25 June 2013

“Chinese Cyber Espionage”

Testimony of

James C. Mulvenon, Ph.D.
Vice-President, Defense Group, Inc. Intelligence Division
Director, Center for Intelligence Research and Analysis

Before the Congressional-Executive Commission on China hearing entitled

“Hearing on Chinese Hacking: Impact on Human Rights and Commercial Rule of Law”

INTRODUCTION

Thank you, Mr. Chairman and the other members of the Congressional-Executive Commission on China for the opportunity to take part in the hearings you are holding today on the topic of "Chinese Hacking: Impact on Human Rights and Commercial Rule of Law." My remarks will focus on Chinese cyber espionage.

Chinese cyber espionage has emerged as a top issue in Sino-US relations, primarily because of concerns about theft of intellectual property. As I discuss in Chapter 9 of my book, *Chinese Industrial Espionage*, there are many different features of Chinese cyber activity towards the United States and there is no "one size fits all" approach for all of them.

The Scale of the Problem

Cyber espionage is the latest and perhaps most devastating form of Chinese espionage, striking at the heart of American military advantage and technological competitiveness. Without mentioning China, General Keith Alexander, NSA Director and Commander, USCYBERCOM, told an audience at the Aspen Security Forum on 26 July 2012 that cyber espionage represents the "greatest transfer of wealth in history." Other government agencies are less circumspect about calling out Beijing for its cyber theft.[i] The Office of the National Counterintelligence Executive's 2011 report *Foreign Spies Stealing US Economic Secrets in Cyberspace* boldly asserts "Chinese actors are the world's most active and persistent perpetrators of economic espionage."[ii] While the media began reporting rumors of large-scale intrusions in 2005,[iii] U.S officials did not publicly acknowledge exfiltrations of data until August 2006, when the Pentagon asserted that hostile civilian cyber units operating inside China had launched attacks against the NIPRNET and downloaded up to 20 terabytes of data.[iv] In March 2007, then Vice-Chairman of the Joint Chiefs General Cartwright told the US-China Economic and Security Review Commission that China was engaged in cyber-reconnaissance, probing computer networks of US agencies and corporations.[v] This view was seconded in the 2007 *China Military Power Report*, an annual Pentagon assessment mandated by the National Defense Authorization Act, which claimed "numerous computer networks around the world, including those owned by the US government, were subject to intrusions that appear to have originated within" the People's Republic of China.[vi] Former White House and DHS cyber official Paul Kurtz told Business Week that the Chinese activity was "espionage on a massive scale"[vii] A 2009 study by Northrup

Grumman for the US-China Economic and Security Review Commission concluded "Chinese espionage in the United States now comprises the single greatest threat to US technology...and has the potential to erode the United States' long-term position as a world leader in S&T [science and technology] innovation and competitiveness."[viii] And the problem appeared to be getting worse over time. Robert Jamison, the top cyber-security official at DHS, told reporters at a March 2008 briefing, "We're concerned that the intrusions are more frequent, and they're more targeted, and they're more sophisticated."[ix] After the Operation Aurora intrusions against Google and other Silicon Valley companies in 2009 and 2010, officials worried that China was escalating its intrusions. Whereas before the activities were targeted at government and military networks, threatening US military advantage and government policies, the new intrusions went beyond state-on-state espionage to threaten American technological competitiveness and economic prosperity.

Because the underlying evidence was classified, government and military officials could not provide detailed evidence of these allegations against the Chinese government and military, which naturally led to scrutiny of the specific attribution to China. In his confirmation testimony questions, current CYBERCOM Commander General Alexander agreed that "attribution can be very difficult."[x] Former senior DHS cybersecurity official Greg Garcia told the New York Times in March 2009 that "attribution is a hall of mirrors."[xi] With respect to China, Amit Yoran, the first director of DHS's National Cyber Security Division cautioned, "I think it's a little bit naive to suggest that everything that says it comes from China comes from China."[xii] Yet other officials were more confident in the assessment of Chinese responsibility. Then Director of the DNI National Counterintelligence Executive, Joel Brenner, told the *National Journal* in 2008:

Some [attacks], we have high confidence, are coming from government-sponsored sites...The Chinese operate both through government agencies, as we do, but they also operate through sponsoring other organizations that are engaging in this kind of international hacking, whether or not under specific direction. It's a kind of cyber-militia...It's coming in volumes that are just staggering.[xiii]

Other reports by non-governmental actors reach varying levels of confidence in their determination of Chinese government involvement.[xiv] Given the technical challenges of attribution, however, a more fruitful approach might be to first understand the strategic context of Chinese cyber espionage, and then ask the question "who benefits?" from the activities attributed to Chinese actors, specifically the possible means, motives and opportunities.

