US advised to examine 'hack back' options against China

November 17 2015, byMatthew Pennington

The United States remains ill-prepared to combat state-backed cyber intrusions from China and lawmakers should look at whether U.S.-based companies be allowed to 'hack back' to recover or wipe stolen data, a congressional advisory body said Tuesday.

That's the primary recommendation of this year's report by the U.S.-China Economic and Security Review Commission that examines the national security implications of the relationship between the two world powers.

The report says China's increasing use of cyber espionage has already cost U.S. companies tens of billions of dollars in lost sales and expenses in repairing the damage from hacking. It says in many cases, stolen trade secrets have been turned over to Chinese government-owned companies.

The commission, typically very critical of Beijing, is appointed by both parties in Congress but makes no bones about the "inadequate" U.S. response, saying China has also infiltrated a wide swath of U.S. government computer networks.

"The United States is ill-prepared to defend itself from cyber espionage when its adversary is determined, centrally coordinated, and technically sophisticated, as is the CCP and China's government," the report says, referring to the ruling Chinese Communist Party.

Cybersecurity has becomes an increasingly sore point in U.S.-China

relations. It remains to be seen whether a September agreement between President Barack Obama and China's President Xi Jinping that neither government will support commercial cyber theft will lead to an easing in the tensions.

Among the most serious breaches in the past year in which China is suspected was against the Office of Personnel Management, revealed in April. Hackers gained access to the personal information of more than 22 million U.S. federal employees, retirees, contractors and others, and millions of sensitive and classified documents.

"The Chinese government appears to believe that it has more to gain than to lose from its cyber espionage and attack campaign. So far, it has acquired valuable technology, trade secrets, and intelligence. The costs imposed have been minimal compared to the perceived benefit. The campaign is likely to continue and may well escalate," says the report.

China describes itself as a victim of hacking and says that is combating cybercrimes. It denied involvement in the OPM hack.

The commission's report says U.S. law does not allow retaliatory cyberattacks by private citizens and corporations, nor does it appear to allow 'hack backs' to recover, erase or alter stolen data in offending computer networks. It says international law has not kept up with developments in cyber warfare, and recommends Congress assess the coverage of U.S. law in this regard.

Congress should also study the feasibility of having a foreign intelligence cyber court to hear evidence from U.S. victims of cyberattacks and decide whether the U.S. government might hack back on a victim's behalf, the report says.

Richard Bejtlich, chief security strategist at FireEye, a U.S. network

security company, said there wouldn't be much appetite in the private sector for this. He said it should be the U.S. government that conducts any counter intrusions, but publicly available information indicates that offensive cyber activities by the U.S. to date have been focused on intelligence targets and centers of state power rather than targeting groups that are hacking the private sector.

"We need to get our hackers to go after their hackers to put pressure on them and disrupt their operations," Bejtlich said. "We need to start with more government pressure, not put the private sector in that role."

The commission's report, which surveys a wide range of economic and security developments in China, also criticizes its censorship and restrictions on Internet content and the impact that has on U.S. businesses. The report accusing China of a "government effort to wall off the fastest-growing market in the world for digital commerce."