"Cyber Espionage and the Theft of U.S. Intellectual Property and Technology"

Testimony of Larry M. Wortzel

before the House of Representatives

Committee on Energy and Commerce Subcommittee on Oversight and Investigations

July 9, 2013

Chairman Murphy, Ranking Member DeGette, members of the Subcommittee, thank you for the opportunity to testify today. I will discuss the role of the People's Republic of China, its military and intelligence services, and its industries in cyber espionage and the theft of U.S. intellectual property and technology. As a member of the U.S.-China Economic and Security Review Commission, I will present some of the Commission's findings on China's cyber espionage efforts, its policies and its goals in stealing technology and intellectual property. The views I present today, however, are my own.

China's cyber espionage activities have been going on for a long time. In 2005, *Time* magazine documented a series of intrusions into U.S. laboratories, including those of the Department of Energy, that was called the *Titan Rain* intrusion set.[1] Corporations often will not disclose cyber penetrations and intellectual property theft because they fear retaliation from the Chinese government, hope for future market access in China, fear the loss of consumer confidence, and fear the loss of stock value.

[1] Nathan Thornborough, "The Invasion of the Chinese Cyberspies (and the man who tried to stop them): An Exclusive Look at how the Hackers called TITAN RAIN are Stealing U.S. Secrets," *Time Magazine*, September 5, 2005 *http://www.cs.washington.edu/education/courses/csep590/05au/readings/titan.rain.htm.*

In Chinese military writings, cyberspace is an increasingly important component of China's comprehensive national power, and a critical element of its strategic competition with the United States.[2] Beijing seems to recognize that the United States' current advantages in cyberspace allow Washington to collect intelligence, exercise command and control of military forces, and support military operations. At the same time, China's leaders fear that the United States may use the open Internet and cyber operations to threaten the Chinese Communist Party's (CCP) legitimacy.

China is using its advanced cyber capabilities to conduct large-scale cyber espionage. To date, China has compromised a range of U.S. networks, including those of the Department of Defense (DOD), defense contractors, and private enterprises. These activities are designed to achieve a number of broad security, political, and economic objectives.

China does not appear to have reduced its cyber effort against the United States despite recent public exposure of Chinese cyber espionage in technical detail.[3] When confronted with public accusations from the United States about its cyber espionage, Beijing usually attempts to refute evidence by pointing to the anonymity of cyberspace and the lack of verifiable technical forensic data. It also shifts the media focus by portraying itself as the victim of Washington's cyber activities and calling for greater international cooperation on cyber security.[4] For example, in response to DOD's 2013 report to Congress, which indicated that China participates in cyber

[2] Larry M. Wortzel, *The Dragon Extends its Reach: Chinese Military Power Goes Global* (Washington, DC: Potomac Books, 2013), pp, 17, 41-41, 134, 145-148.
[3] Dan Mcwhorter, "APT1 Three Months Later – Significantly Impacted, Though Active & Rebuilding," *M-Unition* (May 21, 2013). *https://www.mandiant.com/blog/apt1-months-significantly-impacted-active-rebuilding/.*
[4] William C. Hannas, James Mulvenon, and Anna B. Puglisi, *Chinese Industrial Espionage: Technology Acquisition and Military Modernization*, (London and New York: Routledge, 2013), p. 226.

espionage activities, China's Ministry of Foreign Affairs insisted China is "strongly against any form of hacking activities," and dismissed such charges as "baseless."[5]

I believe that regardless of the evidence that is presented, Chinese Communist Party leaders will continue to deny that the People's Liberation Army (PLA) and other government and intelligence organizations are behind these penetrations. After all, this is the same party and government that deny that anyone was killed in Tiananmen Square when the Chinese military massacred about 2,500 people in June 1989.[6]

However, a number of public U.S. government reports, admissions by private companies that they have been the target of cyber espionage, investigations by cyber security firms, and U.S. press reports contradict Beijing's longstanding denials. There is now evidence that the Chinese government not only is encouraging and shaping these attacks, but also directing and executing them. While attribution is difficult and takes great skill, trend analysis is allowing cyber security professionals to develop a more comprehensive understanding of Chinese cyber actors, tools, tactics, techniques, and procedures.