Strategic context of Chinese cyber espionage: China and cyber as an overt tool of state power

As a rising power, Chinese national interests have logically expanded with the growth in its economic, political, diplomatic and military power. Yet its rise has occurred within a world system still dominated by American unilateral authority. Because of these imbalances, China has naturally sought to find asymmetrical advantages, and cyberspace at first glance appears to be a dimension of national power in which the United States is asymmetrically vulnerable because of its greater dependence on information systems. Moreover, China seems much more comfortable with cyber power as an legitimate, overt tool of state power, especially compared with the United States, which still treats cyber operations as a highly classified, compartmented capability. What do we mean by overt? Countries like China and Russia seems more comfortable with the overt use of cyber conflict, even by non-state proxies acting on their behalf, as we saw in numerous Chinese “patriotic hacker” events in the late 1990s and the Russian cyber conflicts in Estonia in 2007 and Georgia in 2008. When confronted with their potential involvement in these incidents, both Beijing and Moscow appeared to believe that the plausible deniability of the network was a sufficient fig leaf to cover their barely veiled affiliations and common cause with the attacks. By contrast, Washington does not even have a vocabulary for discussing these capabilities in public, as seen in the incoherence of official US comments about possible computer network exploit activities against Milosevic during ALLIED FORCE and the Stuxnet industrial control systems hack in 2011.

Why cyber espionage?

Within the rubric of the Chinese government's view of cyber as a tool of national power, it is clear that this new dimension offers Beijing certain key strategic advantages, particularly with respect to intelligence collection, technological competitiveness, intelligence preparation of the battlefield, and strategic intelligence to policymakers.

Intelligence Collection Advantages

Cyber espionage is now a favored mode of tradecraft for China, principally because of its logistical advantages and the promise of plausible deniability. On the first issue, Joel Brenner highlights the relative ease of cyber versus other traditional forms of espionage: “Cyber-networks are the new frontier of counterintelligence...If you can steal information or disrupt an organization by attacking its networks remotely, why go to the trouble of running a spy?”[xv] Take the case of Greg Dongfan Chung, discussed in Chapter 8, as an example. Managing Chung required significant institutional resources, including case officers, covert communications, money transfers, and travel arrangements. In the end, Chung was caught, and his "perp walk" and public trial proved to be an embarrassment to the Chinese government. Now imagine a scenario in which the same volume of information can be exfiltrated out of Boeing or Rockwell's computer networks in a single evening via an exquisite computer network exploitation operation, covered by the plausible deniability of network intrusions. Given the choice between the two modes, it is only natural that intelligence services would increasingly pick the less risky, cheaper, and faster way of doing business.

Technological Competitiveness Advantages

After more than thirty years of serving as the world's assembly point and export processing zone, the Beijing government has clearly made the decision to transform Chinese economic development by encouraging "indigenous innovation."[xvi] Since 2006, James McGregor and others have highlighted "Chinese policies and initiatives aimed at building 'national champion' companies through subsidies and preferential policies while using China's market power to appropriate foreign technology, tweak it and create Chinese 'indigenous innovations' that will come back at us globally."[xvii] In the information technology sector, McGregor notes "Chinese government mandate to replace core foreign technology in critical infrastructure -- such as chips, software and communications hardware -- with Chinese technology within a decade." Among the tools being actively used to achieve these goals are:

> a foreign-focused anti-monopoly law, mandatory technology transfers, compulsory technology licensing, rigged Chinese standards and testing rules, local content requirements, mandates to reveal encryption codes, excessive disclosure for scientific permits and technology patents, discriminatory government procurement policies, and the continued failure to adequately protect intellectual property rights.[xviii]

