks and countering electronic surveillance and interference.

Dobbins, James, David C. Gompert. David A Shlapak, and Andrew Scobell. "Conflict with China: Prospects, Consequences, and Strategies for Deterrence," report prepared for the US Army, RAND Corporation (2011).

The authors contend that there is evidence of PLA-sanctioned attacks on US networks, with the potential for continued future attacks or an escalation of attacks if left unaddressed.

Finkle, Jim. "State Actor behind slew of cyberattacks," Reuters, 3 August 2011: http://www.reuters.com/article/2011/08/03/us-cyberattacks-idUSTRE7720HU20110803.

The article comments upon the released McAfee report (Revealed: Operation Shady RAT) and the significant number of cyberattacks attributed to 'one state actor'. Although McAfee declined to name the state in the report, several other security experts say the evidence implicates China.

"Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011," Office of the National Counterintelligence Executive. (2011).

The teport notes that computer networks of US Government agencies, private companies, universities, and other institutions have been targeted by cyber espionage with many of the attacks appearing to have originated in China. Report also emphasizes that China's intelligence services, private companies, and other entities frequently exploit Chinese citizens or people with family ties to China for their insider access to corporate networks to steal trade secrets.

Hartnett, Stephen John. "Google and the 'Twisted Cyber Spy' Affair: US-Chinese Communication in an Age of Globalization," Quarterly Journal of Speech 97, no.4 (2011): 411-434.

Google announced in January 2010 that they had been the victim of a highly sophisticated and targeted attack originating from China. Google accused China of stealing intellectual property, comprising the security of its infrastructure, and spying on Chinese dissidents. Hartnett comments that Google's announcement vindicated experts who attested for years prior that China was conducting a massive global cyber campaign.

Klimburg, Alexander. "Mobilising Cyber Power," Survival: Global Politics and Strategy 53, no.1 (2011): 41-60.

Klimburg reveals that Beijing maintains as many as 30,000 'netizens,' all paid by the government, to serve the government's agenda. He also notes that millions of information-technology personnel are employed in state-affiliated enterprises. Klimburg cites the cybersecurity company iDefense, which has tracked over 250 named hacker groups in China, many of which are responsible for US-targeted attacks.

Clarke, Richard A. and Robert Knake. "Cyber War: The Next Threat to National Security and What to Do About It," New York: HarperCollins (2010).

The authors warn of extensive cyber theft of US intellectual property by the PLA and private hacking groups, who provide the information to 'China, Inc.'

Stewart, Joe. "Operation Aurora: Clues in the Code," Dell SecureWorks, 19 January 2010: http://www.secureworks.com/cyber-threat-intelligence/blog/research/20913/.

Stewart argues that Operation Aurora is the latest in a series of attacks originating out of Mainland China. Deducing that the distinctive codebase was all written in Chinese, Stewart concludes: "in my opinion, the use of this unique CRC implementation in Hydraq is evidence that someone from within the PRC authored the Aurora codebase." Furthermore, considering the magnitude of the attack and choice of targets, the evidence indicates a state-sponsored attack campaign.

Krekel, Bryan, George Bakos, and Christopher Barnett. "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation," report prepared by the Northrop Grumman Corporation for the US-China Economic and Security Review Commission (2009).

The scale and complexity of the targeting suggests that efforts are probably sponsored by a mature collection management bureaucracy able to identify and disseminate collection priorities to a diverse set of operators, thereby indicating direct state involvement. The report also identifies six PLA technical reconnaissance bureaus (TRB) with the capability to initiate such attacks located in the Lanzhou, Jinan, Chengdu, Guangzhou, and Beijing regions.

Mazanec, Brian M. "The Art of (Cyber) War," The Journal of International Security Affairs, no.16 (2009).

'Titan Rain' cyberattacks occurred primarily from 2003 to 2005, although some experts believe those responsible are still operating. The attacks involved systematic intrusions into hundreds of US government computers and the networks of our Western allies, with targets ranging from defense contractor networks, military labs, NASA and the World Bank. The US media traced the origin of the attacks to government-sponsored researchers operating out of the Guangdong Province. All evidence supports a state-sanctioned computer network exploitation (CNE) attack.

Mulvenon, James. "PLA Computer Network Operations: Scenarios, Doctrine, Organizations, and Capability," in Beyond the Strait: PLA Missions Other Than Taiwan, eds. Roy Kamphausen, David Lai, and Andrew Scobell, Carlisle, PA: Army War College Strategic Studies Institute (2009).

Mulvenon notes that Chinese military strategists and analysts frequently speak of using cyberattacks to deter the enemy and computer network operations as a powerful asymmetric option to overcome a superior force. He asserts that computer network attack is particularly attractive to the PLA since it has a longer range than conventional weapons, allowing China to directly 'touch' the United States.

Taiwan Ministry of National Defense, Quadrennial Defense Review (2009): http://www.mnd.gov.tw/qdr/en_menu.htm.

> The Taiwanese Defense Ministry asserts: "the PLA has established professional IO Units that […] will wage information operations against its enemies with joint military and civilian participation."

US-China Economic and Security Review Commission. "Hearing on China's Propaganda and Influence Operations, Its Intelligence Activities That Target the United States, and the Resulting Impacts on National Security," Testimony of Kevin Coleman, 30 April 2009.