Threats to U.S. National Security

China's cyber espionage against the U.S. government and defense industrial base poses a major threat to U.S. military operations, the security and well-being of U.S. military personnel, the

[5] Don Lee, "China Dismisses U.S. Accusations of Cyber-Spying," *The Los Angeles Times*, May 07, 2013. *http://articles.latimes.com/2013/may/07/world/la-fg-wn-china-us-cyber-spying-20130507.*

[6] Larry M. Wortzel, "The Tiananmen Massacre Reappraised: Public Protest, Urban Warfare, and the People's Liberation Army," in Andrwe Scobell and Larry M. Wortzel, eds., *Chinese National Decisionmaking Under Stress* (Carlisle,PA: Strategic Studies Institute, 2005), pp. 55-84.

effectiveness of equipment, and readiness. China apparently uses these intrusions to fill gaps in its own research programs, map future targets, gather intelligence on U.S. strategies and plans, enable future military operations, shorten research and development (R&D) timelines for military technologies, and identify vulnerabilities in U.S. systems and develop countermeasures.[7]

Military doctrine in China also calls for attacks on the critical infrastructure of an opponent's homeland in case of conflict, which explains some of the Chinese cyber penetrations in the U.S.[8] One senior researcher at the Chinese Academy of Science said that in wartime, cyber warfare may disrupt and damage the networks of infrastructure facilities, such as power systems, telecommunications systems, and education systems in a country. Other PLA strategists have suggested that China should have the capability to paralyze ports and airports by cyber or precision weapon attacks on critical infrastructure.[9]

A number of instances of Chinese cyber espionage targeting U.S. national security programs have been identified in recent years:

- In a 2012 report to Congress on China's military power, DOD stated its networks are targeted about 50,000 times per year.[10] Although China is not responsible for all of these attacks, DOD has said China poses the dominant threat to its networks.[11] In its 2013 annual report to Congress, DOD for the first time explicitly accused China of committing

[7] U.S.-China Economic and Security Review Commission, *2012 Annual Report to* Congress (Washington, DC: U.S Government Printing Office, November 2012), p. 166.
[8] Wortzel, *The Dragon Extends its Reach,* 142-145.
[9] Ibid., 145.
[10] U.S.-China Economic and Security Review Commission, *2012 Annual Report to* Congress (Washington, DC: U.S Government Printing Office, November 2012), p. 154.
[11] U.S.-China Economic and Security Review Commission, *2012 Annual Report to* Congress (Washington, DC: U.S Government Printing Office, November 2012), p. 155.

cyber espionage. The report states China is using cyber operations to "support intelligence collection against the U.S. diplomatic, economic, and defense industrial base sectors."[12]

- In 2012, the National Aeronautics and Space Administration (NASA) disclosed a cyber intrusion into NASA's Jet Propulsion Laboratory network originating from China-based Internet protocol (IP) addresses. According to NASA, the intruders gained "full, functional control" over the network, enabling them to copy, delete, or modify sensitive files; manipulate user accounts for mission-critical systems; and steal user credentials to access other NASA systems.[13]

- A number of U.S. press reports indicate that since as early as 2007 Chinese cyber operators have repeatedly infiltrated the networks of the F-35 Joint Strike Fighter's major contractors – Lockheed Martin, Northrop Grumman, and BAE Systems – and stolen aspects of its design plans.[14] Some experts, noting the resemblance between China's newest stealth fighter, the J-31, and the F-35, have suggested the J-31 was developed using F-35 design plans.[15]

[12] Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013* (Washington, DC: Department of Defense, 2013), p. 36.
[13] House Committee on Science, Space, and Technology Subcommittee on Investigations and Oversight, *Hearing on NASA Cybersecurity: An Examination of the Agency's Information Security*, testimony of Inspector General Paul K. Martin, 112th Cong., 2nd sess., February 29, 2012. *http://oig.nasa.gov/congressional/FINAL_written_statement_for_%20IT_%20hearing_February_26_edit_v2.pdf*.
[14] U.S.-China Economic and Security Review Commission, *2012 Annual Report to* Congress (Washington, DC: U.S Government Printing Office, November 2012), p. 155.
[15] Trefor Moss, "China's Stealth Attack on the F-35," *The Diplomat*, September 27, 2012. *http://thediplomat.com/flashpoints-blog/2012/09/27/the-fake-35-chinas-new-stealth-fighter/*.