Missing from this excellent list, however, are traditional technical espionage and technical cyber espionage, which many companies believe are already eroding their technical advantage. The logic for these latter approaches is clearly outlined by David Szady, former head of the FBI's counterintelligence unit: "If they can steal it and do it in five years, why [take longer] to develop it?"[xix] Rather than destroying US competitiveness through "cyberwar," former DNI McConnell argues that Chinese entities "are exploiting our systems for information advantage – looking for the characteristics of a weapons system by a defense contractor or academic research on plasma physics, for example – not in order to destroy data and do damage."[xx]

Examples of Chinese cyber espionage to obtain science and technology can be divided into two broad categories: external and insider. The 2011 NCIX report offers three illustrative examples of insider cyber threats:

- David Yen Lee, a chemist with Valspar Corporation, used his access to internal computer networks between 2008 and 2009 to download approximately 160 secret formulas for paints and coatings to removable storage media. He intended to parlay this proprietary information to obtain a new job with Nippon Paint in Shanghai, China. Lee was arrested in March 2009, pleaded guilty to one count of theft of trade secrets, and was sentenced in December 2010 to 15 months in prison.

- Meng Hong, a DuPont research chemist, downloaded proprietary information on organic light-emitting diodes (OLED) in mid-2009 to his personal email account and thumb drive. He intended to transfer this information to Peking University, where he had accepted a faculty position, and sought Chinese government funding to commercialize OLED research. Hong was arrested in October 2009, pleaded guilty to one count of theft of trade secrets, and was sentenced in October 2010 to 14 months in prison.

- Xiangdong Yu (aka Mike Yu), a product engineer with Ford Motor Company, copied approximately 4,000 For documents onto an external hard drive to help obtain a job with a Chinese automotive company. He was arrested in October 2009, pleaded guilty to two counts of theft of trade secrets, and sentenced in April 2011 to 70 months in prison.[xxi]

External cyber threats to scientific and industrial data, believed to originate in China, have been well-documented in reports by outside vendors. Some examples include:

- In its *Night Dragon* report, McAfee documented "coordinated covert and targeted cyberattacks have been conducted against global oil, energy, and petrochemical companies," "targeting and harvesting sensitive competitive proprietary operations and project-financing information with regard to oil and gas field bids and operations."[xxii]

- In his *Shady Rat* report, McAfee's Dmitry Alperovitch identified 71 compromised organizations in one set of intrusions, including 13 defense contractors, 13 information technology companies, and 6 manufacturing companies.[xxiii]

- In January 2010, Google reported a "highly sophisticated and targeted attack on our corporate infrastructure originating from China that resulted in the theft of intellectual property," including source code.[xxiv] Google claimed that the intrusion also targeted "at least twenty other large companies from a wide range of businesses--including the Internet, finance, technology, media and chemical sectors," and was corroborated in separate admissions by Adobe,[xxv]

- In its *GhostNet* report, researchers at Information Warfare Monitor found 1,295 infected computers in 103 countries, including a range of political, diplomatic and economic target organizations such as Deloitte and Touche's New York office.[xxvi] The follow-on report, *Shadows in the Cloud*, identified additional targets, including Honeywell.[xxvii]

Each of these reported intrusions were traced to IP addresses in China, and almost certainly represent only a fraction of the known hacks, given the reluctance of companies to report data breaches.

Intelligence Preparation of the Battlefield (IPB)

It is also important to contextualize China’s interest in cyber espionage within Beijing’s threat perceptions of potential scenarios for military conflict. In the minds of the Chinese leadership, the available evidence suggests that the most important political-military challenges and the most likely flashpoints for Sino-US conflict involve Taiwan or the

South China Sea. Should the late 1990s, the PLA has been hard at work bolstering the hedging options of the leadership, developing advanced campaign doctrines, testing the concepts in increasingly complex training and exercises, and integrating new indigenous and imported weapons systems.

Yet cyber operations are also expected to play an important role in these scenarios, necessitating intelligence preparation of the cyber battlefield. At the strategic level, the writings of Chinese military authors suggest that there are two main centers of gravity in a Taiwan scenario, both of which can be attacked with computer network operations in concert with other kinetic and non-kinetic capabilities. The first of these is the will of the Taiwanese people, which they hope to undermine through exercises, cyber attacks against critical infrastructure, missile attacks, SOF operations, and other operations that have a psyop focus. Based on assessments from the 1995-1996 exercises, as well as public opinion polling in Taiwan, China appears to have concluded that the Taiwanese people do not have the stomach for conflict and will therefore sue for peace after suffering only a small amount of pain. The second center of gravity is the will and capability of the United States to intervene decisively in a cross-strait conflict. In a strategic sense, China has traditionally believed that its ICBM inventory, which is capable of striking CONUS, will serve as a deterrent to US intervention or at least a brake on escalation.[xxviii]