> In written testimony, Kevin Coleman, senior fellow with the Technolytics Institute, identified China as the perpetrator in numerous computer exploitation activities. He also cited reports of malicious code traced back to China found in the computer systems of oil and gas distributors, telecommunications companies, and financial services industries.

US-China Economic and Security Review Commission. "Hearing on China's Propaganda and Influence Operations, Its Intelligence Activities That Target the United States, and the Resulting Impacts on National Security," Testimony of James Mulvenon, 30 April 2009.

> Mulvenon notes that even analysis of open source material only would reveal that China is one, if not the largest, perpetrator of economic espionage against the United States. Although there is no centralized repository of relevant economic espionage cases, Mulvenon counts at least 25 cases since 2004 that fit the rough pattern of Chinese economic and technological espionage against the United States. While he admits the large number may be owed to a lack of professionalism on the Chinese side, he believes that it is reflective of the enormous scale of the activity.

"China's Cyberattacks," International Institute for Strategic Studies, Strategic Comments 13, no.7 (2007).

> The article references several attacks all traced back to China. German computer systems of the Chancellery, and the foreign, economic, and research ministries were attacked by hackers based in Lanzhou, Guangzhou, and Beijing. The attack on an unclassified computer system in the office of Secretary of Defense Robert Gates was tracked back with a high degree of accuracy to China. Furthermore, the government computer networks in the UK, France, and New Zealand had all been targeted and the cases appeared to originate at least in part from within China.

Marquand, Robert and Ben Arnoldy. "China emerges as leader in cyberwarfare," The Christian Science Monitor, 14 September 2007.

> The reporters cite James Mulvenon, an expert on China's military and director of the Center for Intelligence and Research: "the Chinese are the first to use cyberattacks for political and military goals. Whether it is battlefield preparation or hacking networks connected to the German chancellor, they are the first state actor to jump feet first into

21st century cyberwarfare technology. This is clearly becoming a more serious and open problem." They also remark on the fact that since China puts such strong controls over the internet, it is highly unlikely to have hackers perpetrating attacks without government awareness.

"Merkel's China Visit Marred by Hacking Allegations," SpiegelOnline, 27 August 2007: http://www.spiegel.de/international/world/espionage-report-merkel-s-china-visit-marred-by-hacking-allegations-a-502169.html

Germany's domestic intelligence service discovered a Chinese hacking operation which targeted and infected computers in the German chancellery as well as foreign, economy, and research ministries with Chinese spy software. This attack campaign has made German officials fear whether China may also be targeting the computers of German companies to steal technology secrets.

Tkacik, Jr., John J. "Trojan Dragons: China's International Cyber Warriors" WebMemo published by The Heritage Foundation (2007).

Tkacik reiterates USAF General William Lord's statement: "there is a nation state threat by the Chinese." He comments that PLA cyber warfare units have access to source codes for America's office software, which gives them a 'skeleton key' to access every networked government, military, business, and private computer in America. Tkacik states that China targets the US military most intensely, followed by State Department, Commerce Department, DHS, and sectors relating to commerce, academia, industry, finance, and energy.

Thomas, Timothy L. "Comparing US, Russian, and Chinese Information Operations Concepts," Foreign Military Studies Office, DOD (2004).

Thomas argues that the PLA integrated cyber-warfare units into its standard field-army organization over ten years ago. He cites the Guangzhou City militia and its information-warfare battalion comprised of 'computer-network-warfare' and 'electronic-warfare' companies, both with clearly defined computer network attack units.

Liang, Qiao and Wang Xiangsui. "Unrestricted Warfare: China's Master Plan to Destroy America," translated from the Original Chinese Documents, Panama City, Panama: Pan American Publishing Company (2002).

This book by Chinese experts argues that "With technological developments being in the process of striving to increase the types of weapons, a breakthrough in our thinking can open up the domain of the weapons kingdom at one stroke. As we see it, a single man-made stock-market crash, a single computer virus invasion, or a single rumor or scandal that results in a fluctuation in the enemy country's exchange rates or exposes the leaders of an enemy country on the Internet, all can be included in the ranks of new-concept weapons."

Hachigan, Nina. "China's Cyber-Strategy," Foreign Affairs 80, no.2 (2001): 118-133.

Hachigan outlines the history of China's adoption and use of the internet, commenting that officials in Beijing believe that an adequately designed network will foremost serve the interests of the central government. She also included a 1999 example from when the Taiwanese President announced that Taipei should deal with Beijing on a state-to-state basis and 20 Taiwanese government websites were attacked. Analysts asserted that the hackers were both Chinese civilians and PLA specialists.

Houqing, Wang and Zhang Zingye. "The Science of Military Campaigns," Beijing, China: NDU Press (2000).

PRC strategists write that "we must send a message to the enemy through computer network attack, forcing the enemy to give up without fighting."

Daohai, Lu, ed. "Information Operations," Beijing, China: PLA Arts and Literature Press (1999).

Daohai writes that computer network attacks on nonmilitary targets are designed to "shake war resoluteness, destroy war potential and win the upper hand in war," as an asymmetric, preemptive attack strategy.

Zhongwen, Huo and Wang Zongxiao. "Sources and Techniques of Obtaining National Defense Science and Technology Intelligence," Beijing: Kexue Jishu Wenxuan Publishing Co. (1991): http://www.fas.org/irp/world/china/docs/sources.html.

The authors, who are Chinese military officers) argue that the majority of intelligence requirements can be met by accessing and analyzing open-source material.