- U.S. press reporting indicates that, beginning in 2007, Chinese cyber actors appear to have infiltrated the networks of QinetiQ, a defense contractor specializing in military robotics, satellites, and combat helicopter technology. Undetected for several years, the hackers stole millions of pages of sensitive research documents, and used QinetiQ as a back door into U.S. military networks. In 2012, the PLA released a bomb disposal robot with characteristics similar to one of QinetiQ's designs.[16]

- In May 2013, *The New York Times*, citing a classified report by the Defense Science Board, stated that over several years Chinese cyber actors have compromised the designs of more than fifty sensitive U.S. technologies and advanced weapons systems, including the Patriot missile system, Aegis ballistic missile defense system, V-22 Osprey, F/A-18 fighter, and Littoral Combat Ship.[17]

Threats to U.S. Industry

China's cyber espionage against U.S. commercial firms poses a significant threat to U.S. business interests and competiveness in key industries. General Keith Alexander, commander of U.S. Cyber Command, assessed that the financial value of these losses is about $338 billion a year, including intellectual property losses and the down-time to respond to penetrations,

[16] Michael Riley and Ben Elgin, "China's Cyberspies Outwit Model for Bond's Q," *Bloomberg*, May 2, 2013. *http://www.bloomberg.com/news/2013-05-01/china-cyberspies-outwit-u-s-stealing-military-secrets.html.*
[17] Ellen Nakashima, "Confidential Report Lists U.S. Weapons System Designs Compromised by Chinese Cyberspies," *New York Times*, May 27, 2013. *http://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html#.*

although not all those losses are to Chinese activity.[18] Chinese entities engaging in cyber and other forms of economic espionage likely conclude that stealing intellectual property and proprietary information is much more cost-effective than investing in lengthy R&D programs.[19] These thefts support national science and technology development plans that are centrally managed and directed by the PRC government.

The Chinese government, including the PLA and the Ministry of State Security, supports these activities by providing state-owned enterprises (SOEs) information and data extracted through cyber espionage to improve their competitive edge, cut R&D timetables, and reduce costs. The strong correlation between compromised U.S. companies and those industries designated by Beijing as "strategic" industries[20] further indicates a degree of state sponsorship, and likely even government support, direction, and execution of Chinese economic espionage.[21] Such governmental support for Chinese companies enables them to out-compete U.S. companies, which do not have the advantage of leveraging government intelligence data for commercial gain.[22]

---

[18] Josh Rogin, "NSA Chief: Cybercrime Consitutues the 'Greatest Transfer of Wealth in History'," *Foreign Policy: The Cable,* July 9, 2012, *http://thecable.foreignpolicy.com/posts/2012/07/09/nsa_chief_cybercrime_constitutes_the_greatest_transfer_of_wealth_in_history*

[19] Mike McConnell, Michael Chertoff, and William Lynn, "China's Cyber Thievery is a National Policy – And Must Be Challenged," *Wall Street Journal*, January 27, 2012. *http://online.wsj.com/article/SB10001424052970203718504577178832338032176.html*.

[20] The Commission on the Theft of Intellectual Property, *The IP Commission Report*, (Washington, DC: National Bureau of Asian Research, May 2013), p. 12. *http://ipcommission.org/report/IP_Commission_Report_052213.pdf.*

[21] U.S.-China Economic and Security Review Commission, *2012 Annual Report to* Congress (Washington, DC: U.S Government Printing Office, November 2012), p. 156.

[22] In the late 1980s and early 1990s a debate took place in Congress on whether the U.S. Intelligence Community (IC) should share information and/or intelligence assets with U.S. companies to provide those companies an advantage against foreign competitors. In 1991, Director of the Central Intelligence Agency Robert Gates, in a speech to the IC, stated clearly that the CIA would limit itself to helping U.S. companies safeguard themselves from foreign intelligence operations. Robert Gates, "The Future of American Intelligence," (Washington, DC: U.S. Intelligence Community, December 4, 2011).

It is difficult to quantify the benefits Chinese firms gain from cyber espionage. We don't know everything about the kinds of information targeted and taken, nor do we always attribute theft to a specific Chinese actor. Some thefts may never be detected. In terms of business intelligence, some targets of cyber-theft likely include information related to negotiations, investments, and corporate strategies including executive emails, long-term business plans, and contracts. In addition to cyber-theft, Chinese companies almost certainly are acquiring information through traditional espionage activities, which limits our ability to identify the impact of cyber espionage in particular. Nevertheless, it is clear that China not only is the global leader in using cyber methods to steal intellectual property, but also accounts for the majority of global intellectual property theft.[23] Chinese actors have on several occasions in recent years leveraged cyber activities to gain sensitive or proprietary information from U.S. enterprises:

- In June 2013, the Department of Justice filed charges against a Chinese energy firm, Sinovel Wind Group, alleging it stole secrets from AMSC (previously American Superconductor Corporation). In 2005, the two companies partnered together, leveraging AMSC's high-technology components and Sinovel's specialization in low-cost manufacturing. Once Sinovel was able to reproduce AMSC's technology after stealing its proprietary source codes, the Chinese firm broke the partnership, cancelled existing orders, and devastated AMSC revenue. AMSC later filed several lawsuits in Chinese courts, where Sinovel's assets are located. While the case continues to move slowly

