

## **Panetta talks cyber issues with Chinese, but experts see no decline in attacks out of China**

LOLITA C. BALDOR Associated Press

BEIJING (AP) -- Despite several years of escalating diplomacy and warnings, the U.S. is making little headway in its efforts to tamp down aggressive Chinese cyberattacks against American companies and the government.

U.S. Defense Secretary Leon Panetta, who is wrapping up three days of meetings with military and civilian leaders, said he has brought the issue up at every session and come away with little more than agreements to talk again.

Meanwhile, cybersecurity analysts say the computer-based attacks emanating from China continue unabated, and in fact are expanding and focusing more intently on critical American oil, gas and other energy companies.

"No diplomatic actions have made a difference," said Richard Bejtlich, chief security officer for the Virginia-based cybersecurity firm Mandiant. "They remain aggressive - they're kicked out one day and try to get back in the next day."

He said the China-backed hackers' tactics are also evolving, and they are more often going after corporate computer systems by breaching software weaknesses, rather than simply trying to get into a network by duping an individual employee. And he said they appear to be increasingly targeting lucrative energy companies.

Efforts by officials across the U.S. government have not seemed to have any impact, Bejtlich said, adding: "The Chinese don't seem to care. So I don't have any hope that the dialogue is reaching anyone of any note."

Panetta, who is leaving China on Thursday, met with China's leader-in-waiting, Xi Jinping, Wednesday and afterward told reporters that he urged Xi and other leaders to have an ongoing dialogue with the United States about the cyber threat.

"I think it's clear that they want to engage in a dialogue on this issue," Panetta said, "and I guess that's the most important thing. That's the beginning of trying to perhaps be able to develop an approach to dealing with cyber issues that has some semblance of order here as opposed to having countries basically all flying in the dark."

Chinese officials have steadfastly denied the cyberattacks, saying they also are victims of computer hackers and breaches.

But nine months ago senior U.S. intelligence officials for the first time publicly accused China of systematically stealing American high-tech data for its own national economic gain. It was the most forceful and detailed airing of U.S.

allegations against Beijing after years of private complaints, and it launched a more open push to combat the attacks.

James Lewis, a cybersecurity expert with the Center for Strategic and International Studies, said the U.S. is starting to push the Chinese harder on the issue, but the administration needs to do more.

"The damage from Chinese cyber espionage is easy to overstate but that doesn't mean we should accept it," he said. "The Bush administration was unaware of the problem; this administration needs to come up with a more dynamic response."

Cyber experts and U.S. officials agree that one of the biggest threats is the possibility of a miscalculation when a cyber breach triggers a clash between the two nations and there is no underlying relationship that can be used to discuss or work out the problem.

"How do you make sure something doesn't go off course and become a flashpoint for a bigger crisis?" Lewis said.

He added that the People's Liberation Army has been more confrontational lately, and lingering questions remain about the relationship between the Chinese political leaders and the military, and whether the civilian officials can effectively rein in the PLA.

Bejtlich and others describe a hierarchy of hackers in China that includes three main groups: those who are employed directly by the government, those who are affiliated with universities or quasi-government agencies and the so-called patriotic hackers who work on their own but direct their attacks against the U.S. and Western interests.

Bejtlich said some of the state-sponsored hackers appear to moonlight, stealing data from Western companies perhaps as a way of making more money. As long as they don't present a threat to China or Chinese companies, it is tolerated.

Panetta has warned repeatedly that cyberattacks and cyberwarfare could set off the next war. And U.S. officials and security experts say government and private industry systems are constantly being probed, breached and attacked. A key threat is an attack against critical infrastructure, including the electric grid, power plants or financial networks, that could plunge the U.S. into crisis.

Officials have said that at this point the main threats from China are intelligence espionage and the theft of corporate and high-tech data, rather than an all-out act of war. But they warn that hackers in China, many of whom work for, are backed by or are tolerated by the Chinese government, are capable of highly sophisticated attacks.

## **Panetta talks cyber issues with Chinese, but experts see no decline in attacks**

Published on Electronic Component News (<http://www.ecnmag.com>)

---

<http://www.ecnmag.com/news/2012/09/panetta-talks-cyber-issues-chinese-experts-see-no-decline-attacks-out-china>