Closer to its borders, the PLA has been engaged in an active program of equipment modernization, purchasing niche "counter-intervention" capabilities such as anti-ship ballistic missiles, long-range cruise missiles and submarines to shape the operational calculus of the American carrier strike group commander on station.[xxix] According to the predictable cadre of “true believers,” both of the centers of gravity identified above can be attacked using computer network operations. In the first case, the Chinese IO community believes that CNO will play a useful psychological role in undermining the will of the Taiwanese people by attacking infrastructure and economic vitality. In the second case, the Chinese IO community envisions computer network attacks against unclassified NIPRNET and its automated logistics systems as an effective way to deter or delay US intervention into a military contingency and thereby permit Beijing to achieve its political objectives with a minimum of fighting. *In both cases, China must conduct substantial computer network exploitation (the military term for cyber espionage) for intelligence preparation of this battlefield, and the alleged intrusion set into NIPRNET computer systems would appear to fulfill this military requirement.*

Why does the Chinese military believe that the deployment phase of US military operations, particularly the use of the unclassified NIPRNET for logistics deployments, is the primary focus of vulnerability? Since DESERT STORM in the early 1990s, the PLA has expended significant resources analyzing the operations of what it often and euphemistically terms “the high-tech enemy.”[xxx] When Chinese strategists contemplate how to affect US deployments, they confront the limitations of their current conventional force, which does not have range sufficient to interdict US facilities or assets beyond the Japanese home islands.[xxxi] Nuclear options, while theoretically available, are nonetheless far too escalatory to be used so early in the conflict.[xxxii] Theater missile systems, which are possibly moving to a mixture of conventional and nuclear warheads, could be used against Japan or Guam, but uncertainties about the nature of a given warhead would likely generate responses similar to the nuclear scenario.[xxxiii] Instead, PLA analysts of US military operations presciently concluded that the key vulnerability was the mechanics of deployment itself. Specifically, Chinese authors highlight DoD’s need to use civilian backbone and unclassified computer networks (known as the NIPRNET), which is a function of the requirements of global power projection, as an "Achilles Heel." There is also recognition of the fact that operations in the Pacific are especially reliant on precisely coordinated transportation, communications, and logistics networks, given what PACOM calls the “tyranny of distance”[xxxiv] in the theater. PLA strategists believe that a disruptive computer network attack against these systems or affiliated civilian systems could potentially delay or degrade US force deployment to the region while allowing the PRC to maintain a degree of plausible deniability.

The Chinese are right to highlight the NIPRNET as an attractive *and* accessible target, unlike its classified counterparts. It is attractive because it contains and transmits critical deployment information in the all-important time-phased force deployment list (known as the “tip-fiddle”), which is valuable for both intelligence-gathering about US military operations but also a lucrative target for disruptive attacks. In terms of accessibility, it was relatively easy to gather data about the NIRPNET from open sources, at least before 9/11. Moreover, the very nature of the system is the source of its vulnerabilities, since the needs of global power project mandate that it has to be unclassified and connected to the greater global network, albeit through protected gateways.[xxxv]

DoD’s classified networks, on the other hand, are an attractive but less accessible target for the Chinese. On the one hand, these networks would be an intelligence gold mine, and is likely a priority computer network exploit target. On the other hand, they are less attractive as a computer network attack target, thanks to the difficulty of penetrating its high defenses. Any overall Chinese military strategy predicated on a high degree of success in penetrating these networks during crisis or war is a high-risk venture, and increases the chances of failure of the overall effort to an unacceptable level.

Chinese CNE or CNA operations against logistics networks could have a detrimental impact on US logistics support to operations. PRC computer network exploit activities directed against US military logistics networks could reveal force deployment information, such as the names of ships deployed, readiness status of various units, timing and destination of deployments, and rendezvous schedules. This is especially important for the Chinese in times of crisis, since the PRC in peacetime utilizes US military web sites and newspapers as a principal source for deployment information. An article in October 2001 in *People's Daily*, for example, explicitly cited US Navy web sites for information about the origins, destination and purpose of two carrier battle groups exercising in the South China Sea.[xxxvi] Since the quantity and quality of deployment information on open websites has been dramatically reduced after 9/11, the intelligence benefits (necessity?) of exploiting the NIPRNET have become even more paramount.[xxxvii] Computer network attack could also delay re-supply to the theater by misdirecting stores, fuel, and munitions, corrupting or deleting inventory files, and thereby hindering mission capability.

