US, China trade charges on cyberattacks

February 19 2013, by Veronika Oleksyn

The United States and China on Tuesday traded charges over cyberattacks after a security firm alleged that Beijing controled hackers who have penetrated the US government, companies and media.

The US firm Mandiant said that cyberattacks had been traced back to a non-descript, 12-story building on the outskirts of Shanghai, where China's army was believed to be in charge of hundreds if not thousands of hackers.

In a 74-page report, the firm said that the hacking group "APT1"—from the initials "Advanced Persistent Threat"—was believed to be a branch of what is known as Unit 61398 of the People's Liberation Army.

"We believe that APT1 is able to wage such a long-running and extensive cyber espionage campaign in large part because it receives direct government support," Mandiant said.

US officials voiced concern about the charges in the report but were cautious. White House spokesman Jay Carney said that US officials "regularly raise this issue with Chinese officials, including officials in the military."

State Department spokeswoman Victoria Nuland said that cybertheft was a "serious concern" that comes up "in virtually every meeting we have with Chinese officials" and has been raised "at the highest levels."

"We consider this kind of activity a threat not only to our national

security but also to our economic interests and (we are) laying out our concerns specifically so that we can see if there's a path forward," she said.

Earlier, China's defense ministry said its army had never supported any kind of hacking activity.

"Not only are reports that China's army has been involved in hacking unprofessional, they do not fit with the facts," the ministry said in a statement to AFP.

"Hacking attacks are a global problem. Like other countries, China also faces the threat of hacking attacks, and is one of the main countries falling victim to hacking attacks."

The country's foreign ministry rejected "groundless accusations" of Chinese involvement in hacking and also said Beijing was itself a major victim, with most overseas cyberattacks against it originating in the United States.

The United States has been stepping up its cyber warfare capabilities. The United States and Israel are widely believed to have unleashed the Stuxnet virus several years ago in a bid to cripple Iran's contested nuclear program.

High-profile US media outlets including The New York Times and The Wall Street Journal, as well as social media giant Twitter, have reported brazen IT attacks that have raised concerns about Chinese hackers.

The New York Times said hackers stole its corporate passwords and accessed the personal computers of 53 employees after the newspaper published a report on the family fortune of China's Premier Wen Jiabao.

Clients including The New York Times have hired Mandiant to clean up their systems after cyberattacks.

In its report, Mandiant alleged that APT1—known also as "Comment Crew" for its practice of planting viruses on the comment sections of websites—has stolen hundreds of terabytes of data from at least 141 organizations spanning 20 industries.

The New York Times, which was given early access to the report, said the researchers had found that the Comment Crew was increasingly focused on companies involved in US infrastructure, including in its electrical power grid, gas lines and water works.

One target, the newspaper reported, was a company with remote access to more than 60 percent of oil and gas pipelines in North America.

In his State of the Union address last week, US President Barack Obama said the potential ability of outsiders to sabotage critical US infrastructure was a major concern.

"We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy," he said.