China's Approach to Cyber Operations: Implications for the United States

Testimony before the Committee on Foreign Affairs

House of Representatives

Hearing on "The Google Predicament: Transforming U.S. Cyberspace Policy to Advance Democracy, Security, and Trade."

By

Larry M. Wortzel

Commissioner
U.S.-China Economic and Security Review Commission

Wednesday, March 10, 2010

Rayburn House Office Building

China's Approach to Cyber Operations: Implications for the United States

Larry M. Wortzel

Chairman Berman, Ranking Member Ros-Lehtinen, Members of the Committee, thank you for the opportunity to appear today to discuss how the People's Republic of China approaches cyber warfare, cyber espionage, and how the United States might respond.

It is a pleasure to appear before you today on an issue of great significance to the United States and, indeed, the world. The views I will present here today are my own. They are a product not only of my service on the U.S.-China Economic and Security Review Commission, but from my service as a military officer with significant background in intelligence and counterintelligence activities as well as decades of study of China.

The attacks on Google that prompted this hearing are the most recent example of a series of penetrations into the computer networks of American companies, departments of the U.S Government, and even some members of Congress.

As the U.S.-China Economic and Security Review Commission has documented in its 2009 *Annual Report to Congress*, "China is the origin of extensive malicious cyber activities that target the United States."[1] Attribution of cyber penetrations and malicious cyber activity is difficult, and even quite sensitive, because if one describes how attribution is achieved, it tells the intruder how to modify its operations and make them more effective.

Our Commission, in a contracted report on "The Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation," provided a case study of a multi-day penetration into the computer systems of an American high technology company and how the data acquired was transferred to an Internet protocol address in China.[2] The report also discussed the principal institutional and individual "actors" in Chinese computer network operations as well as the characteristics of network exploitation activities that are frequently attributed to China.

In the case of the Google penetrations, apparently servers at two schools in China, Jiaotong University in Shanghai and Lanxiang Vocational School in Shandong Province, were used in routing the attacks.[3] Still, even if the attacks can be traced to China, it is not clear who ordered the attacks. I want to give you my own views on how, through circumstantial evidence, knowledge of the organizations in China responsible for intelligence, security activities and repression or control of the Chinese population, and logic, one can pick out the most likely actors in some of these Chinese computer networks operations.

I will discuss three types of malicious Chinese computer network operations: Those that strengthen political and economic control in China; those that gather economic, military or technology intelligence and information; and those that reconnoiter, map and gather targeting information in U.S. military, government, civil infrastructure or corporate networks for later exploitation or attack.

First, skilled computer operators in China routinely exploit systems to gain information about what certain political dissidents may say, how they use the web, and with whom they may communicate. The organizations in China most likely to put the information related to individual accounts belonging to people who may be politically active taken in the Google penetrations to use are those responsible for internal security, repression or control of the Chinese population, and control over the distribution of information. These are the Ministry of State Security, the Public Security Bureau, and organizations of the Chinese Communist Party such as the Party's Central Propaganda Department.[4]

I concede that I cannot prove this beyond a reasonable doubt in a court of law. There may be a group of patriotic hackers in China who just hate criticism of the Communist Party and would take such action. But I believe such persistent, systematic and sophisticated attacks, some of which have taken place in the United States, in China, in Germany, and in the United Kingdom, most likely are state-directed. In addition to the Google attacks, there have been attacks on such religious groups as Falun Gong and on adherents of the Dalai Lama, both of which have been singled out by the Chinese Communist Party leadership for suppression. It is the organs of control and repression in China that need the type of information that was extracted from Google and who most profit from such penetrations.

