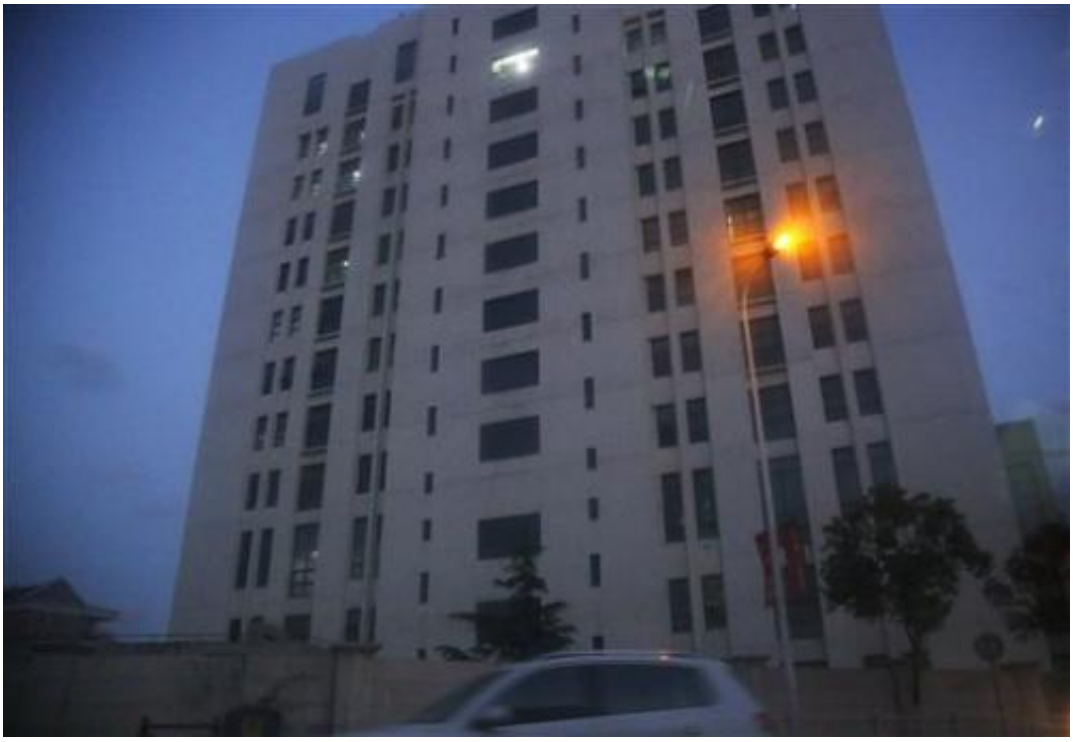
Cyberattacks a growing irritant in US-China ties

May 8 2013, by Christopher Bodeen



In this Feb. 19, 2013 file photo, the building housing "Unit 61398" of the People's Liberation Army is seen in the outskirts of Shanghai. Signs are growing that China's massive allegedly state-sponsored computer hacking is imperiling its relations with the U.S., lending urgency to fledgling efforts by the sides to engage on the issue. (AP Photo/File)

(AP)—Signs are growing that the sustained surge in cyberattacks emanating from China is imperiling its relations with the U.S., lending

urgency to fledgling efforts by both governments to engage on the issue.

The Pentagon this week said China appeared to be cyberspying against the U.S. government, the first time it has made such an assertion in its annual report on Chinese military power. A bill introduced in the Senate on Tuesday would require the president to block imports of products using stolen U.S. technology or made by companies implicated in computer theft.

Washington's sudden focus on Chinese hacking comes after rising complaints from U.S. businesses about theft of trade secrets. Amid growing evidence that the People's Liberation Army and other state-backed groups are behind the infiltrations, Beijing's statements that the cyberhacking allegations are groundless—repeated anew Wednesday by the Chinese Defense Ministry—are being broadly dismissed.

