US investigating Google claim of China hacking

June 2 2011, By PAISLEY DODDS and RAPHAEL G. SATTER , Associated Press

In this July 17, 2006 file photo, Google workers walk by a Google sign at company headquarters in Mountain View, Calif. Google says computer hackers in China broke into the Gmail accounts of several hundred people, including senior government officials in the U.S. and political activists. The attacks announced Wednesday, June 1, 2011 on Google's blog aren't believed to be tied to a more sophisticated assault originating from China in late 2009 and early last year. (AP Photo/Paul Sakuma, File)

(AP) -- Authorities in the United States are investigating a Google claim that hackers in China stole email details of senior U.S. government officials - an issue that illustrates the problem of attribution in cyberspace, the coordinator for cyber issues at the U.S. State Department said Thursday.

Google disclosed Wednesday that personal Gmail accounts of several hundred people, including senior U.S. government officials, military personnel and political activists, had been breached. The company said it traced the origin of the attacks to Jinan, China, the home city of a military vocational school whose computers were linked to an assault 17 months ago on Google's systems. China has said it does not support hacking.

"The issue of attribution and knowing whether a state or non-state actors are involved is a huge problem in cybersecurity," Christopher Painter, coordinator for cyber issues for the State Department, told The Associated Press on the sidelines of a cybersecurity conference in London. He declined further comment on the Google claim.

Yuan Xu of the Internet Society of China, an industry group, defended her country's actions against phishing - the type of attack that Google says was used against its users. Phishing fools users into giving their personal details to rogue websites.

She declined to comment on the specifics of the Google case, saying she didn't know enough about it, but noted that the CNCERT - one of China's Internet watchdogs - regularly shares the addresses of suspected phishing websites with its international partners.

Yuan said that, on Internet security issues, companies in China and the United States "would like to see cooperation with each other."

Michael Chertoff, a secretary for Homeland Security under President George W. Bush, said the reported hack illustrated the need for officials in sensitive positions to steer clear of unsecured email communication.

He said senior government workers needed to police their own "cyber-hygiene."

"You'd want to have some policy of using secure - encrypted - email," he told the AP.

Hundreds of international delegates from governments and the private sector converged for the two-day conference to try to agree on the basics - how to enforce cybersecurity regulations across borders, what to do about countries that don't want to be regulated, how to protect government and company data and who will ultimately control cyberspace?

One of Thursday's topics was how to protect privacy without cloaking criminality, and whether cyberattacks could be seen as acts of war in the future.

Painter said many current cyber issues were covered under international humanitarian law that countries had signed up to.

"We don't need a new treaty," he said. "We need a discussion around the norms that are in cyberspace, what the rules of the road are and we need to build a consensus around those topics."

Hundreds of international delegates from governments and the private sector converged for the two-day conference to try to agree on the basics - how to enforce cybersecurity regulations across borders, what to do about countries that don't want to be regulated, how to protect government and company data and who will ultimately control cyberspace?

Michael Rake of BT Group PLC, one of the world's largest telecommunications companies, warned that world powers are being drawn into a high-tech arms race, with many already able to fight a war without firing a single shot.

"I don't think personally it's an exaggeration to say now that basically you can bring a state to its knees without any military action whatsoever," Rake said. He said it was "critical to try to move toward some sort of cyber technology nonproliferation treaty."

The suggestion drew a mixed response from cyberwarriors gathered in London for a conference on Internet security, although at least one academic praised it for highlighting the need to subject online interstate attacks to some kind of an international legal framework.

Cyberweapons and cyberwarfare have increasingly preoccupied policymakers as hacks and computer viruses grow in complexity.

Recent high-profile attacks against Sony Corp. and Lockheed Martin Corp. have made headlines, while experts described last year's discovery of the super-sophisticated Stuxnet virus - thought to have been aimed at sabotaging Iran's disputed nuclear program - as an illustration of the havoc that malicious programs can wreak on infrastructure and industry.

"You can close vital systems, energy systems, medical systems," Rake said. "The ability to have significant impact on a state is there."

More information:
The EastWest Institute: http://www.ewi.info/

The Telecommunication Union's response center: http://bit.ly/llCTv3