The second type of malicious activity is designed to gather information of military, technical, scientific or economic value. Gathering this type of information may speed the development and fielding of weapons in China, improve technology in sectors of China's industries while saving time and money in research and development, and often compromises valuable intellectual property. The organizations of the Chinese government with the missions and capabilities to conduct such activities span both military and civilian agencies in China, to include the People's Liberation Army (PLA) Technology Reconnaissance Department (signals intelligence or 3rd Department); the Electronic Countermeasures and Radar Department (4th Department); the Ministry of State Security; and the state-owned companies in China's broad military-industrial complex.[5]

Not all of this cyber espionage may be government controlled.[6] There may be plenty of cyber-espionage "entrepreneurs" in China who operate outside government control that could be working on behalf of Chinese companies or the 54 state-run science and technology parks around the country.

Let us be candid, however. When the Department of Justice is prosecuting several espionage cases involving the acquisition of defense technology or information from US companies or Department of Defense agencies, an unidentified official of the Chinese government is cited as the recipient of the information, and the same type of data is being stolen by cyber penetrations, a logical person would conclude that some of this activity is directed by the Chinese government.

The recent attacks against Google exhibit the traits of both of these types of attacks. Google's investigators discovered that, not only had the "Gmail" accounts of Chinese rights activists been compromised, but Google's most cherished intellectual property--its source code--had been targeted.[7] It is therefore both the organs of control and repression in China, as well as China's technological base, that need the type of information that was extracted from Google and who most profit from the penetrations.

The third type of cyber activity may be the most dangerous for our national security. This is where foreign intelligence or military services penetrate the computers that control our vital national infrastructure or our military, reconnoiter them electronically, and map or target nodes in the systems for future penetration or attack. Malicious code is often left behind to facilitate future entry.

Regarding this third type of computer network penetration by China, General James Cartwright, then Commander of the U.S. Strategic Command (USSTRATCOM) and currently Vice Chairman of the Joint Chiefs of Staff, suggested that "I don't think the [United States] has gotten its head around the issue yet, but I think that we should start to consider that [effects] associated with a cyber attack could, in fact, be in the magnitude of a weapon of mass destruction."[8]

General Cartwright testified before the U.S.-China Economic and Security Review Commission that China is actively engaging in cyber reconnaissance by probing the computer networks of U.S. government agencies as well as private companies.[9] General Cartwright told the Commission that a denial of service attack by China has the potential to cause cataclysmic harm if conducted against the United States on a large scale and could paralyze critical infrastructure or military command and control. China currently is thought by many analysts to have the world's largest denial-of-service capability.[10]

The data collected from these computer reconnaissance campaigns can be used for myriad purposes. Obviously, it has intelligence value for the information that may be extracted. It also helps to identify weak points in the networks. Probes into government systems help a potential adversary to understand how leaders in the United States think and to discover the communication patterns of American government agencies and private companies. General Cartwright testified that this information is akin to that which in times past had to be gathered by human intelligence over a much longer period of time. Computer penetrations also amount to extensions into a different part of the electromagnetic spectrum of warfare and information gathering that had been done by signals intelligence collection. Cartwright went on to say that in today's information environment, the intelligence exfiltration that once took years can be accomplished in a matter of minutes in a single download session.

In a recent editorial, former National Security Agency director and Director of National Intelligence Admiral Mike McConnell reinforced General Cartwright's admonition. Admiral McConnell argued that just as in the Cold War when the United States aimed to protect itself against nuclear attack, today we must endeavor to protect "our power grids, air and ground transportation, telecommunications, and water filtration systems" against the chaos that could result from successful cyber attacks.[11]

In April 2007, while in China, a delegation of Commissioners met with officers from the PLA's premier strategy research institute, the Academy of Military Sciences. When questioned about cyber attacks, the Chinese military officers noted that scholars hold differing opinions about whether a computer network attack may constitute an act of war. Some argued it meets that definition, but others argued that a network attack alone without corresponding conventional attacks does not constitute an act of war.

However, the PLA officers acknowledged that if a cyber attack targets the military capabilities of another country and does significant damage, conventional counterattacks are warranted. They also noted the frequent difficulty in accurately identifying the source of cyber attacks and argued that the source must be clearly identified before a counterattack could be responsibly launched.

