Testimony before the House Committee on Foreign Affairs

By

Dr. Larry M. Wortzel

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

Hearing Entitled
"Investigating the Chinese Threat: Military and Economic Aggression"

Wednesday, March 28, 2012

Rayburn House Office Building

Madam Chairman, Ranking Member Berman, members of the committee, thank you for the opportunity to appear today. On March 7, 2012, the U.S.-China Economic and Security Review Commission released a report prepared for it by Northrop Grumman Corporation on Chinese capabilities for cyber espionage and for computer network operations, or cyber warfare.

The report concluded, among other things, that the Chinese People's Liberation Army places a high priority on modernizing its command, control, communications, computers, intelligence surveillance and reconnaissance (C4ISR) systems and capabilities. This has been a catalyst for the development of an integrated information warfare capability that can defend military and civilian computer networks while seizing control of an adversary's information systems in a conflict. According to the Commission's report, "computer network operations have become fundamental to the PLA's strategic campaign goals for seizing information dominance early" in a military operation "and using it to enable and support other PLA operations throughout a conflict." At the same time, the report concludes, "during peacetime, computer

network exploitation has likely become a cornerstone of PLA and civilian intelligence collection operations supporting national military and civilian strategic goals."

The Commission report tells us that China's computer network exploitation activities to support espionage opened rich veins of information that was previously inaccessible or could only be mined in small amounts with controlled human intelligence operations. The Northrop Grumman Corporation report for the Commission is not the only evidence of how China is using computer espionage to support its military and civilian modernization goals. A November 11, 2011 report on the PLA intelligence and cyber reconnaissance infrastructure also supports the view that China is making a coordinated effort to combine civilian and military programs and both offensive and defensive capabilities. Researchers at the Project 2049 Institute, an independent think tank based in Arlington, Virginia, documented how the PLA General Staff Department's Third Department and Fourth Department are organized and structured to systematically penetrate communications and computer systems, extract information and exploit that information.[1]

Three former U.S. officials, Mike McConnell, former Director of National Intelligence; Michael Chertoff, former Secretary of Homeland Security; and William Lynn, former Deputy Secretary of Defense, said in a January 27, 2012 *Wall Street Journal* opinion piece that: "The Chinese government has a national policy of espionage in cyberspace. In fact, the Chinese are the world's most active and persistent practitioners of cyber espionage today." McConnell, Chertoff and Lynn point out that "it is more efficient for the Chinese to steal innovations and intellectual property that to incur the cost and time of creating their own."

This opinion piece followed a warning about Chinese espionage from the U.S. National Counterintelligence Executive, or NCIX. In an October 2011 report to Congress, the NCIX said

that "Chinese actors are the world most active and persistent perpetrators of economic espionage. US private sector firms and cyber security specialists have reported an onslaught of computer network intrusions that have originated in China," but the Intelligence Community cannot confirm who exactly was responsible. This NCIX report documents intrusions into the computer systems of global oil and energy companies, Google's networks, the networks of a US Fortune 500 manufacturing corporations, and the details on US mergers and acquisitions, and related pricing and financial data.[2]

The Commission's 2009 Annual Report to Congress, citing a *Wall Street Journal* article, discussed "intruders, probably operating from China, that exfiltrated 'several terabytes of data related to design and electronics systems' of the F-35 Lightning II," one of the most advanced fighter planes under development.[3] In addition, Lockheed Martin Corporation, Northrop Grumman Corporation, and British Aerospace and Engineering reportedly all have experience penetrations from hackers based in China in the past three years.[4]

This cyber espionage takes place in parallel to or in conjunction with other forms of espionage. According to the National Counterintelligence Executive, "of the seven cases that were adjudicated under the Economic Espionage Act (18 USC 1831 and 1832) in Fiscal Year 2010, six involved China." An article in a March 2012 manufacturing newsletter notes that "there have been at least 58 defendants charged in federal court related to Chinese espionage since 2008."[5] Some of China's targets are stealth technology, naval propulsion systems, electronic warfare systems for our ships and aircraft, and nuclear weapons.

