Made in China: Waking Up to U.S. National Security Cyberthreats

A Chinese proverb warns that "there are always ears on the other side of the wall." A modern adaption might warn that Chinese are on the other end of your Internet connection. There is increasing reason to heed that warning. For example, in March 2009, GhostNet, an electronic spy network based mainly in China, was reported to have infiltrated 1,300 computers in 103 countries' government offices.[1] While Russia and Israel are considered to be the larger troublemakers in cyberspace, China distinguishes itself for having the *fastest-growing* and *most active* cyber attack program of all nations. This fact is a serious warning to the United States – a clear wakeup call!

China is engaging in "the single largest, most intensive foreign intelligence gathering effort since the Cold War" against the United States.[2] In addition to traditional military and espionage activities, China views intelligence gathering as "a core mission of the People's Liberation Army (PLA)". The evolution of China's cyber activities began in the 1990's when the Ministry of Public Security partnered with foreign network systems firms (many from the U.S.) to monitor information on the Internet. By 1998, the Chinese had a sophisticated system that effectively monitored all domestic Internet and wireless traffic.

In 2003, the PLA had organized their first cyberwarfare unit, which reached operational capability the following year.[3] According to a 2006 Chinese defense white paper, the PLA established a "strategic goal of building informationized armed forces and being capable of winning informationized wars by the mid-21st century."[4] To achieve this goal, the PLA reduced their forces by 200,000 troops and invested somewhere between $50 to $100 billion per year in developing new capabilities and establishing new cyber militia units.[5] A significant investment is reported to be a 1,100 person cyber operation at Hainan Island (complete with a James Bond-style submarine cave), also home to some key Chinese military units. Canadian researchers have found a number of cyber attacks to have originated there and U.S. Navy ships near the island have been harassed.[6]

It is an understatement to say that the Chinese have made good on their intentions. "U.S. military and government networks and computer systems continue to be the target of intrusions that appear to have originated from within the PRC (People's Republic of China)," reported U.S. Navy Admiral Robert Willard, Commander of U.S. Pacific Command.[7] In

---

[1] Department of Defense, "Annual Report TO Congress; Military and Security Developments Involving the People's Republic of China 2010," May 2010, http://www.defense.gov/pubs/pdfs/2010_cmpr_final.pdf.
[2] Michael Stevens, "China's Cyber Threat Growing," S*ecurityWeek*, July 8, 2010, http://www.securityweek.com/chinas-cyber-threat-growing.
[3] John J. Tkacik, Jr., "Trojan Dragon: China's Cyber Threat," February 8, 2008, http://www.heritage.org/research/reports/2008/02/trojan-dragon-chinas-cyber-threat.
[4] Stevens, op.cit.
[5] Richard Parker, "It's Not Just the Russians Who Are Spying on the U.S.," *Canada.com*, July 2, 2010, http://www.canada.com/technology/just+Russians+spying/3228905/story.html.
[6] Medius Research, "China, Cyber Espionage and U.S. National Security," July 5, 2010, http://www.scribd.com/full/33788819?access_key=key-1lcdjsqzz3z5v5apqrfu.
[7] Statement of Admiral Robert F. Willard, U.S. Navy Commander, U.S. Pacific Command before the House Armed Services Committee on U.S. Pacific Command Posture, March 23, 2010, http://armedservices.house.gov/pdfs/FC032510/Willard_Testimony032510.pdf.

2003, the Pentagon began monitoring PLA cyber operations and found the Chinese had already identified network vulnerabilities in critical Pentagon systems across the United States. By 2006, the Chinese were behind attacks on the State and Commerce Departments, the office of Rep. Frank Wolf, and the Naval War College.[8] In June 2007, information from 150 computers at the Department of Homeland Security were quietly penetrated and sent to a Chinese-language Web site.[9] That summer also featured attacks on systems at the Defense (NIPRNet) and State departments by Chinese military hackers. The 2008 Obama and McCain campaigns also suffered hits, forcing all campaign senior staff to replace their Blackberries and laptops. China was also believed to be behind the 2009 data theft from Lockheed Martin's F-35 fighter program. Some even suspect China to be involved in the 2003 east coast power outage and another in Florida in 2008.