Mr. Chairman, Ranking Member Ros-Lehtinen, computer systems play a crucial role in modern economies today. They are vital links in the transmission of energy, fuel, power, banking and financial data, and transportation systems.[12] They are also key components in our national security.

As important components of our national security, however, they make excellent targets. Our unclassified government and military computer systems also have been penetrated, as discussed in the U.S.-China Economic and Security Review Commission reports cited earlier. Data related to our newest defense systems has been compromised and information therein exfiltrated, probably to China, including "several terabytes of data related to design and electronics systems" of the F35 Lightning II, one of the United States' most advanced fighter planes."[13]

According to an article in the *Wall Street Journal,* a senior U.S. intelligence official told the newspaper that "The Chinese have attempted to map our infrastructure, such as the electrical grid, so have the Russians."[14] The article also cites a former Department of Homeland Security Official, who told the *WSJ* that "the espionage appeared pervasive across the U.S. and doesn't target a particular company or region."

The types of activities discussed the *Wall Street Journal* article are not mere speculation on the part of U.S. officials. Chinese researchers at the Institute of Systems Engineering of Dalian University of Technology published a paper on how to attack a small U.S. power grid sub-network in a way that would cause a cascading failure of the entire U.S. west-coast power grid.[15] Ironically, the two Chinese researchers got access to the power grid vulnerability data from U.S. public information. Two other researchers in China, exploiting academic publications from American researchers, analyzed the shortcoming of computer network attacks and introduced a new network attack platform that could include "viruses, worm classes, and a Trojan Horse logic bomb."[16]

Lieutenant General Liu Jixian, of the PLA Academy of Military Science, writes that the PLA must develop asymmetrical capabilities including space-based information support, and networked-focused ‘soft attack,’ against potential enemies.[17] Xu Rongsheng, Chief Scientist at the Cyber Security Lab of the Institute for High Energy Physics of the Chinese Academy of Sciences, told a Chinese news reporter that:

> *“Cyber warfare may be carried out in two ways. In wartimes, disrupt and damage the networks of infrastructure facilities, such as power systems, telecommunications systems, and education systems, in a country; or in military engagements, the cyber technology of the military forces can be turned into combat capabilities.”*[18]

Other military strategists from China’s military academies and schools of warfare theory have suggested that the PLA ought to have the capability to alter information in military command and control or logistics systems to deceive U.S. forces on resupply missions or divert supplies, as well as to be able to paralyze ports and airports by cyber or precision weapon attacks on critical infrastructure.[19]

Simply stated, the Chinese armed forces and the security services take the United States as a potential enemy. Conflict is not a certainty, but cyber operations and cyber intelligence collection are already underway and there are regular attacks on the United States from sites in China.

Chinese People’s Liberation Army organizations are being trained and prepared in military doctrine to “expand the types of targets or objectives for armed conflict to command and control systems, communications systems and infrastructure.”[20] Military strategist Wang Pufeng argues that “battlefield situations awareness is the core of information age warfare, which means that one must be able to destroy or jam the systems that are fundamental to [an adversary’s] situational awareness.”[21]

With regard to information warfare, Wang Baocun, one of the leading information warfare specialists in the Chinese military, reminds readers in China that “the global information grid and global command and control systems are fundamental to the American defense system, including global positioning satellites.”[22] In other Chinese military publications, there are suggestions that to be successful in information age warfare, one’s own military must have certain capabilities and must be able to interfere with an adversary’s ability to exploit the results of “reconnaissance, thermal imaging, ballistic missile warning, and radar sensing.”[23]

All of this suggests that it is the Chinese military and intelligence services that are behind many of the penetrations of our defense systems. In response, the United States should take measures to strengthen the cyber and critical infrastructure of the nation. Senior officials in the Defense and State Departments should not hesitate to raise with Chinese officials complaints about cyber penetrations or attempts to use computer systems and the World Wide Web to further repress the Chinese people, or to attack people who speak out in other counties about Chinese oppression.

