Commercial cyberspying, theft promise rich payoff (Update 2)

February 20 2013, by Joe Mcdonald

In this Nov. 7, 2012 photo, U.S. and Chinese national flags are hung outside a hotel during the U.S. Presidential election event, organized by the U.S. embassy in Beijing. As public evidence mounts that the Chinese military is responsible for stealing massive amounts of U.S. government data and corporate trade secrets, the Obama administration is eyeing fines and other trade actions it may take against Beijing or any other country guilty of cyberespionage. The Chinese government, meanwhile, has denied involvement in the cyber-attacks tracked by Mandiant. Instead, the Foreign Ministry said that China, too, is a victim of hacking, some of it traced to the U.S. Foreign Ministry spokesman Hong Lei cited a report by an agency under the Ministry of Information Technology and

Industry that said in 2012 alone that foreign hackers used viruses and other malicious software to seize control of 1,400 computers in China and 38,000 websites. (AP Photo/Andy Wong)

For state-backed cyberspies such as a Chinese military unit implicated by a U.S. security firm in a computer crime wave, hacking foreign companies can produce high-value secrets ranging from details on oil fields to advanced manufacturing technology.

This week's report by Mandiant Inc. adds to mounting suspicion that Chinese military experts are helping state industry by stealing secrets from Western companies possibly worth hundreds of millions of dollars. The Chinese military has denied involvement in the attacks.

"This is really the new era of cybercrime," said Graham Cluley, a British security expert. "We've moved from kids in their bedroom and financially motivated crime to state-sponsored cybercrime, which is interested in stealing secrets and getting military or commercial advantage."

Instead of credit card numbers and other consumer data sought by crime gangs, security experts say cyberspies with resources that suggest they work for governments aim at better-guarded but more valuable information.

Companies in fields from petrochemicals to software can cut costs by receiving stolen secrets. An energy company bidding for access to an oil field abroad can save money if spies can tell it what foreign rivals might pay. Suppliers can press customers to pay more if they know details of their finances. For China, advanced technology and other information from the West could help speed the rise of giant state-owned companies

seen as national champions.

"It's like an ongoing war," said Ryusuke Masuoka, a cybersecurity expert at Tokyo's Center for International Public Policy Studies, a private think tank. "It is going to spread and get deeper and deeper."

Mandiant, headquartered in Alexandria, Virginia, said it found attacks on 141 entities, mostly in the United States but also in Canada, Britain and elsewhere.

Attackers stole information about pricing, contract negotiations, manufacturing, product testing and corporate acquisitions, the company said. It said multiple details indicated the attackers, dubbed APT1 in its report, were from a military unit in Shanghai, though there was a small chance others might be responsible.

Target companies were in four of the seven strategic industries identified in the Communist Party's latest five-year development plan, it said.

"We do believe that this stolen information can be used to obvious advantage" by China's government and state enterprises, Mandiant said.

China's military is a leader in cyberwarfare research, along with its counterparts in the United States and Russia. The People's Liberation Army supports hacker hobby clubs with as many as 100,000 members to develop a pool of possible recruits, according to security consultants.

Mandiant said it traced attacks to a neighborhood in Shanghai's Pudong district where the PLA's Unit 61398 is housed in a 12-story building. The unit has advertised online for recruits with computer skills. Mandiant estimated its personnel at anywhere from hundreds to several thousand.

On Wednesday, the PLA rejected Mandiant's findings and said computer addresses linked to the attacks could have been hijacked by attackers elsewhere. A military statement complained that "one-sided attacks in the media" destroy the atmosphere for cooperation in fighting online crime.

Many experts are not swayed by the denials.

"There are a lot of hackers that are sponsored by the Chinese government who conduct cyberattacks," said Lim Jong-in, dean of Korea University's Graduate School of Information Security.

The United States and other major governments are developing cyberspying technology for intelligence and security purposes, though how much that might be used for commercial spying is unclear.

"All countries who can do conduct cyber operations," said Alastair MacGibbon, the former director of the Australian Federal Police's High Tech Crime Center.

"I think the thing that has upset people mostly about the Chinese is ... that they're doing it on an industrialized scale and in some ways in a brazen and audacious manner," said MacGibbon, who now runs an Internet safety institute at the University of Canberra.

China's ruling party has ambitious plans to build up state-owned champions in industries including banking, telecoms, oil and steel. State companies benefit from monopolies and other official favors but lack skills and technology.

Last year, a group of Chinese state companies were charged in U.S. federal court in San Francisco in the theft of DuPont Co. technology for making titanium dioxide, a chemical used in paints and plastics.

In 2011, another security company, Symantec Inc., announced it detected attacks on 29 chemical companies and 19 other companies that it traced to China. It said the attackers wanted to steal secrets about chemical processing and advanced materials manufacturing.

In Australia, a report by the attorney general this week said 20 percent of 225 companies surveyed had experienced a cyberattack in the previous year.

Australian mining companies make a tempting target because of their knowledge about global resources, said Tobias Feakin, head of national security at the Australian Strategic Policy Institute, a think tank.

As Chinese resource producers expand abroad, "you could see the motivation for understanding the Australian competition and infiltrating their systems," Feakin said.

China has long been cited by security experts as a center for Internet crime. They say some crimes might be carried out by attackers abroad who remotely control Chinese computers. But experts see growing evidence of Chinese involvement.

Few companies are willing to confirm they are victims of cyberspying, possibly fearing it might erode trust in their business.

"When companies admit their servers were hacked, they become the target of hackers. Because the admission shows the weakness, they cannot admit," said Kwon Seok-chul, president of Cuvepia Inc., a security firm in Seoul.

An exception was Google Inc., which announced in 2010 that it and at least 20 other companies were hit by attacks traced to China. Only two other companies disclosed they were targets. Google cited the hacking

and efforts to snoop on Chinese dissidents' email as among reasons for closing its China-based search service that year.

Mandiant cited the example of an unidentified company with which it said a Chinese commodity supplier negotiated a double-digit price increase after attackers stole files and emails from the customer's chief executive over 2½ years beginning in 2008.

"It would be surprising if APT1 could continue perpetrating such a broad mandate of cyberespionage and data theft if the results of the group's efforts were not finding their way into the hands of entities able to capitalize on them," the report said.