Administration developing penalties for cybertheft

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)

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.

Portrait of accused China cyberspy unit emerges

Unit 61398 of the People's Liberation Army has been recruiting computer experts for at least a decade. It has made no secret of details of community life such as badminton matches and kindergarten, but its apparent purpose became clear only when a U.S. Internet security firm accused it of conducting a massive hacking campaign against North American targets.

Hackers with the Chinese unit have been active for years, using online handles such as "UglyGorilla," Virginia-based firm Mandiant said in a report released Tuesday as the U.S. prepared to crack down on countries responsible for cyber espionage. The Mandiant report plus details collected by The Associated Press depict a highly specialized community of Internet warriors working from a blocky white building in Shanghai:

—RECRUITING THE SPIES: Unit 61398, alleged to be one of several hacking operations run by China's military, recruits directly from universities. It favors high computer expertise and English language skills. A notice dated 2003 on the Chinese Internet said the unit was seeking master's degree students from Zhejiang University's College of Computer Science and Technology. It offered a scholarship, conditional on the student reporting for work at Unit 61398 after graduation.

—CYBERSPY WORKPLACE: Mandiant says it traced scores of cyberattacks on U.S. defense and infrastructure companies to a neighborhood in Shanghai's Pudong district that includes the 12-story building where Unit 61398 is known to be housed. The building has office space for up to 2,000 people. Mandiant estimates the number of personnel in the unit to be anywhere from hundreds to several thousand. The surrounding neighborhood is filled with apartment buildings, tea houses, shops and karaoke bars.

—THE UNIT 61398 COMMUNITY: While the building's activities may be top secret, Unit 61398's status in the community as a military division

is not. It turns up in numerous Chinese Internet references to community events, including a 2010 accord with the local government to set up a joint outreach center on family planning. Other articles describe mass weddings for officers, badminton matches and even discussion of the merits of the "Unit 61398 Kindergarten." Other support facilities include a clinic, car pool, and guesthouse—all standard for the military's often self-contained communities across China.

—THE PIPELINE: The Mandiant report describes a special arrangement made with China Telecom for a fiber optic communication infrastructure in the Unit 61398 neighborhood, pointing to its need for bandwidth and its elite status. The contract between the two refers to Unit 61398 as belonging to the General Staff Department 3rd Department, 2nd Bureau, and says China Telecom agreed to the military's suggested price due to "national defense construction" concerns.

—MODUS OPERANDUS: The cyberspies typically enter targeted computer networks through "spearfishing" attacks, in which a company official receives a creatively disguised email and is tricked into clicking on a link or attachment that then opens a secret door for the hackers, Mandiant says. The cyberspies would steal and retransmit data for an average of just under a year, but in some cases more than four years. Information technology companies were their favorite targets, followed by aerospace firms, pointing to a key area of interest as China seeks to develop its own cutting-edge civilian and military aircraft.

—ONLINE HANDLES: Mandiant identifies three of the unit's hackers by their screen names. It says one of them, "UglyGorilla," was first detected in a 2004 online forum posing a question to a cybersecurity expert about whether China needed a dedicated force to square off against an online cohort being mustered by the United States. The user of another screen name, "Dota," appears to be a fan of Harry Potter;

Mandiant said references to the book and movie character appear as answers to his computer security questions.

Unit 61398 hackers were sometimes identified as the "Comment Crew" by security companies due to their practice of inserting secret backdoors into systems by using code embedded in comments on websites.

—REVEALING TWEETS: And what helped Mandiant track down the source of hacking into more than 140 companies and organizations from the U.S. and elsewhere? Facebook and Twitter.

China's "Great Firewall" of Internet filtering blocks those U.S.-based social networks, but Unit 61398 operators got around that by accessing them directly from the unit's system. Mandiant was able to see that Facebook and Twitter accounts were being accessed from Internet Protocol addresses connected to the unit. It's not clear whether those accounts aided in hacking or were simply for the hackers' personal use.

"These actors have made poor operational security choices, facilitating our research and allowing us to track their activities," the report says.