[23] The Commission on the Theft of American Intellectual Propoerty, *The IP Commission Report* (Washington, DC: May 2013), pp. 3, 18. *http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf.*

through the Chinese legal system, adding to AMSC's legal fees, Sinovel is reaping the profits of stolen technology.[24]

- In 2013, Mandiant, a private cyber-security firm, provided detailed technical information tracing the activities of a known cyber threat group, APT1, to a building believed to house the PLA's 2nd Bureau of the General Staff Department's Third Department. According to Mandiant, the Third Department is responsible for conducting at least some of the PLA's computer network operations. Since 2006, the Third Department's Shanghai-based 2nd Bureau committed at least 141 network intrusions across fifteen countries and twenty major industries, from information technology to financial services. 81 percent of the victims were organizations either located in the United States or with U.S.-based headquarters. Mandiant concludes the unit receives "direct government support."[25]

- Aside from its 2nd Bureau in Shanghai, the PLA Third department has another eleven operational bureaus, three research institutes, four operations centers, and sixteen technical reconnaissance units in military regions with operational forces.[26] Not all of these are directing their actions against the United States, and there are no public reports available about what cyber espionage they may have conducted like the Mandiant report about the 2nd Bureau.

[24] Melanie Hart, "Criminal Charges Mark New Phase in Bellweather U.S.-China Intellectual Property Dispute," *Center for American Progress*, June 27, 2013. *http://www.americanprogress.org/issues/china/news/2013/06/27/68339/criminal-charges-mark-new-phase-in-bellwether-u-s-china-intellectual-property-dispute/.*
[25] Mandiant, "APT1: Exposing One of China's Cyber Espionage Units," February 2013, pp. 22-23. *http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.*
[26] United States Department of Defense, *Directory of PRC Military Personalities* (Washington, DC: Defense Intelligence Agency, March 2013), *passim*.

- In an October 2011 report, the U.S. Office of the National Counterintelligence Executive (ONCIX) linked multiple cyber intrusions and instances of intellectual property theft to Chinese individuals or China-based computer systems. The report concludes the "growing interrelationships between Chinese and U.S. companies…will offer Chinese government agencies and businesses increasing opportunities to collect sensitive U.S. economic information."[27]

- In 2011, McAfee, a U.S.-based internet security firm, detailed a series of "covert and targeted cyber [attacks]," dubbed "Night Dragon." Originating primarily from servers in China, "Night Dragon" targeted oil, energy, and petrochemical companies in the United States and other countries, ultimately gaining access to executive accounts and highly sensitive documents over several years.[28]

- Also in 2011, McAfee detailed the activities of "Operation Shady RAT," a cyber actor that compromised data from 49 U.S. entities, including defense contractors, energy companies, real estate companies, and information and communications technology firms, among others.[29] Following the publication of McAfee's report, several security experts asserted that "Operation Shady RAT" was a Chinese government operation.[30]

---

[27] 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*, (Washington DC: October 2011), *http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf.*

[28] McAfee, *White Paper: Global Energy Cyberattacks: 'Night Dragon'* (Santa Clara, CA: McAfee Foundstone Professional Services and McAfee Labs, February 10, 2011), p. 4. *http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf.*

[29] Dmitri Alperovich, *Revealed: Operation Shady RAT* (Santa Clara, CA: McAfee, August 2011). *http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf.*

[30] Laura Saporito and James A. Lewis, "Cyber Incidents Attributed to China," Center for Strategic and International Studies. *http://csis.org/files/publication/130314_Chinese_hacking.pdf.*

- The PLA in 2009 may have conducted a "spearphishing" campaign against the Coca-Cola Corporation. The alleged attack coincided with Coca-Cola's attempts to acquire China Huiyuan Juice Group for $2.4 billion, which would have been the largest foreign takeover of a Chinese company. Hackers gained access to sensitive corporate documents, presumably targeting Coca-Cola's negotiation strategy. Shortly after the FBI informed Coca-Cola that its network was compromised, the acquisition collapsed.[31]

Outlook

There is an urgent need for Washington to compel Beijing to change its approach to cyberspace and deter future Chinese cyber theft. The Chinese government does not appear to be inclined to curb its cyber espionage in any substantial way. Merely naming perpetrators will not affect this centrally directed behavior.