The advantages to this strategy are numerous: (1) it is available to the PLA in the near-term; (2) it does not require the PLA to be able to attack/invade Taiwan with air/sea assets; (3) it has a reasonable level of deniability, provided that the attack is sophisticated enough to prevent tracing; (4) it exploits perceived US casualty aversion, over-attention to force protection, the tyranny of distance in the Pacific, and US dependence on information systems; and (5) it could achieve the desired operational and psychological effects: deterrence of US response or degrading of deployments. *Looking back over more than ten years of China-origin intrusions into the very NIPRNET systems identified by PLA analysts as a high-priority network attack target as early as 1995, the logic of the intrusion sets becomes much clearer.*

Strategic Intelligence

An additional motivation for cyber espionage is strategic intelligence about the policies and intentions of civilian and military officials as well as the internals of debates within the US government and political parties:

1. In June 2006, the State Department was victimized by a series of intrusions at its foreign posts and headquarters in Washington. According to the *Associated Press*, “hackers stole sensitive information and passwords, and implanted ‘back doors’ in unclassified computers to allow them to return.” Employees told the *AP* that State’s East Asian and Pacific Affairs Bureau was particularly hard hit by the intrusion, suggesting that the intruders had a special interest in Asia-related information.[xxxviii] Two reporters from *Business Week* relate the story of what happened:

"The attack began in May, 2006, when an unwitting employee in the State Dept.'s East Asia Pacific region clicked on an attachment in a seemingly authentic e-mail. Malicious code was embedded in the Word document, a congressional speech, and opened a Trojan "back door" for the code's creators to peer inside the State Dept.'s innermost networks. Soon, cyber security engineers began spotting more intrusions in State Dept. computers across the globe. The malware took advantage of previously unknown vulnerabilities in the Microsoft operating system. Unable to develop a patch quickly enough, engineers watched helplessly as streams of State Dept. data slipped through the back door and into the Internet ether. Although they were unable to fix the vulnerability, specialists came up with a temporary scheme to block further infections. They also yanked connections to the Internet. One member of the emergency team summoned to the scene recalls that each time cyber security professionals thought they had eliminated the source of a "beacon" reporting back to its master, another popped up. He compared the effort to the arcade game Whack-A-Mole. The State Dept. says it eradicated the infection, but only after sanitizing scores of infected computers and servers and changing passwords."[xxxix]

2. In 2007, intruders broke into the e-mail system for Defense Secretary Robert Gates’s office, and the Pentagon shut down about 1,500 computers for more than a week while the attacks continued. Officials told the *Financial Times* “an internal investigation has revealed that the incursion came from the People’s Liberation Army. One senior US official said the Pentagon had pinpointed the exact origins of the attack. Another person familiar with the event said there was a ‘very high

level of confidence...trending towards total certainty' that the PLA was responsible."[xl]

3. In the summer of 2008, the FBI informed both the Obama and McCain presidential campaigns that their computer systems had been infiltrated. *Newsweek* quoted an FBI agent as telling both teams: "You have a problem way bigger than what you understand...You have been compromised, and a serious amount of files have been loaded off your system."[xli] The *Financial Times* later cited investigators "had determined that the attacks originated from China, but cautioned that they had not ascertained whether they were government-sponsored, or just unaffiliated hackers."[xlii] In a cybersecurity policy speech early in his Presidency, Obama referred to the incident: "I know how it feels to have privacy violated because it has happened to me and the people around me. It's no secret that my presidential campaign harnessed the Internet and technology to transform our politics. What isn't widely known is that during the general election hackers managed to penetrate our computer systems. To all of you who donated to our campaign, I want you to all rest assured, our fundraising website was untouched. So your confidential personal and financial information was protected. But between August and October, hackers gained access to emails and a range of campaign files, from policy position papers to travel plans. And we worked closely with the CIA -- with the FBI and the Secret Service and hired security consultants to restore the security of our systems."[xliii]

These three sample cases show that Beijing clearly views cyber as a collection modality for obtaining strategic intelligence at the highest levels of the US Government.

