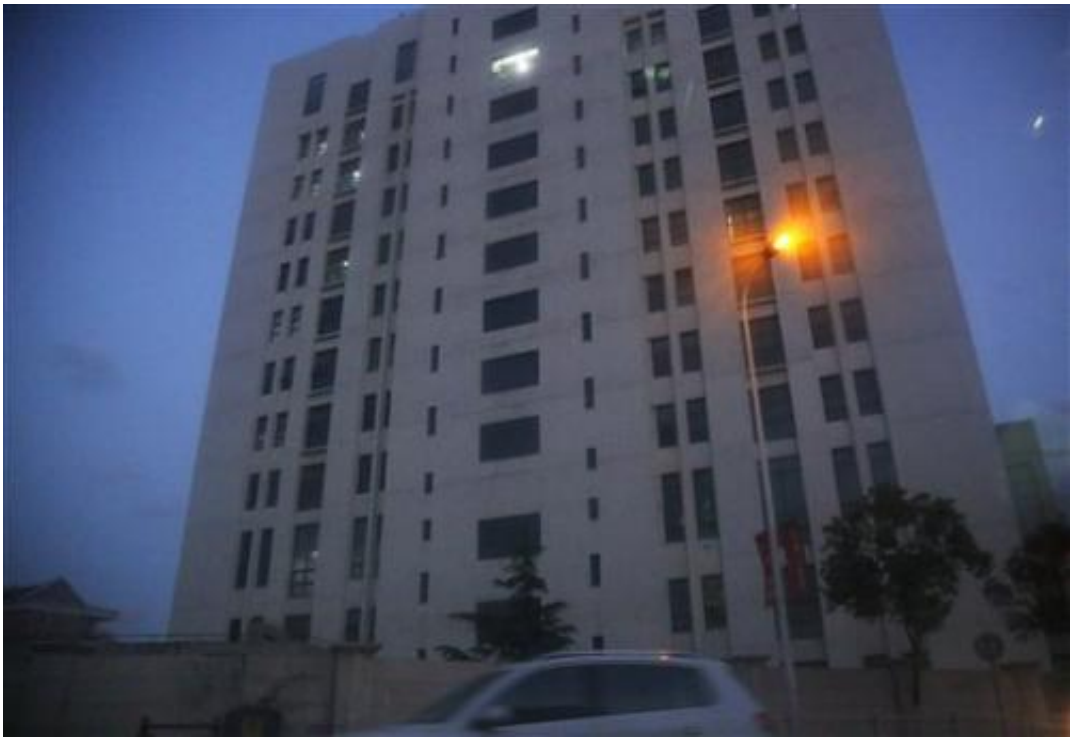
US ready to strike back against China cyberattacks

February 20 2013, by Lolita C. Baldor



The building housing "Unit 61398" of the People's Liberation Army is seen in the outskirts of Shanghai, Tuesday Feb. 19, 2013. Cyberattacks that stole information from 141 targets in the U.S. and other countries have been traced to the Chinese military unit in the building, a U.S. security firm alleged Tuesday. According to the report by the Virginia-based Mandiant Corp., it has traced the massive amount of hacking back to the 12-story office building run by "Unit 61398", and that the attacks targeted key industries including military contractors and companies that control energy grids. China dismissed the report as "groundless."(AP Photo)

(AP)—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.

According to officials familiar with the plans, the White House will lay out a new report Wednesday that suggests initial, more-aggressive steps the U.S. would take in response to what top authorities say has been an unrelenting campaign of cyberstealing linked to the Chinese government. The officials spoke on condition of anonymity because they were not authorized to speak publicly about the threatened action.

The White House plans come after 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. After analyzing breaches that compromised more than 140 companies, Mandiant has concluded that they 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 cyber-command, 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 Mandiant's 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 former FBI executive assistant director Shawn Henry. "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, now 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, adding that "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."

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.

"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 PLA'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' 2006-2010 Twitter archive of about 170 billion tweets totals 133.2 terabytes.

"At some point we do have to call the Chinese out on this," said Michael Chertoff, Homeland Security secretary under President George W. Bush and now chairman of the Chertoff Group, a global security firm. "Simply rolling over and averting our eyes, I don't think is a long-term strategy."

Richard Bejtlich, the chief security officer at Mandiant, said the company decided to make its report public in part to help send a message to both the Chinese and U.S. governments.

"At the government level, I see this as a tool that they can use to have discussions with the Chinese, with allies, with others who are concerned about this problem and have an open dialogue without having to worry about sensitivities around disclosing classified information," Bejtlich said. "This problem is overclassified."

He said the release of an unclassified report that provides detailed evidence will allow authorities to have an open discussion about what to do.

Mandiant's report is filled with high-tech details and juicy nuggets that led to its conclusion, including the code names of some of the hackers, like Ugly Gorilla, Dota and SuperHard, and that Dota appears to be a fan of Harry Potter because references to the book and movie character appear as answers to his computer security questions.

The White House would not comment on the report expected Wednesday.

"We have repeatedly raised our concerns at the highest levels about cybertheft with senior Chinese officials, including in the military, and we will continue to do so," said Caitlin Hayden, spokeswoman for the National Security Council. "The United States and China are among the world's largest cyber actors, and it is vital that we continue a sustained, meaningful dialogue and work together to develop an understanding of acceptable behavior in cyberspace."

Sen. Dianne Feinstein, D-Calif., chairman of the Senate Intelligence Committee, said the report reinforces the need for international

agreements that prohibit cybercrimes and have a workable enforcement mechanism.