Later this week, the U.S.-China Economic and Security Review Commission will hold a roundtable with leaders in the cyber security field to explore a range of potential Congressional actions and policies, including the following:

- Expose China's illicit behavior in cyberspace and present detailed evidence of Chinese cyber espionage. Jason Healey, director of the Cyber Statecraft Initiative at the Atlantic

[31] David E. Sanger et al., "Chinese Army Unit Is Seen as Tied to Hacking Against U.S.," *New York Times*, February 19, 2013. *http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html?hp&_r=0&pagewanted=all*; Ben Elgin et al., "Coke Gets Hacked and Doesn't Tell Anyone," *Bloomberg*, November 4, 2012. *http://www.bloomberg.com/news/2012-11-04/coke-hacked-and-doesn-t-tell.html.*

Council, recently suggested that the U.S. government should task the intelligence community to release periodic reports detailing Chinese espionage.[32]

- Link Chinese economic espionage to trade restrictions and bilateral issues in which Beijing seeks compromises from Washington. The *Deter Cyber Theft Act* (S. 884), a bi-partisan bill recently introduced in the U.S. Senate, would allow the President to restrict the import of specific goods in order to protect intellectual property rights and DOD supply chains, and require further study of foreign industrial espionage.

- Encourage the U.S. government, military, and cleared defense contractors to implement measures to reduce the effectiveness of Chinese cyber operations and increase the risk of conducting such operations for Chinese organizations. For example, measures such as "meta-tagging, watermarking, and beaconing"[33] can help identify sensitive information and code a digital signature within a file to better detect intrusion and removal.[34] These tags also might be used as evidence in criminal, civil, or trade proceedings to prove that data was stolen.

- Continue or expand bilateral cooperation with China on credit card and bank crime.

[32] Jason Healey, "How the U.S. Should Respond to Chinese Cyberespionage," *New Atlanticist Policy and Analysis Blog*, Atlantic Council, February 25, 2013. *http://www.acus.org/new_atlanticist/how-us-should-respond-chinese-cyberespionage.*
[33] The Commission on the Theft of Intellectual Property, *The IP Commission Report* (Washington, DC: National Bureau of Asian Research, May 2013), p. 81.
http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf.
[34] Cisco, "Data Loss Prevention," *http://www.cisco.com/en/US/netsol/ns895/index.html.*

- Prohibit Chinese firms using stolen U.S. intellectual property from accessing U.S. financial markets. As recommended by the Commission on the Theft of Intellectual Property in its 2013 report, the U.S. Secretary of the Treasury and Secretary of Commerce could be empowered to "deny the use of the American banking system to foreign companies that repeatedly benefit from the misappropriation of American intellectual property."[35]

- Prosecute or punish firms that benefit from cyber-theft, regardless of whether or not they are involved in specific cyber espionage. Companies may not be willing to cooperate with Chinese cyber actors if it means risking civil and criminal litigation and frozen assets.[36]

My personal view is that the President already has an effective tool that he has not used. General Alexander put the annual cost of cyber theft at $338 billion a year. To put that number in perspective, a new *Gerald R. Ford*- class aircraft carrier costs about $12 billion. Given the magnitude of these losses, the President could employ his authority under the International Emergency Economic Power Enhancement Act (IEEPA, 50 USC 1701, PL 110-96) to declare that the cyber-enabled theft of intellectual property represents an "extraordinary threat to the national security…or economy of the United States."

[35] The Commission on the Theft of Intellectual Property, *The IP Commission Report* (Washington, DC: National Bureau of Asian Research, May 2013), p. 66.
http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf.
[36] Stewart Baker, "The Attribution Revolution," *Foreign Policy*, June 17, 2013.
http://www.foreignpolicy.com/articles/2013/06/17/the_attribution_revolution_plan_to_stop_cyber_attacks?page=full.

Under this declaration, the President, in consultation with Congress, may investigate, regulate, and freeze transactions and assets, as well as block imports and exports in order to address the threat of cyber theft and espionage. While this authority has traditionally been employed to combat international financing of terrorist organizations and the proliferations of weapons of mass destruction, there is no statutory limitation that prevents the President from applying the IEEPA to cyber espionage issues.[37]

This committee's job is made harder by the reluctance of companies to admit that cyber theft has taken place. The government and industry must work more closely to detect cyber penetrations and to respond. No interagency effort can monitor intrusions on every corporate network. But the government and industry can do better at detecting and responding to cyber theft.

Thank you for the opportunity to appear today. I am happy to respond to any questions you may have.

[37] 50 U.S.C. § 1701. *http://uscode.house.gov/download/pls/50C35.txt.*