At the same time, we should keep in mind that in some areas of cyber crime, such as credit card theft rings and the theft of banking information, China's law enforcement services have cooperated with the United States. And not all computer-hacking in China is controlled by the government. For certain types of banking and criminal activities, China has prosecuted its hackers.

In the following paragraphs I present some of my own views on cyber defenses and policy for your consideration:

We must monitor and defend our computer systems. Deploying robust intrusion detection systems such as the EINSTEIN 2 and 3 systems to monitor computer network flow and give us real-time alerts about malicious or harmful activity on our government computer systems is crucial to national security.[24] This type of scanning should be expanded to include monitoring activity on critical infrastructure networks and on defense contractors who are working on classified defense programs.

Congress should ensure that the appropriate federal agencies are working with their counterparts in allied and friendly countries to detect and combat malicious cyber activity.

The U.S. government must assist in protecting U.S. critical infrastructure systems and, in fact, has the obligation to do so. The government should not inhibit industry's efforts to protect itself and should help ensure that utilities, banks, and businesses have the tools necessary for cyber defense. Regarding this issue, the National Research Council suggests that private companies (including those that operate the nation's infrastructure) may undertake all the passive defensive actions they see fit, and that the government should provide assistance.[25]

The Critical Infrastructure Protection Act (PL 107-296) created a program that enhances information-sharing between the private sector and government and protects the information that is shared. However, if might be useful to review anti-trust exemptions for companies that share information on infrastructure protection. The Internet Security Alliance has called for such a review.

What is left unresolved in law, however, according to a 2009 National Research Council study, is whether private companies and individuals have the right of self-defense through an active response (a counterattack). The Council suggests a review of the Computer Fraud and Abuse Act, Title 18 USC, Section 1030, with a goal of clarifying provisions of the law that make intentional damaging of any computer connected to the Internet a crime and exploring whether an active response should be criminalized.[26] The National Research Council report also presents an excellent discussion of the costs and benefits associated with any government counterattacks.[27]

It will be impossible for the government to pay for all of the necessary security improvements to the level required by the current threat, especially with the private sector running so many parts of our nation's critical infrastructure. The assessment of who will foot the bill must be done on a case-by-case basis. However, the government must set minimum standards for protection and if industry fails to implement the appropriate levels of protection, then the government will likely have to intervene and enforce stricter regulations.

Congress could assist in this process by enacting reforms that would allow infrastructure owners to deduct the full cost of security-related spending in the year such expenses are incurred. Allowing industries to write off security spending all at once will reduce the significant costs, thereby improving the all-important bottom line for companies investing in security.

Attacks such as the one on Google, partially intended to control media and target people critical of the government in that Communist "People's Democratic Dictatorship," underscore that it is important to keep the Internet free. United States policy should be to keep the Internet out of the control of some as-yet unnamed United Nations body or commission that can be institutionalized to allow authoritarian states like China to use it to repress their populations or restrict the free flow of ideas.

The State Department and other agencies of the Executive Branch should work with like-minded allies in other countries, human rights organizations and companies to monitor and develop common responses to the use of the Internet for repression.

I support laws like the Patriot Act that permit law enforcement and intelligence agencies to monitor and fight terrorists.

More work needs to be done on in defining when cyber penetrations or attacks amount to acts of war, where the perpetrator knows that a computer network attack may "directly cause destruction and serious injury."[28] Congress should require that the Departments of Defense, State and Justice explore these issues. Congress also should encourage such organizations as the American Bar Association and Federally Funded Research and Development Centers to work on these legal issues.

My view is that the Departments of Defense and State, with allied governments, should develop a declaratory policy on criteria to categorize computer network attacks as a use of force under international law.

The U.S.-China Economic and Security Review Commission, on which I serve, has recommended that Congress examine any agreement involving Internet service providers that addresses pressures from the Chinese government to provide personally identifiable information about Internet users. The Commission also recommended that Congress investigate whether Chinese government press and Internet censorship violates China's obligations as a member of the World Trade Organization.

