THE WALL STREET JOURNAL.

Chinese Hackers Hit U.S. Media

Wall Street Journal, New York Times Are Breached in Campaign That Stretches Back Years

Published January 31, 2013

The New York Times

Bank Hacking Was the Work of Iranians, Officials Say

Published: January 8, 2013

The New York Times

In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back

Published: October 23, 2012

Bloomberg

China-Based Hacking of 760 Companies Shows Cyber Cold War

Published Dec 14, 2011

The Washington Post

Chinese cyberspies have hacked most Washington institutions, experts say

Published February 20, 2013

The list of those hacked in recent years includes law firms, think tanks, news organizations, human rights groups, contractors, congressional offices, embassies and federal agencies.

Pentagon acknowledges Chinese cyberthreat

Published February 19, 2013

MANDIANT

APT1

Exposing One of China's Cyber Espionage Units

China cyberattack

US firm Mandiant has issued a 74-page report on a global cyber espionage campaign by what it says is a Chinese government-backed organization dubbed APT1 (Advanced Persistent Threat 1)

APT1 global attacks since 2006

141 organizations targeted in 15 countries

"One of the most prolific cyber espionage groups in terms of sheer quantity of information stolen": Mandiant

Source: Mandiant

AFP

CISPA: What the bill does

- 31 page bill that breaks down legal barriers so the government can share classified cyber threat information with private companies
- Voluntary, private-sector solution
- Passed the House last year with 206 R's, 42 D's
- Allows the private sector to protect its networks and the intellectual property and private customer records that reside on it

CISPA: What the bill doesn't do

- Create a government surveillance program
- Allow the NSA to read Americans' emails
- Create a big, regulatory scheme with mandates and standards
- Allow the government to get their hands on individuals' personally identifiable information

CISPA: Privacy Protections

- Only allows the government to receive, use and retain information that relates to a cyber threat
- In that cyber threat information, it requires the government to minimize any personally identifiable information it may receive
- Restricts private to private sharing
- Deletes national security use purpose
- Requires the Intelligence Community's Inspector General to annually review and report on the program
- Adds role for the Privacy and Civil Liberties Oversight Board
- No information can be used for marketing

Key Supporters of CISPA

Review and Outlook – May 22, 2012

Who's Afraid of #CISPA?

A modest cybersecurity bill deserves support.

"If Congress ignores the ill-informed noise on Twitter and passes this or a similar bill, the U.S. will be better positioned to guard against a "digital Pearl Harbor."