China Expands Cyberspying in U.S., Report Says

OCTOBER 22, 2009

Congressional Advisory Panel in Washington Cites Apparent Campaign by Beijing to Steal Information From American Firms

By SIOBHAN GORMAN

WASHINGTON -- The Chinese government is ratcheting up its cyberspying operations against the U.S., a congressional advisory panel found, citing an example of a carefully orchestrated campaign against one U.S. company that appears to have been sponsored by Beijing.

The unnamed company was just one of several successfully penetrated by a campaign of cyberespionage, according to the U.S.-China Economic and Security Review Commission report to be released Thursday. Chinese espionage operations are "straining the U.S. capacity to respond," the report concludes.

The New Battleground

A report from a congressional advisory panel tracks China-related cyberattacks and events that may have spurred them.

Reuters

China's embassy in Belgrade was damaged in a 1999 bombing by the U.S.

May 1999: The accidental U.S. bombing of the Chinese Embassy in Belgrade, Serbia, leads to a series of defacements of U.S. government Web sites by Chinese hackers.

Associated Press

A Chinese fighter and a U.S. Navy plane (remains above) collided in 2001

April 2001: The collision of a U.S. Navy reconnaissance plane and a Chinese F-8 fighter sparks denial of- service attacks and Web defacements from both sides against government and private sites.

November 2004: Chinese hackers reportedly attack multiple unclassified U.S. military systems including the Defense Information Systems Agency, and the Army Space and Strategic Defense installation.

November 2006: Chinese hackers attack the U.S. Naval War College computer infrastructure, possibly targeting war-game information on the networks. The college's Web and email systems are down for at least two weeks while the investigation takes place.

Oak Ridge National Lab

Oak Ridge Lab, targeted in 2007

October 2007: China is suspected as the source of a malicious email targeting 1,100 employees at the Oak Ridge National Lab. Eleven staff members possibly opened the attachment, allowing the attackers to gain access to a database at the nuclear-weapons laboratory.

March 2009: A Canadian study describes a cyberespionage network that targeted more than 1,300 hosts including those at the German, Indian, Pakistani and Portuguese embassies. The operators responsible for the network were all from China.

More

See the full report on Chinese cyberspies by Northrop Grumman.

The bipartisan commission, formed by Congress in 2000 to investigate the security implications of growing trade with China, is made up largely of former U.S. government officials in the national security field.

The commission contracted analysts at defense giant Northrop Grumman Corp. to write the report. The analysts wouldn't name the company described in the case study, describing it only as "a firm involved in high-technology development."

The report didn't provide a damage assessment and didn't say specifically who was behind the attack against the U.S. company. But it said the company's internal analysis indicated the attack originated in or came through China.

The report concluded the attack was likely supported, if not orchestrated, by the Chinese government, because of the "professional quality" of the

operation and the technical nature of the stolen information, which is not easily sold by rival companies or criminal groups. The operation also targeted specific data and processed "extremely large volumes" of stolen information, the report said.

"The case study is absolutely clearly controlled and directed with a specific purpose to get at defense technology in a related group of companies," said Larry Wortzel, vice chairman of the commission and a former U.S. Army attaché in China. "There's no doubt that that's state-controlled."

Attacks like that cited in the report hew closely to a blueprint frequently used by Chinese cyberspies, who in total steal $40 billion to $50 billion in intellectual property from U.S. organizations each year, according to U.S. intelligence agency estimates provided by a person familiar with them.

"Modern-day espionage doesn't involve cloak and dagger anymore," said Tom Kellermann, a vice president at Core Security Technologies, a cybersecurity company. "It's all electronic."

China is among more than 100 countries that have the capability to conduct cyberspying operations.

The bulk of the report describes the growing ambitions of the Chinese military in cyberspace and its efforts to develop the capability to destroy adversary networks with physical and cyberattacks in the event of a crisis.

Wang Baodong, a spokesman for the Chinese Embassy in Washington, criticized the commission as "a product of Cold War mentality" that was "put in place to pick China to pieces." He added: "Accusations of China conducting, or 'likely conducting' as the commission's report indicates, cyberspace attacks or espionage against the U.S. are unfounded and unwarranted."

In the highly organized cyberspy scheme that drained valuable research and development information from a U.S. company, the report said, the hackers "operated at times using a communication channel between a host with an [Internet] address located in the People's Republic of China and a server on the company's internal network."

In the months leading up to the 2007 operation, cyberspies did extensive reconnaissance, identifying which employee computer accounts they wanted

to hijack and which files they wanted to steal. They obtained credentials for dozens of employee accounts, which they accessed nearly 150 times.

The cyberspies then reached into the company's networks using the same type of program help-desk administrators use to remotely access computers.

The hackers copied and transferred files to seven servers hosting the company's email system, which were capable of processing large amounts of data quickly. Once they moved the data to the email servers, the intruders renamed the stolen files to blend in with the other files on the system and compressed and encrypted the files for export.

Before exporting the data, the collection team used employee accounts to take over four desktop computers to direct the final stage of the operation.

They selected at least eight U.S. computers outside the company, including two at unidentified universities, as a drop point for the stolen data before sending it overseas. The high Internet traffic volume on university networks provides excellent cover.

The spies activated the operation on all seven servers almost simultaneously, which suggested a plan to export the data as quickly as possible. The company's computer-security team eventually detected the outflow of data, but "not before significant amounts of the company's data left the network," according to the report.

The report highlights several departments of China's military, the People's Liberation Army, responsible for components of cyberspying. Together these divisions oversee electronic spying and attack efforts, as well as research and development.

The PLA has also been creating a number of cyberwarfare militia units, which draw on civilians in the telecommunications and technology sectors, as well as academia, the report found.

Printed in The Wall Street Journal, page A9