With regard to China's cyber activities in the United States and the impact on national security, the Commission recommended that Congress assess the effectiveness of and resourcing for law enforcement, defense and intelligence community initiatives that aim to develop effective and reliable attribution techniques for computer exploitation and computer attacks.

The Commission also recommended that Congress urge the administration to develop measures to deter malicious Chinese cyber activity directed at critical U.S. infrastructure and U.S. government information systems.

Thank you for the opportunity to testify today. I will be pleased to respond to any questions the Committee may pose.

Dr. Larry M. Wortzel is a commissioner on the U.S.-China Economic and Security Review Commission. He was appointed by Republican Leader Boehner. Dr. Wortzel is a retired U.S. Army Colonel. During his 32-year military career, he spent 25 years as an intelligence officer. His operational experience is in signals intelligence collection, human-source intelligence collection, and counterintelligence. Dr. Wortzel served two tours of duty as a military attaché in the American Embassy in the People's Republic of China. He has written three books on China and edited ten other books on the Chinese military. His most recent research and writing has focused on exploiting Chinese military publications on People's Liberation Army doctrine for nuclear warfare, space warfare, and cyber warfare.

[1] Quote from Joel Brenner, former director of the National Counterintelligence Executive, Office of the Director of National Intelligence, in U.S.-China Economic and Security Review Commission, *2009 Report to Congress,* 111th Congress, First Session, Washington, DC: U.S. Government Printing Office, November 2009, p. 167. Archived at www.uscc.gov.

[2] *US-China Economic and Security Review Commission Report on the Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation,* an assessment prepared for the Commission by the Northrop Grumman Corporation, Maclean, VA, October 9, 2009. http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf

[3] *The Wall Street Journal,* "China Real Time Report," "Hacking Probe Elevates Lanxiang School," February 22, 2010, http://blogs.wsj.com/chinarealtime/2010/02/22/hacking-probe-elevates-lanxiang-school/tab/article/

[4] U.S.-China Economic and Security Review Commission, *2009 Report to Congress,* 111th Congress, First Session, pp. 289-309.

[5] Ibid. See also, *Directory of PRC Military Personalities,* October 2008; Timothy L. Thomas, *Decoding the Virtual Dragon: Critical Evolutions in the Science and Philosophy of China's Information Operations and Military Strategy* (Fort Leavenworth, KS: Foreign Military Studies Office, 2007); Ellis Melvin, "A Study of the Chinese People's Liberation Army Military Region Headquarters Department Technical Reconnaissance Bureau"; James Mulvenon, "PLA Computer Network Operations: Scenarios, Doctrine, Organizations, and Capability," in Roy Kamphausen, David Lai, and Andrew Scobell, eds., *Beyond the Strait: PLA Missions Other Than Taiwan* (Carlisle, PA: Strategic Studies Institute, April 2009); Wang

Zhengde, *Jiedu Wangluo Zhongxin Zhan (Interpretation of Network Centric Warfare)* (Beijing: Guofang Gongye Chubanshe, 2004); Wei Baofu and Zhao Xiaosong, *Junshi Xinxi Youxiu Lun (Theory of Military Information Superiority)* (Beijing: National Defense University Press, 2008); and Larry M. Wortzel, "China Goes on the Cyber-Offensive," *Far Eastern Economic Review,* January/February 2009.

[6] U.S.-China Economic and Security Review Commission, *2009 Report to Congress,* 111th Congress, First Session, Section 3: "China's Human Espionage Activities that Target the United States and the Resulting Impacts on U.S. National Security, pp. 158-162.

[7] Kim Zetter, "Hack of Google, Adobe Conducted Through Zero-Day IE Flaw," *Wired.com,* January 1`4, 2010. http://www.wired.com/threatlevel/2010/01/hack-of-adob/#ixzz0exPw8kuh.

