Hacking incidents ignite fears over China

February 2 2013, by Rob Lever

This week, the New York Times and Wall Street Journal reported that their computer networks had been compromised, alleging it was an effort by the Chinese government to spy on news media operating in the country.

A series of brazen cyberattacks on America's most high-profile media outlets has revived concerns over Chinese hackers, who analysts say are likely linked to the secretive Beijing government.

The attacks, part of a string of incidents traced back to Chinese servers associated with previous intrusions, underscore an urgent need for Washington to pressure Beijing to rein in its digital warriors, experts say.

Other security professionals argue it is hard to be certain the attacks stem from China or that the hackers acted at the behest of the government.

This week, the New York Times and Wall Street Journal reported that their computer networks had been compromised, alleging it was an effort by the Chinese government to spy on news media operating in the country.

James Lewis, cybersecurity specialist at US thinktank the Center for Strategic and International Studies, said there is evidence that backs the allegations of Chinese government involvement.

Hackers from China have previously been linked to attacks on US defense giant Lockheed-Martin, Google and Coca-Cola. Other reports say Chinese hackers have tried to infiltrate the Pentagon's computers and those of US lawmakers.

Twitter also revealed it had been hit by a "sophisticated" cyber attack similar to those that recently hit the NY Times and WSJ, and that the passwords of about 250,000 users were stolen. Twitter however did not yet confirm the source of the intrusion.

Outgoing US Secretary of State, Hillary Clinton, pictured at the State Department in Washington, DC, on February 1, 2013. Clinton said on Thursday that there has been an increase in cyber-hacking attacks on both state institutions and private companies.

"The Chinese don't play by the rules that the rest of the world plays by," Lewis told AFP. "That's partly because they don't understand them and partly because they don't value them."

Lewis said the level of attacks is "reaching an intolerable level" and will force a US government response that goes beyond words.

The Wall Street Journal reported on Friday that in his coming book, Google chairman Eric Schmidt brands China an Internet menace that sanctions cyber crime for economic and political gain.

"The New Digital Age" is authored by Schmidt in a collaboration with

Jared Cohen, a former US State Department advisor who heads a Google Ideas think tank. The book is due for release in April.

The authors reportedly brand China "the world's most active and enthusiastic filterer of information" and "the most sophisticated and prolific" hacker of foreign companies.

The New York Times said it had fallen victim to hackers possibly connected to China's military, linking the attacks to its expose of the vast wealth amassed by a top leader's family.

Outgoing US Secretary of State Hillary Clinton said Thursday that there has been an increase in hacking attacks on both state institutions and private companies.

"We have to begin making it clear to not only the Chinese... that the

United States is going to be having to take actions to protect not only our governments but our private sector from this kind of illegal intrusion," she said.

Graham Cluley, senior technology consultant at British security firm Sophos, said news media had not considered themselves likely targets of attacks until now.

He said that if the recent reports are accurate, the goal is likely "to track who the journalists may be meeting and take actions against those people."

This typically involves "a long-term undercover effort" where hackers seek to prowl computer systems unnoticed.

Cluley said that even if the source of attacks is confirmed, "it's very hard to neutralize" because hackers can simply move. "Do you want to knock an entire country off the Internet?"

China's defense ministry reiterated comments this week that it "never supported any hacking attacks."

Ryan Sherstobitoff, a researcher with the security firm McAfee, said that "it's hard to pinpoint the origin" of the attacks because computer traffic can be routed through various locations.

Chinese Premier, Wen Jiabao, pictured at the EU headquarters in Brussels, on October 6, 2010. The New York Times said it had fallen victim to hackers possibly connected to China's military, linking the sophisticated attacks to its expose of the vast wealth amassed by Wen family.

But he said the overwhelming majority of computer infiltrations come from employees mistakenly opening booby-trapped email attachments faked to appear as if it came from a colleague.

This technique, known as "spear phishing," ends up installing malware that can remain on a network and allow hackers to view or control data.

"There is certainly a rise in the numbered of these targeted attacks," Sherstobitoff said.

The Times said hackers stole corporate passwords and targeted the

computers of 53 employees, in response to the newspaper's investigation into the vast wealth amassed by a top Chinese leader's family.

The newspaper said Bloomberg News was also targeted by Chinese hackers. And the Beijing correspondent of Canada's Globe and Mail newspaper said he had been hacked in 2011 in an effort to find China-related files.

Jody Westby, a cybersecurity consultant and adjunct faculty member at the Georgia Institute of Technology, said the attacks "shine a glaring spotlight on the inadequacies of US diplomacy in addressing cyber threats."

Andrew Mertha, a Cornell University specialist on China, said the cyber spying highlights Beijing's awkward efforts to extend its global influence.