

## White House announces anti-theft trade strategy (Update)

February 20 2013, by Nedra Pickler

---



The building housing "Unit 61398" of the People's Liberation Army is seen in the outskirts of Shanghai, Tuesday Feb. 19, 2013. Cyberattacks that stole information from 141 targets in the U.S. and other countries have been traced to the Chinese military unit in the building, a U.S. security firm alleged Tuesday. According to the report by the Virginia-based Mandiant Corp., it has traced the massive amount of hacking back to the 12-story office building run by "Unit 61398", and that the attacks targeted key industries including military contractors and companies that control energy grids. China dismissed the report as "groundless."(AP Photo)

The Obama administration announced new efforts Wednesday to fight the growing theft of American trade secrets, a broad but relatively restrained response to a rapidly emerging global problem that was brought into sharp focus this week by fresh evidence linking cyberstealing to China's military.

Mentioning China but not specifically targeting that country, Attorney General Eric Holder announced the plan, which includes a new diplomatic push to discourage intellectual property theft abroad along with better coordination at home to help U.S. companies protect themselves.

The administration says indications are that economic espionage is increasing, not only through electronic intrusion over the Internet but also through the recruitment of former employees of U.S. companies with knowledge of inside trade information.

"Particularly in this time of economic recovery, this work is more important than it ever has been before," Holder said at the White House announcement of the administration's strategy.

"As new technologies have torn down traditional barriers to international business and global commerce, they've also made it easier for criminals to steal trade secrets—and to do so from anywhere in the world," Holder said. "A hacker in China can acquire source code from a software company in Virginia without leaving his or her desk. With a few keystrokes, a terminated or simply unhappy employee of a defense contractor can misappropriate designs, processes, and formulas worth billions of dollars."

Earlier this week, a Virginia-based cybersecurity firm, Mandiant, accused a secret Chinese military unit in Shanghai of years of cyberattacks against more than 140 companies, a majority of them

American. The accusations and supporting evidence increased pressure on the United States to take more action against the Chinese for what experts say has been years of systematic espionage.

The Chinese government denied being involved in cybertheft, with China's defense minister calling the Mandiant report deeply flawed. China's Foreign Ministry said that country has also been a victim of hacking, much of it traced to the United States.

Wednesday's Obama administration report did not target any one violator, but the China problem was evident in the case studies it cited. Those examples did not involve cyberattacks but rather the theft of hundreds of millions of dollars in trade secrets by former employees of U.S. corporations including Ford Motor Co., DuPont Co., General Motors Corp., Cargill, Dow Chemical Co., Valspar and Motorola.

The administration report didn't threaten any specific consequences for theft of trade secrets, and no new fines or other trade actions were announced. It included five actions to protect American innovation:

- Applying diplomatic pressure by senior officials to foreign leaders to discourage theft.
- Promoting best practices to help industries protect against theft.
- Enhancing U.S. law enforcement operations to increase investigations and prosecutions.
- Reviewing U.S. laws to determine if they need to be strengthened to protect against theft.
- Beginning a public awareness campaign.

President Barack Obama signed an executive order last week aimed at helping protect the computer networks of American industries from cyberattacks. It called for the development of voluntary standards to protect the computer systems that run critical sectors of the economy such as the banking, power and transportation industries. It directed U.S. defense and intelligence agencies to share classified threat data with those companies.

He also prodded Congress during his State of the Union address to go further.

"Now, Congress must act as well by passing legislation to give our government a greater capacity to secure our networks and deter attacks," Obama said.

The president said America's enemies are "seeking the ability to sabotage our power grid, our financial institutions and our air traffic control systems. We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy."

Copyright 2013 The Associated Press. All rights reserved. This material may not be published, broadcast, rewritten or redistributed.

Citation: White House announces anti-theft trade strategy (Update) (2013, February 20) retrieved 12 September 2024 from <https://phys.org/news/2013-02-white-house-anti-theft-strategy.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.