[8] U.S.-China Economic and Security Review Commission, *2007 Report to Congress,* 110th Congress, First Session, Washington, DC: U.S. Government Printing Office, November 2007, pp. 95-96. Archived at www.uscc.gov.

[9] Ibid.

[10] Robert Marquand and Ben Arnoldy, "China's hacking skills in spotlight," *The Seattle Times,* September 16, 2007.

[11] Mike McConnell, "How to win the cyber-war we're losing," *The Washington Post,* February 28, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html

[12] Larry M. Wortzel, Ph.D., *Securing America's Critical Infrastructures: A Top Priority for the Department of Homeland Security,* Heritage Lecture #787, Washington, DC: The Heritage Foundation, May 7, 2003. Available at www.heritage.org See also http://www.sciencedirect.com/science?_ob=ArticleURL&_udi=B6VF9-4VVGGTJ-1&_user=10&_rdoc=1&_fmt=&_orig=search&_sort=d&_docanchor=&view=c&_acct=C000050221&_version=1&_urlVersion=0&_userid=10&md5=c9229601b87210270a7c800b9f7f9eab

[13] U.S.-China Economic and Security Review Commission, *2009 Report to Congress,* 111th Congress, First Session, p. 167.

[14] Siobhan Gorman, "Electricity Grid in the U.S. Penetrated by Spies," *The Wall Street Journal,* April 8, 2009, www.onlinewsj.com/Article/sb123911480520409908 5.html

[15] Jian-wei Wang and Li-Li Rong, "Cascade-Based Attack Vulnerability on the US Power Grid," Institute of System Engineering, Dalian University of Technology, China, January 15, 2009, in *Safety Science,* Vol. 47, Issue 10, December 2009, pp. 1332-1336.

[16] Mao Chengpin and Fang Bingbing, South China Normal University, "Research of Attack Taxonomy Based on Network Attack Platform," *Beijing Jisuanji Xitong Yingyong,* Chinese Academy of Science Software Institute, in Open Source Center CPP20090928670001.

[17] Liu Jixian, "Innovation and Development in the Research of Basic Issues of Joint Operations," *China Military Science,* 3-2009, in Open Source Center CPP20090928563001

[18] *Dongfang Zaobao, July 10, 2009,* in Open Source Center CPP20090710045002

[19] Min Zengfu, ed., *Kongjun Junshi Sixiang Gailun (An Introduction to PLA Air Force Military Thought)* (Beijing: Jiefangjun Chubanshe, 2006), pp. 175-176; also see Jiang Yamin Yuan *Zhan (Long Distance Operations),* Beijing: Military Science Press, 2007.

[20] Zhao Erquan, "Lun Xinxihua Zhanzheng dui Wuzhang Chongtu fa de Shenyaun Sixiang," in Liu Jixian and Liu Zheng, eds., *Xin Jishu Geming yu Junshi Fazhi Jianshe (The New Technical Revolution and Building our Military)* (Beijing: Jiefang Jun Chubanshe, 2005, pp. 498-505.

[21] Shen Weguang, JieXijiang, Ma Ji and Li Jijun, *Zhongguo Xinxi Zhan (China's Information Warfare* (Beijing: Xinhua Press, 2005, p. 82-83.

[22] Ibid. pp. 86-87.

[23] Wei Yufu, and Zhao Xiaosong, *Junshi Xinxi Youxiu Lun,* pp. 287-290.

[24] See Kim Zetter, "U.S. Declassifies Part of Secret Cybersecurity Plan," *Wired,* March 2, 1020, http://www.wired.com/threatlevel/2010/03/us-declassifies-part-of-secret-cybersecurity-plan/

[25] National Research Council, *Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington, DC: The National Academies Press, 2009), pp. 200-203.

[26] Ibid. pp. 204-212.

[27] Ibid. pp. 239-292.

[28] The National Research Council Report discusses this in Appendix D., pp. 356-358. The Council also cites Michael Schmitt, “Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework,” *Columbia Journal of Transnational Law* 37:885-937, 1999.