This is a mere sampling. In the first six months of 2009, the Department of Defense recorded nearly 44,000 incidents of malicious cyber activity from sources ranging from criminal hackers to foreign governments. While the cost of lost data is unknown, remediation for these attacks cost more than $100 million.[10] Cyber espionage alone is estimated to cost the U.S. up to $200 billion a year.[11]

American businesses are also prime targets for China. For example, Northrop Grumman has experienced electronic intrusions and disruptions coming from sites inside China since 1999.[12] American businesses in China, like Google and domain name provider GoDaddy, have been harassed by intrusive government practices. Notably, Microsoft had to provide source codes of its Office software to the Chinese government in order to do business there.[13] Chinese companies also increasingly manufactures COTS microchips and semiconductors, making it challenging for the U.S. to meet secure and classified chip needs.

Addressing the threats posed by China's cyber forces has become a national security priority. China's cyber attack efforts threaten to impede the flow of forces and supplies to a crisis area, and "boost the ability to attack an adversary's satellite communications and sensor systems, critical transportation and energy infrastructure, ports of embarkation, and command systems."[14] Marine Corps Gen. James Cartwright, vice chairman of the Joint Chiefs of Staff, also reported that some penetrations of Pentagon systems were "an effort to map out U.S. government networks in order to cripple America's command-and-control systems in the event of a future attack."[15]

---

[8] Josh Rogin, "The Top 10 Chinese Cyber Attacks (that we know of)," *Foreign Policy*, January 22, 2010, http://thecable.foreignpolicy.com/posts/2010/01/22/the_top_10_chinese_cyber_attacks_that_we_know_of.
[9] Tkacik, op.cit.
[10] Larry Wortzel and Rep. Randy Forbes, "In Building Cyber Defense, Knowledge is Power," *Federal Times*, June 20, 2010, http://www.federaltimes.com/article/20100620/ADOP06/6200302/-1/RSS
[11] Parker, op.cit.
[12] James Fallows, "Cyber Warriors," *The Atlantic*, March 2010, http://www.theatlantic.com/magazine/archive/2010/03/cyber-warriors/7917/.
[13] Tkacik, op.cit.
[14] Wortzel and Forbes, op.cit.
[15] Ibid.

Countering this threat is not without it challenges. First, there are questions about how to characterize alleged Chinese activities – as espionage or war? Also significant is how the relationship between Chinese hackers, military, and government is "blurred." Joel Brenner, the government's senior counterintelligence official, noted that "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."[16]

What can the U.S. do to bolster its cybersecurity against the Chinese and other cyber adversaries? U.S. Cyber Command Director, General Keith Alexander, believes that "a network sectioned off from the rest of the Internet is probably inevitable for systems crucial to national security."[17] Setting up this secure network would be technically simple, but politically complicated. Creating this "Secure Zone" would require cooperation between the Pentagon, Department of Homeland Security, the FBI, and the private sector, which owns 85% of the U.S.' critical infrastructure. The laws covering additional powers during cyber attacks and questions about who should regulate civilian cybersecurity are still undetermined. In addition to developing technical counter capabilities, the U.S. needs to ensure that components for IT systems come from trustworthy sources. Chinese commercial investments in cyber-related enterprises also require ongoing examination. China, specifically, must remain an intelligence security risk.

Ancient Chinese military general Sun Tzu wrote in his classic *The Art of War* that, "In all fighting, the direct method may be used for joining battle, but indirect methods will be needed in order to secure victory." The philosophy is disturbingly similar for modern-day China, which believes that "seizing control of an adversary's information flow [is] a prerequisite to air and naval superiority."[18] While most nations engage in cyber espionage activities and develop cyber warfare capabilities, none do it with the large-scale focus and commitment of the Chinese. According to Adm. Willard, China's cyber "threats challenge our ability to operate freely in the cyber commons, which in turn challenges our ability to conduct operations during peacetime and in times of crisis."[19]

The Chinese cyberthreat is surely a wakeup call for America. Just like many goods on store shelves across the country, America's number one cybersecurity concern now reads "Made in China".

[16] Shane Harris, "China's Cyber-Militia," *National Journal*, May 31, 2008, http://www.nationaljournal .com/njmagazine/cs_20080531_6948.php.
[17] Gautham Nagesh, "NSA chief envisions 'secure zone' on Internet to guard against attacks," *The Hill*, September 23, 2010, http://thehill.com/blogs/hillicon-valley/technology/120565-alexander-wants-a-secure-network-for-businesses.
[18] Stevens, op.cit.
[19] Willard, op.cit.