The Northrop Grumman report to the Commission has some dire warnings. The report tells us that China's government supplements university research and development on computer network operations. Further, in support of military operations, according to the report, cyber-

attacks are particularly appealing to China's military because cyber actions do not have clear attribution "fingerprints," unlike "ballistic missiles, airstrikes, or troop landings." And such attacks would likely be pre-emptive, occurring at the time of or just before the initiation of hostilities. Other researchers make the point that cyber-attacks are inexpensive and provide a lot of effect at a minimal cost.[6]

A PLA strategy for orchestrating cyber-attacks and other forms of combat is "Integrated Network Electronic Warfare," or INEW. This strategy employs electronic warfare, psychological operations, deception, computer network operations, and kinetic strike, or traditional firepower warfare.

For just a minute, I would like to depart from my role as a commissioner explaining the Commission's report and its implications and give you my personal views on this development in Chinese war fighting doctrine. In doing so, I will draw on over 40 years of military and academic experience following China and its armed forces. I was a U.S. Army strategist, intelligence officer and foreign area officer, during which time I served twice as a military attaché in China.

Those of us who served in the military during the Cold War remember a Soviet military doctrine called Radio-electronic Combat, or REC. This doctrine combined electronic warfare, communications intercept, radio-direction finding, and strikes by artillery, helicopters, aircraft, missiles and rockets. The Soviet doctrine called for the capacity to degrade an adversary's combat capability by sixty percent at the outset of any conflict, in other words, at "zero-hour." Thirty percent of the damage was expected from electronic warfare, disrupting or destroying enemy communications and command and control, and thirty percent from kinetic attack.

In my view the PLA Integrated Network Electronic Warfare doctrine is Soviet Radio-electronic Combat on Chinese steroids. Chinese doctrine has added in computer network operations that would disrupt not only command and control, but also logistics and resupply systems. This INEW doctrine is fully integrated with space warfare designed to degrade an adversary's space based sensor and communications systems. And it also includes provisions for precision strikes on U.S. bases, forces, and embarkation areas in the homeland. To be effective, the strategy must be executed at the very first phase of any conflict.

To return to the details of the Northrop Grumman report, it also expresses concerns about some of China's largest telecommunications firms such as Huawei Shenzhen Technology Company, Zhongxing Telecom (ZTE) and Datang Telecom Technology, Ltd. The report notes that these firms may not always be directly linked to the PLA or Chinese C4ISR modernization, but "they benefit from a background network of state research institutes and government funding in programs that have affiliation or sponsorship of the People's Liberation Army." Further, the report explains how a triumvirate of Chinese military institutions, government research organizations, and universities are working to fulfill national programs for basic research and scientific and technological modernization with military applications.[7]

Computer network exploitation or cyber reconnaissance operations during peacetime also identify the nodes in an information system or in an adversary's critical infrastructure that would be attacked or taken over in a conflict. The Northrop Grumman report provides hypothetical scenarios based on PLA writings that show how "Chinese commanders may elect to use deep access to critical U.S. networks carrying logistics and command and control data to collect highly valuable real-time intelligence or to corrupt the data without destroying networks or hardware."[8] Moreover, the report's authors have identified in PLA strategic writings ideas for

applying "paralysis warfare" in electronic and computer attacks against US command and control and logistics systems.[9]

The U.S. military's NIPRNET (Non-secure Internet Protocol Routing Network) is particularly vulnerable to computer network attack and exploitation. This network carries much of the time phasing and force lists for deployments, personnel data, and communications with civilian contractors.[10] An attack on the NIPRNET or the corruption of its data could affect the delivery of repair parts, ammunition, and aerial refueling.[11]

Finally, the Commission's report documents vulnerabilities in the U.S. telecommunications supply chain.[12] Foreign governments or intelligence services could leverage backdoors built into hardware or coded into firmware of software to gain unauthorized access to systems. The report tells us that "without strict control of the complex upstream manufacturing channel a manufacturer of routers, switches, or other telecommunications hardware is exposed to innumerable points of possible tampering and must rely on rigorous and often expensive testing to ensure that the semiconductors being delivered are trustworthy." Similarly, the lack of controls in equipment and component distribution channels creates opportunities for bad actors to funnel compromised goods to consumers, including industry and government.