"Hacking has become a significant sore spot in the U.S.-China relationship," said Abe Denmark, senior director of the National Bureau of Asian Research, an independent U.S.-based think tank. "It encompasses security, trade and intellectual property rights, and has become an issue of strategic significance to Washington."

Thus far, President Barack Obama's administration has mostly sought to apply pressure and avoid a confrontation that could set off a Chinese backlash at a time when Washington wants to keep the economy afloat. The issue was raised on recent visits by U.S. officials, including Secretary of State John Kerry and Chairman of the Joint Chiefs of Staff Gen. Martin Dempsey, although Dempsey said that no specific measures to discourage such activity were discussed.

The sides also agreed to form a joint working group to address the matter, adding it to the other disputes that bedevil ties, including trade, North Korea, Iran, Chinese territorial claims and human rights.

There are scant signs of progress so far, with State Department spokesman Patrick Ventrell saying only that "we look forward to engaging in that dialogue."

Chinese hacking and cyberspying are described by experts to be so widespread and persistent that it has caused billions of dollars in economic losses and become an issue of U.S. national security by possibly placing critical infrastructure at risk. Washington is trying to beef up defenses by working with Internet companies and security firms.

The Pentagon report released Monday said China is using its cyber capabilities to collect intelligence against U.S. diplomatic, economic and defense programs. And the report warned that the skills needed for such espionage are similar to those needed to conduct more aggressive cyberattacks.

Though the Pentagon did not pinpoint sources of the hacking, U.S.-based Internet security firm Mandiant said in a February report that it traced years of cyberattacks against 140 mostly American companies to a People's Liberation Army unit in Shanghai. Mandiant executives say attacks originating in China have continued since then, with the exception of those from Shanghai-based Unit 61398 that had been highlighted in its earlier report.

China has called the accusations groundless, saying it's impossible to tell the origin of cyber-intrusions, and complained that it too is a target of hacking, with many attacks coming from the U.S.

"As everyone knows, it's America that is the real 'hackers empire,' People's Daily, the Communist Party's flagship newspaper, wrote in a commentary.

Though China has provided scant specifics, the National Security

Agency was tasked in 1997 with developing ways to attack foreign computer networks, according to recently declassified information released last month by the National Security Archive of George Washington University. One of the most successful acts of cyber-sabotage—the insertion of the Stuxnet virus into computer systems for Iran's nuclear program in 2010—is believed to have been the work of the U.S. and Israel.

China's Defense Ministry dismissed the Pentagon report, calling it an attempt to "turn black into white and mislead international public opinion," in a statement that did not directly address the assertions about cyberspying and the overall rising capabilities of the PLA.

"In recent years, the United States vigorously developed advanced weapons and equipment and formed an offensive cyberwarfare unit. This is obvious to the international community. The United States has no right to make irresponsible remarks on China's legitimate building of its defense and military," the ministry said.

James Mulvenon, a specialist on the Chinese military and cyberwarfare at Washington, D.C.-based consultancy Defense Group Inc. scoffed at the dismissal. He tweeted: "'Groundless accusations,' eh? Wasted 100s of hours fighting in my networks."

With Beijing so far not forthcoming, often partisan forces in Washington are coalescing around the need for tougher action.

The Senate bill was introduced by a bipartisan group of senators, including Democrat Carl Levin of Michigan and Republican John McCain of Arizona. While it doesn't mention China as a specific target of sanctions, a news release on the legislation notes that "recent reports indicate that China is by far the largest source of theft attempts against U.S. companies."

"We need to call out those who are responsible for cyber theft and empower the president to hit the thieves where it hurts most—in their wallets, by blocking imports of products from companies that benefit from this theft," Levin was quoted as saying in the release.

The Senate's bipartisan approach, rising attention from the administration and public expressions of concern from the normally pro-Beijing business community illustrate how the issue has already reached critical mass, said Yu Maochun, a China scholar at the U.S. Naval Academy in Annapolis, Maryland.

"The Chinese hacking is so staggering and so significantly un-American that it has actually united major bickering and partisan sections of American society, the same way Pearl Harbor or Sept. 11 did," Yu said.