Administration Developing Penalties for Cybertheft

LOLITA C. BALDOR, Associated Press

WASHINGTON (AP) — Evidence of an unrelenting campaign of cyberstealing linked to the Chinese government is prompting the Obama administration to develop more aggressive responses to the theft of U.S. government data and corporate trade secrets.

A report being released Wednesday considers fines and other trade actions against China or any other country guilty of cyber-espionage. Officials familiar with the administration's plans spoke on condition of anonymity because they were not authorized to speak publicly about the threatened action.

The Chinese government denies being involved in the cyberattacks cited in a cybersecurity firm's analysis of breaches that compromised more than 140 companies. On Wednesday, China's Defense Ministry called the report deeply flawed.

Mandiant, a Virginia-based cybersecurity firm, released a torrent of details Monday that tied a secret Chinese military unit in Shanghai to years of cyberattacks against

U.S. companies.

Mandiant concluded that the breaches can be linked to the People's Liberation Army's Unit 61398.

Military experts believe the unit is part of the People's Liberation Army's cybercommand, which is under the direct authority of the General Staff Department, China's version of the Joint Chiefs of Staff. As such, its activities would be likely to be authorized at the highest levels of China's military.

The release of the Mandiant report, complete with details on three of the alleged hackers and photographs of one of the military unit's buildings in Shanghai, makes public what U.S. authorities have said less publicly for years. But it also increases the pressure on the U.S. to take more forceful action against the Chinese for what experts say has been years of systematic espionage.

"If the Chinese government flew planes into our airspace, our planes would escort them away. If it happened two, three or four times, the president would be on the phone and there would be threats of retaliation," said Shawn Henry, former FBI executive assistant director. "This is happening thousands of times a day. There needs to be some definition of where the red line is and what the repercussions would be."

Henry, the president of the security firm CrowdStrike, said that rather than tell companies to increase their cybersecurity, the government needs to focus more on how to deter the hackers and the nations that are backing them.

James Lewis, a cybersecurity expert at the Center for Strategic and International Studies, said that in the past year the White House has been taking a serious look at responding to China.

"This will be the year they will put more pressure on, even while realizing it will be hard for the Chinese to change. There's not an on-off switch," Lewis said.

In denying involvement in the cyberattacks tracked by Mandiant, China's Foreign Ministry said China too has been 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 that in 2012 alone foreign hackers used viruses and other malicious software to seize control of 1,400 computers in China and 38,000 websites.

"Among the above attacks, those from the U.S. numbered the most," Hong said at a daily media briefing, lodging the most specific allegations the Chinese government has made about foreign hacking.

Cybersecurity experts say U.S. authorities do not conduct similar attacks or steal data from Chinese companies but acknowledge that intelligence agencies routinely spy on other countries.

China is clearly a target of interest, said Lewis, noting that the U.S. would be interested in Beijing's military policies, such as any plans for action against Taiwan or Japan.

In its report, Mandiant said it traced the hacking back to a neighborhood in the outskirts of Shanghai that includes a white 12-story office building run by the army's Unit 61398.

Mandiant said there are only two viable conclusions about the involvement of the Chinese military in the cyberattacks: Either Unit 61398 is responsible for the persistent attacks, or they are being done by a secret organization of Chinese speakers, with direct access to the Shanghai telecommunications infrastructure, who are engaged in a multi-year espionage campaign being run right outside the military unit's gates.

"In a state that rigorously monitors Internet use, it is highly unlikely that the Chinese government is unaware of an attack group that operates from the Pudong New Area of Shanghai," the Mandiant report said, concluding that the only way the group could function is with the "full knowledge and cooperation" of the Beijing government.

The unit "has systematically stolen hundreds of terabytes of data from at least 141 organizations," Mandiant wrote. A terabyte is 1,000 gigabytes. The most popular version of the new iPhone 5, for example, has 16 gigabytes of space, while the more expensive iPads have as much as 64 gigabytes of space. The U.S. Library of Congress' 2006-10 Twitter archive of about 170 billion tweets totals 133.2 terabytes.

___

Associated Press writers Christopher Bodeen, Gillian Wong, Charles Hutzler and Joe McDonald contributed to this report.