Senate: China hacked military contractor networks (Update)

September 17 2014, by Jack Gillum

Senate Armed Services Committee Chairman, Sen. Carl Levin, D-Mich., talks to reporters about cyberattacks from China, Wednesday, Sept. 17, 2014 on Capitol Hill in Washington. China's military hacked into computer networks of civilian transportation companies hired by the Pentagon at least nine times, breaking into computers aboard a commercial ship, targeting logistics companies and uploading malicious software onto an airline's computers, Senate investigators said Wednesday. (AP Photo/Lauren Victoria Burke)

China's military hacked into computer networks of civilian transportation companies hired by the Pentagon at least nine times, breaking into computers aboard a commercial ship, targeting logistics companies and uploading malicious software onto an airline's computers, Senate investigators said Wednesday.

A yearlong investigation announced by the Senate Armed Services Committee identified at least 20 break-ins or other unspecified cyber events targeting companies, including nine successful break-ins of contractor networks. It blamed China's government for all the most sophisticated intrusions, although it did not provide any detailed evidence.

The Senate report did not identify which transportation companies were victimized.

Investigators said China's military was able to steal emails, documents, user accounts and computer codes. They also said China compromised systems aboard a commercial ship contracted by Transcom for logistics routes, and hacked into an airline the U.S. military used.

The committee's chairman, Sen. Carl Levin, a Democrat, said the hacking put at risk the security of U.S. military operations. He called his committee's findings "very disturbing."

China's government did not immediately respond Wednesday to telephone messages and emails from The Associated Press requesting comment in Beijing, its embassy in Washington and offices at the United Nations.

Senate Armed Services Committee Chairman, Sen. Carl Levin, D-Mich., right, and Sen. Jim Inhofe, R-OK, talk to reporters about cyberattacks from China, Wednesday, Sept. 17, 2014 on Capitol Hill in Washington. China's military hacked into computer networks of civilian transportation companies hired by the Pentagon at least nine times, breaking into computers aboard a commercial ship, targeting logistics companies and uploading malicious software onto an airline's computers, Senate investigators said Wednesday. (AP Photo/Lauren Victoria Burke)

The newly declassified Senate report says defense contractors have generally failed to report to the Pentagon hacker break-ins of their systems as required under their business agreements.

Levin, whose staff investigated the break-ins with the committee's top Republican, Oklahoma Sen. Jim Inhofe, said government agencies also failed to share information among themselves about intrusions. He said that hampers the government's ability to protect national security.

For instance, the committee said some contractors that contacted the FBI about break-ins may have not separately reported the intrusions to Transcom because the firms assumed the bureau already had notified the Pentagon. Levin said he and Inhofe were working on a bill to streamline the reporting process.

Federal data show more than $4 billion in contracts went to firms in 2012 and 2013 for the Civil Reserve Air Fleet, a Transcom partnership with private airlines that supplements Pentagon airlifts during wars or natural disasters. Six of 11 companies that investigators contacted about cyber intrusions were CRAF airlines.

The largest recipient of reserve fleet funding during that period, FedEx Corp., did not answer questions from the AP on Wednesday asking whether it was a victim of hacking. In a written statement, it instead said generally it was "confident in the integrity and safety of our systems, including those supportive of our government contracts."

Other Transcom contractors included firms that have since filed for bankruptcy and ended operations, including Georgia-based World Airways Inc. and Oregon-based Evergreen International Airlines.

The significant intrusions were characterized as "advanced-persistent attacks," a category of cyber threats so sophisticated they are frequently associated with foreign governments. Of those APT-linked intrusions, Transcom was made aware of only two, which the committee's report said was troubling.

Some intrusions appeared to come from mundane ruses that targeted employees by email, a practice known as spear-phishing. In 2013, for example, an unnamed CRAF airline was the victim of a phishing attack that investigators suspect led to malicious software being downloaded on the airline's network.

Earlier this summer, in an apparently unrelated investigation, the U.S. accused five members of the Chinese military of hacking computers for economic espionage purposes. It said they hacked into five U.S. nuclear and technology companies' computer systems and a major steel workers union's system, conducting economic espionage and stealing confidential business information, sensitive trade secrets and internal communications for competitive advantage.

Although Attorney General Eric Holder vowed to bring them to a U.S. courtroom to face the groundbreaking criminal charges, they are believed to be living freely. The Senate committee said Wednesday it hadn't referred its Transcom probe to the Justice Department.