Chinese government denials

"The lady doth protest too much, methinks" – Shakespeare, *Macbeth*

In counterintelligence offices in Washington, one often sees the following sign: "Admit Nothing, Deny Everything, Make Vigorous Counter-Accusations". This philosophy is also a deeply held conviction of the Chinese side when it comes to discussing their possible role in cyber intrusions. First, they admit nothing and deny everything. When asked about the China-origin intrusions into German Chancellor Angela Merkel's office network, for example, "the Chinese Embassy in Berlin describing the accusation of state-controlled hacking as “irresponsible speculation without a shred of evidence.”[xliv] Chinese officials also point to Chinese laws as an ironclad defense of its own lack of involvement. Reacting to accusations from that Chinese hackers were responsible for the intrusions revealed by Google in January 2010, Foreign Ministry spokeswoman Jiang Yu countered that "Chinese law proscribes any form of hacking activity."[xlv] After the release of the Office of the National Counterintelligence Executive's 2011 "Report to Congress on Foreign Economic Collection and Industrial Espionage," Chinese officials denigrated the quality of the analysis, asserting that "identifying the attackers without carrying out a comprehensive investigation and making inferences about the attackers is both unprofessional and irresponsible."[xlvi] Then, the Chinese government impugns the motives of the accusers, making its own counter-accusations. In his response to questions about GhostNet, Foreign Ministry spokesman Qin Gang accused foreigners of having a “Cold War mentality”:

> The problem now is that some people abroad are keen to fabricate the rumor of the so-called ‘Chinese cyber spy network.’ The allegation is utterly groundless...There is a ghost called Cold War and a virus called China's threat theory overseas. Some people, possessed by this ghost and infected with this virus, fall ill from time to time. Their attempts of using rumors to disgrace China will never succeed. We should rightly expose these ghosts and viruses.[xlvii]

Wang Baodong, a spokesman for the Chinese government at its embassy in Washington, darkly hinted that "anti-China forces" are behind the allegations.[xlviii] After the US-China Economic and Security Review Commission’s release of a Northrup-Grumman report on Chinese cyber espionage, Qin Gang railed:

> The report takes no regard of the true situation..It is full of prejudice, and out of ulterior motive. We urge the so-called commission not to see China through colored lens and not to do things that interfere with China’s internal affairs and undermine China-US relations.[xlix]

Finally, the Chinese government describes itself as the victim of cyber intrusions**.** After a detailed expose of Chinese cyber espionage appeared in *Business Week*, Wang Baodong emailed the magazine’s editors, claiming that China is "frequently intruded and attacked by hackers from certain countries."[l] When asked in early 2010 about Google's complaint that it had been hacked from China, Foreign Ministry spokesman Ma Zhaoxu said

Chinese companies have also been hacked, adding that China resolutely opposes the practice.[li] Other officials have cited the fact that most of the world's botnets are controlled from servers in the United States, insinuating that Washington needed to get its own cybersecurity in order before accusing other countries of hacking. Finally, the Chinese government tries to paint itself as the patron of global cybersecurity, in contrast to the "militarized" US approach to cyber: "China is ready to build, together with other countries, a peaceful, secure and open cyberspace order."[lii] While Beijing's style of strategic communications is not limited to cyber espionage, as seen in its rhetoric during crises (Belgrade Embassy bombing in 1999, EP-3A hostage crisis in 2001, etc..), the reaction of its officials has the unintended consequence of increasing suspicion.

How good are they? Or does it matter?