There are ways to make penetrations of a U.S. system more difficult, such as by hiding the identification of ultimate end-users. But in one noteworthy instance, as pointed out by Representative Frank R. Wolf in 2006, a computer configuration clearly intended to be put on a classified computer network was ordered by the U.S. State Department from a Chinese company.[13] As recently as last month, in response to an inquiry from Representative Wolf and his staff, another commissioner and I, working independently of the commission as a body, learned that the U.S. Army ordered a large number of computers from a Chinese company

destined for installation critical to our NIPRNET-based logistics system, our intelligence organizations, and installations that repair some of our most sensitive electronic sensors. One lesson from that incident is that although Department of Defense and Army procurement and acquisition officials believe they can exercise security cautions and exclude some purchases from foreign firms on purchases of information technology equipment destined to go into weapons systems that are controlled under the United States Munitions List (Part 121 of the International Traffic in Arms Regulation or ITAR), they think that the DOD cannot exclude foreign manufactured computer systems from going to a defense installation or on a system that is not ITAR controlled. These acquisition officials believe that concerns that a foreign manufacturer may not be reliable or a system may have trapdoors are not enough, in themselves, to allow procurement officials to exclude that manufacturer.

Speaking for myself, not for the Commission as a body, it seems to me that the enterprise information architecture of the Department of Defense, indeed perhaps the whole U.S. government, should be a national security concern.

The way that existing legislation is interpreted should be altered, allowing procurement and cyber security officials to exercise due caution if they cannot assure the security of a system. If existing legislation cannot be interpreted differently, and can only be applied to munitions list items, then new legislation may be required.

Further, in my personal view, Congress should consider directing the executive branch to maintain a classified list of countries, people and companies that pose a serious cyber threat to our government and industry. Such a listing could be validated across the intelligence community and vetted by the Foreign Intelligence and Surveillance Court. During the procurement process cleared government officials should be required to consult that list and then

exclude people or companies on such a list from introducing hardware or software into government networks.

Attribution is particularly difficult in the case of cyber penetrations or attacks. But in cases where our counterintelligence or security officials are able to attribute an attack to a foreign person, in a closed federal court such as the Foreign Intelligence and Surveillance Court, law enforcement authorities should be able to seek a warrant for arrest. And in the case of a foreign company, there should be a statutory prohibition on a company judged to be involved in cyber espionage from doing business in the United States. The Department of State should not be permitted to issue a visa to a person who is judged by the Foreign Intelligence and Surveillance Court to be involved in cyber espionage unless there is also a plan to bring that person to trial when he or she enters the United States.

Other researchers argue that attribution is imperfect. Their view is that the U.S. government should hold a foreign government responsible for controlling its citizens involved in cyber-attack or cyber-crime. That may work for cyber-criminals or hackers, but in the case of China, if the entire structure of the intelligence, military and national industry is involved in cyber espionage, it may not be adequate.

With respect to cyber warfare, it is clear that this activity is a legitimate domain of war. The United States and NATO already have incorporated cyber campaigns into military planning in a number of conflicts. Chinese military literature, as documented in the Commission's March 7, 2012 report, also includes provisions for cyber-attacks at the outset of any conflict; it is likely that other countries with cyber capabilities would do the same thing. My personal view is that this means that the United States should have a clear policy that declares that attacks in cyber

space are acts of war and that the U.S. may respond with force, not necessarily in the same domain of war. That is, a cyber-attack may generate a weapons strike and a state of war.

Thank you for the opportunity to testify today. I welcome any questions you may have.

---

[1] http://project2049.net/documents/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf
[2] http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf
[3] U.S. China Economic and Security Review Commission, *2009 Report to Congress* (Washington, DC: Government Printing Office, November 2009), p. 167-168.
[4] http://securityblog.verizonbusiness.com/2012/03/16/weekly-intelligence-summary-2012-03-16.)
[5] http://www.manufacturing.net/articles/2012/03/let-me-count-the-ways-china-is-stealing-our-secrets
[6] See David C. Gompert and Phillip C. Saunders, *The Paradox of Power: Sino-American Strategic Restraint in an Age of Vulnerability* (Washington, DC: National Defense University Press, 2011).
[7] http://www.uscc.gov/RFP/2012/USCC%20Report_Chinese_CapabilitiesforComputer_NetworkOperationsandCyberEspionage.pdf, p. 55-62.
[8] Ibid. p. 31.
[9] Ibid.
[10] Ibid. pp. 33-35.
[11] Ibid. pp. 37-38.
[12] Ibid. pp. 82-93.
[13] http://www.nytimes.com/2006/05/23/washington/23lenovo.html?_r=1&ref=frankrwolf