# Press Release | Press | United States Commitee on Armed Services

armed-services.senate.gov/press-releases/sasc-investigation-finds-chinese-intrusions-into-key-defense-contractors

## SASC investigation finds Chinese intrusions into key defense contractors

## Report describes threats to transportation systems, gaps in reporting requirements

Wednesday, September 17, 2014
WASHINGTON – Hackers associated with the Chinese government successfully penetrated the computer systems of U.S. Transportation Command contractors at least 20 times in a single year, intrusions that show vulnerabilities in the military's system to deploy troops and equipment in a crisis, a Senate Armed Services Committee investigation has found.

The year-long investigation found that TRANSCOM, which is responsible for global movement of U.S. troops and equipment, was only aware of two of those intrusions. It also found gaps in reporting requirements and a lack of information sharing among government entities that left the command largely unaware of computer compromises by China of contractors that are key to the mobilization and deployment of military forces.

These and other findings are included in a report, "Inquiry into Cyber Intrusions Affecting U.S. Transportation Command Contractors," that the committee approved unanimously this spring. The committee released an unclassified version of the report today.

"These peacetime intrusions into the networks of key defense contractors are more evidence of China's aggressive actions in cyberspace," said Sen. Carl Levin, D-Mich., the committee's chairman. "Our findings are a warning that we must do much more to protect strategically significant systems from attack and to share information about intrusions when they do occur."

"We must ensure that cyber intrusions cannot disrupt our mission readiness" said Senator Jim Inhofe, R-OK, the committee's ranking member. "It is essential that we put into place a central clearinghouse that makes it easy for critical contractors, particular those that are small businesses, to report suspicious cyber activity without adding a burden to their mission support operations."

The committee investigation focused on a little-recognized but vital U.S. military asset: the ability to tap civilian air, shipping and other transportation assets to rapidly deploy U.S. forces in times of crisis. Through programs such as the Civil Reserve Air Fleet, commercial transportation companies, some of whom do little or no CRAF-related business in peacetime, become key elements of TRANSCOM's plans for moving troops and equipment around the world.

The committee found that in a 12-month period beginning June 1, 2012, there were about 50 intrusions or other cyber events into the computer networks of TRANSCOM contractors. At least 20 of those were successful intrusions attributed to an "advanced persistent threat," a term used to designate sophisticated threats commonly associated with governments. All of those intrusions were attributed to China. Among the investigation's findings:

> A Chinese military intrusion into a TRANSCOM contractor between 2008 and 2010 that compromised emails, documents, user passwords and computer code.
>
> A 2010 intrusion by the Chinese military into the network of a CRAF contractor in which documents, flight details, credentials and passwords for encrypted email were stolen.
>
> A 2012 Chinese military intrusion into multiple systems onboard a commercial ship contracted by TRANSCOM.

The investigation found significant gaps in information sharing regarding cyber intrusions. A committee survey of a small subset of TRANSCOM contractors discovered 11 intrusions by China into contractor networks. The investigation also found that the FBI or DoD were aware of at least nine other successful intrusions by China into TRANSCOM contractors. Of those 20 intrusions, TRANSCOM was only made aware of two.

That gap was in part a result of contractors and TRANSCOM lacking a common understanding of what intrusions ought to be reported to TRANSCOM. Also, DoD agencies lack a clear understanding as to what information about cyber intrusions can and should be shared with TRANSCOM and other agencies within the Department.

The committee also found that cyber intrusion reporting requirements are focused on intrusions that affect DoD data. Some TRANSCOM contractors, such as several CRAF airlines, however, may do little or no business with the military until called upon in a crisis. Peacetime intrusions at those companies may not involve immediate loss of military information, but could leave those companies vulnerable to loss of information or disruption of operations when they are activated to support military operations.

In response to the investigation's findings, the committee included a provision in its version of the National Defense Authorization Act for Fiscal Year 2015 directed at addressing reporting gaps and improving the way in which the Department disseminates information about cyber intrusions into the computer networks of operationally critical contractors.

Specifically, the provision directs the Secretary of Defense to establish procedures for designating companies as "operationally critical contractors" and tightening requirements that those contractors report successful cyber penetrations by known or suspected government actors. It also requires DoD to establish new procedures to assist contractors in detecting and mitigating cyber threats while ensuring protections for trade secrets, commercial or financial information.

The provision requires the Secretary to assess existing reporting requirements and DoD policies and systems for sharing information on cyber intrusions. It also requires the Secretary to designate a single DoD component to receive intrusion reports from contractors and other government agencies and to issue guidance ensuring that intrusion-related information is shared with appropriate DoD components.

###

## Related Files

Adobe Acrobat document.SASC_Cyberreport_09-17-14