Measuring Chinese cyber espionage capability also involves the assessment of a group or country's ability to generate new attack tools or exploits. Outside analysts, many of whom are programmers themselves, tend to reify countries like Russia that abound with highly talented programmers, and look down upon countries or individuals that simply use off-the-shelf "script kiddie" tools or exploit known vulnerabilities, preferring to admire more advanced cyber operators who can discover their own "zero-day" vulnerabilities.[liii] Indeed, analysts who have examined Chinese intrusions in detail often comment on their relative lack of sophistication and especially their sloppy tradecraft,[liv] leaving behind clear evidence of the intrusion and sometimes even attribution-related information. For example, analysts who examined possible Chinese intrusions into energy companies concluded that Chinese hackers were "incredibly sloppy," "very unsophisticated," "made mistakes and left lots of evidence."[lv] Perhaps the Chinese cyber operators are so convinced of the plausible deniability afforded by the current global network architecture that they do not see the need to hide more effectively, or perhaps they believe that their communications are secure because they are using Chinese language. Both are true to some extent, especially the latter, as many Chinese correctly perceive that their difficult language is actually the country's first line of defense, its first layer of cryptography, and there actually few foreigners with the skills or bandwidth to penetrate the veil. Most important, however, the Chinese probably perceive that they do not need to "up their game" because their relatively primitive and sloppy efforts have thus far been wildly successful and therefore see no need to change. In fact, one could argue that China's cyber espionage successes to date are more a function of the vulnerability of US systems than any inherent capability on the Chinese side. As time passes, however, one would expect Chinese capability to improve, particularly as information about China-origin intrusions becomes more widespread and victims begin to take concrete measures to protect themselves. This view is endorsed by former counterintelligence chief Joel Brenner, who told the *National Journal* in 2008 that Chinese hackers are "very good and getting better all the time."[lvi]

[i] "General Warns of Dramatic Increase of Cyber-Attacks on US Firms," *Los Angeles Times*, 27 July 2012.

[ii] Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011*, October 2011, http://www.dni.gov/reports/20111103_report_fecie.pdf

[iii] Tom Espiner, "Chinese Hackers US Military Defenses," *Silicon,com*, November 2005; and Bradley Graham, "Hackers Attack Via Chinese Web Sites," *The Washington Post*, August 2005.

[iv] Dawn Onley, Dawn and Patience Wait, "Red Storm Rising: DoD's Efforts to Stave Off Nation- State Cyber Attacks Begin with China," *Government Computer News*, August 2006.

[v] See General James E. Cartwright, in hearing, *China's Military Modernization and Its Impact on the United States and the Asia-Pacific,* US-China Economic and Security Review Commission, 110th Cong, 1st Sess., March 29-30, 2007, p. 90, at www.uscc.gov/hearings/2007hearings/transcripts/mar_29_30/mar_29_30_07_trans.pdf.

[vi] Shane Harris, "China's Cyber Militia," *National Journal*, 31 May 2008.

[vii] Brian Grow, Keith Epstein and Chi-Chu Tschang, "The New E-spionage Threat," *Business Week*, 21 April 2008, pp.32-41.

[viii] Bryan Krekel, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, published by the US-China Economic and Security Review Commission, 9 October 2009.

[ix] Harris, “China’s Cyber Militia.”

[x] "Advance Questions for Lieutenant General Keith Alexander USA, Nominee for Commander, United States Cyber Command," published by Senate Armed Services Committee, accessed at: http://armed-services.senate.gov/statemnt/2010/04%20April/Alexander%2004-15-10.pdf

[xi] Shaun Waterman, “Chinese Cyberspy Network Pervasive,” *Washington Times*, 30 March 2009.

[xii] Harris “China’s Cyber Militia.”

[xiii] Ibid.

[xiv] For a range of views on the attribution issue, see Krekel, *Capability of the People’s Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*; McAfee® Foundstone® Professional Services and McAfee Labs™, *Global Energy Cyberattacks: ‘Night Dragon’*, 10 February 2011; Shishir Nagaraja and Ross Anderson, “The Snooping Dragon: Social-Malware Surveillance of the Tibetan Movement,” UCAM-CL-TR-746, University of Cambridge Computer Laboratory Technical Report 746, March 2009; Dmitri Alperovitch, *Revealed: Operation Shady RAT*, McAfee, August 2011; and Information Warfare Monitor, *Tracking GhostNet: Investigating a Cyber Espionage Network*, Toronto: SecDev and Citizen Lab, 29 March 2009.

[xv] Harris, “China’s Cyber Militia.”

[xvi] James McGregor, “China’ s Drive for ‘indigenous Innovation;: A Web of Industrial Policies,” Washington, DC: US Chamber of Commerce, July 2010.

[xvii] James McGregor, "Time to rethink US-China trade relations," *Washington Post*, 19 May 2010. See also McGregor, “China's Drive for 'Indigenous Innovation.”

[xviii] Ibid.

[xix] Nathan Thornburgh, “The Invasion of the Chinese Cyberspies (and the Man Who Tried to Stop Them,” *Time*, 29 August 2005.

[xx] Nathan Gardels, "China is Aiming at America’s Soft Underbelly: The Internet," *The Christian Science Monitor*, 5 February 2010, accessed at:

http://www.csmonitor.com/Commentary/Global-Viewpoint/2010/0205/China-is-aiming-at-America-s-soft-underbelly-the-Internet

[xxi] Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace.*

[xxii] McAfee, *Night Dragon*.

[xxiii] Alperovitch, *Operation Shady RAT*.

[xxiv] http://googleblog.blogspot.com/2010/01/new-approach-to-china.html

[xxv] http://blogs.adobe.com/conversations/2010/01/adobe_investigates_corporate_n.html

[xxvi] Information Warfare Monitor, *Tracking GhostNet: Investigating a Cyber Espionage Network*, Toronto: SecDev and Citizen Lab, 29 March 2009, accessed at: http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network

[xxvii] Information Warfare Monitor and Shadowserver, *Shadows in the Cloud: Investigating Cyber Espionage 2.0*, Toronto: SecDec and Citizen Lab, 6 April 2010, found at www.shadows-in-the-cloud.net

[xxviii] Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2011*, p.3.

[xxix] Ibid., pp.2-4, 28-29.

[xxx] Ibid., p.22.

[xxxi] Ibid., p.31.

[xxxii] Ibid., p.34.

[xxxiii] Ibid., pp.29,78.

[xxxiv] For a PACOM/J4 perspective on the issue, see http://www.navsup.navy.mil/scnewsletter/2009/jan-feb/cover1

[xxxv] For an unclassified summary, see http://www.disa.mil/Services/Network-Services/Data/SBU-IP.

[xxxvi] “Whom, If Not China, Is US Aircraft Carriers' Moving onto South China Sea Directed Against?” *Renmin Ribao*, 24 August 2001.

[xxxvii] The Department of Defense’s revised web site administration guidance, which can be found here

(http://www.defenselink.mil/webmasters/policy/dod_web_policy_12071998_with_amendments_and_corrections.html), specifically prohibits the following: "3.5.3.2. Reference to unclassified information that would reveal sensitive movements of military assets or the location of units, installations, or personnel where uncertainty regarding location is an element of a military plan or program."

[xxxviii] "Computer Hackers Attack State Dept.," *Associated Press*, 12 July 2006.

[xxxix] Grow, Epstein and Tschang, "The New E-spionage Threat."

[xl] Sevastopluo, Demetri, "Chinese Hacked into Pentagon," *FT.com*, 3 September 2007.

[xli] Evan Thomas, "Center Stage," *Newsweek*, 6 November 2008; David Byers, Tom Baldwin and Tim Reid, "Obama computers 'hacked during election campaign'," *Times Online*, 7 November 2008.

[xlii] *Financial Times*, November 2008.

[xliii] "Remarks by the President on Securing our Nation's Cyber Infrastructure," Office of the Press Secretary, The White House, 29 May 2009.

[xliv] "Merkel's China Visit Marred by Hacking Allegations," *Spiegel Online International*, 27 August 2007.

[xlv] Helft, Miguel, and John Markoff, "Google Alerted Activists of Attacks," *New York Times*, 15 January 2010.

[xlvi] "China Rebuts US Accusation of Hacker Attacks," *China Daily*, 31 October 2011.

[xlvii] "China Denies Allegations on 'Cyber Spy Network'."

[xlviii] Grow, Epstein and Tschang, "The New E-spionage Threat."

[xlix] Clayton, Mark, "Google cyber attack: the evidence against China," *Christian Science Monitor*, 13 January 2010.

[l] Grow, Epstein and Tschang, "The New E-spionage Threat."

[li] "China Says Google, Foreign Firms Must Respect Laws," *CIOL*, 19 January 2010.

[lii] "China Rebuts US Accusation of Hacker Attacks," *China Daily*, 31 October 2011.

[liii] http://en.wikipedia.org/wiki/Zero-day_attack

[liv] Keizer, Gregg, “Chinese Hackers Called Sloppy but Persistent,” *Computerworld*, 12 February 2011.

[lv] Ibid.

[lvi] Harris, “China’s Cyber Militia.”