HSTODAY.US
Insight & Analysis for Government Decision Makers

Search

Enter keywords

Sponsored by:

GENERAL DYNAMICS
Information Technology

Read the digital edition of *Homeland Security Today.*

Read the digital edition of *National Guard Today.*

About Us | Contact Us | Advertise | Subscribe to Magazine

Home | Briefings | Blogs | Channels | Focused Topics | Media Library | Resources | Newsletters | Events & Awards | Industry News | Magazine

Counternarcotics, Terrorism & Intelligence

Chinese Cyber Espionage Concerns Point To 'Deep Contamination'

By: Dan Verton
10/12/12

SHARE

'The House Permanent Select Committee on Intelligence on Oct. 8 recommended that two of China's largest telecommunications firms be blocked from business in the US involving critical national infrastructure, and that US government contractors should not use equipment manufactured by the two companies in government enterprises.

The two companies, Huawei Technologies Co. and ZTE Corp., "cannot be trusted to be free of foreign state influence and thus pose a security threat to the United States and to our systems," stated the bipartisan House Intelligence Committee *Investigative Report on the US National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*.

As a result, "US government systems, particularly sensitive systems, should not include Huawei or ZTE equipment, including component parts," the report recommended.

But while the House intelligence committee report raises an important alarm about the rising tide of Chinese hacker attacks against US government networks and private sector trade secrets, security experts warn the larger problem of Chinese cyber espionage goes well beyond any potential threat that Huawei and ZTE may pose.

"When I was a computer crimes prosecutor in the 1990s, we were very concerned about other countries stealing trade secrets from American companies, such as Russia, France, and Israel," said Peter Toren, an intellectual property and computer crimes expert with Weisbrod Matteis & Copley in Washington, DC and a former prosecutor in the Department of Justice (DOJ) Intellectual Property and Computer Crimes Division.

"But if you look at the cases in the last five years, the only international involvement is Chinese. There is no other [significant] involvement," Toren said. "I just don't see that as a coincidence. It's obvious that both the Chinese government and Chinese companies are seeking both legally and illegally to obtain trade secrets."

In fact, Toren recently conducted an analysis of the latest economic espionage cases prosecuted by DOJ. His findings show that of the 50 most recent economic espionage cases more than 30 percent have some sort of link to China. Those links, he said, often involved subtle direction by the Chinese government or Chinese companies that targeted US technology for the purpose of competing with US companies.

The House intelligence committee report released this week, however, is the latest in a series of red flags raised about Huawei and ZTE. Not only has the government of Australia blocked Huawei from participating in its national broadband project, but Great Britain took extraordinary steps to set up a separate security evaluation and certification process for Huawei equipment before it is allowed to be

Channels

- DHS
- DoD/National Defense
- Global
- Federal/State/Local
- FEMA
- US Coast Guard
- US National Guard

Focused Topics

- Airport & Aviation
- Biometrics & ID Management
- Border Security
- Counternarcotics, Terrorism & Intelligence
- Customs & Immigration
- Cybersecurity
- Emergency Management/Disaster Preparedness
- Information Technology
- Infrastructure Security
- Interoperable Communications
- Port & Cargo
- Public Health
- Public Safety
- Surveillance, Protection & Detection
- Transportation

Ask The Experts

Join *Ask the Expert's* Patrick Schambach, vice president and general manager of CSC's Department of Homeland Security Division, in a discussion about the latest in homeland and government security. Check out the current discussion: "We recently saw deployed throughout the UK telecommunications infrastructure.

And a year ago this month, a bipartisan group of senators wrote to the chairman of the Federal Communications Commission (FCC) warning the FCC about a proposed deal between Sprint, Huawei and ZTE.

“We are very concerned that these companies are being financed by the Chinese government and greatly influenced by the Chinese military, which may create an opportunity for the Chinese military to manipulate switches, routers or software embedded in American telecommunications network so that communications can be intercepted, tampered with or purposely misrouted,” wrote US Sens. Jon Kyl (R-Ariz.), Joe Lieberman (ID-Conn.) and Susan Collins (R-Maine). “This would pose a real threat to our national security.”

China’s grand strategy

It is in the Peoples Republic of China (PRC) where the military-industrial complex truly comes to life. Nowhere is this more evident than in the 1997 "16-Character Policy" that makes it official PRC policy to deliberately intertwine state-run and commercial organizations for the benefit of PRC military modernization.

In their literal translation, the 16 characters mean as follows:

- Jun-min jiehe (Combine the military and civil)
- Ping-zhan jiehe (Combine peace and war)
- Jun-pin youxian (Give priority to military products)
- Yi min yan jun (Let the civil support the military)

The 16-Character Policy is important because of what it does for the PRC’s industrial and economic espionage program: It provides commercial cover for trained spies who work directly for the PRC’s military establishment. And their only mission in life is to gain access to, and steal the high-tech tools and systems developed by, the US and its Western allies.

The two primary PRC organizations involved in actively collecting US technological secrets are the Ministry of State Security (MSS) and the Military Intelligence Department (MID) of the People’s Liberation Army (PLA). The MSS relies upon professionals, such as research scientists and others employed outside of intelligence circles, to collect information of intelligence value. In fact, some research organizations and other non-intelligence arms of the PRC government direct their own autonomous collection programs.

Many of these so-called “princelings” — named for their political family connections within the PRC’s Communist Party — use their political and business connections abroad to surreptitiously acquire technologies developed by US firms. They employ a wide range of tactics, including managing covert collection operations, acquiring the assets of various US-based commercial businesses and even establishing front companies to gain access to sensitive and proprietary technologies.

Recent studies suggest that there are currently more than 3,000 corporations operating in the US that have ties to the PRC and its technology collection program. Many are US-based subsidiaries of Chinese-owned companies. And while in the past they were relatively easy to identify, recent studies indicate that many have changed their names in an effort to distance themselves from their PRC owners.

Deep contamination

Huawei and ZTE have become the poster companies of what the real concerns are. They manufacture the equipment that forms the central nervous system of telecommunications networks. And their hardware is *already* embedded in tens of millions of devices globally, providing what one economic espionage investigator called a “deep contamination” challenge for US companies and government agencies.

“Malware, as well as zombie behavior and non-user controlled communications instructions, can be embedded not only in personal computer applications, but also in firmware and in primary and ancillary chip sets,” said Steve Lee, managing partner of Steve Lee & Associates in Los Angeles and a former defense industry computer science expert.

“To the extent that computer technologies are manufactured in China, it is subject to being contaminated with malware that resides way below the application layer. It’s not a difficult thing to embed malware into the silicon – the chipset, the firmware,” Lee said.

“We’ve found malware in the firmware of some very high quality communications gear, such as encrypted radios that have ethernet ports in them. And it’s not just PCs. This can be happening at the equipment and component level, such as printers, communications gear, switches and all of the kinds of things that go into a network.”

The specific concern about the Huawei equipment is that “those devices are sending beacons, maybe just a single packet of data, to somebody outside the network to let them know it is up and running and can be contacted or controlled remotely,” explained Jason Lewis, the chief scientist at Lookingglass Cyber Solutions Inc. in Baltimore, MD and a former global network exploitation and vulnerability analyst with the National Security Agency (NSA).

And on networks that handle millions of packets per second, “you wouldn’t even know that is happening," Lewis noted.

heightened homeland security risk levels around the anniversary of Osama Bin Laden’s death, including tightened security at airports. Should air travelers be more nervous at times like this?”

Click here to ask Pat a question.

Click here to participate in this security discussion.

Education Directory

- Askew School of Public Administration and Policy, Florida State University
- Auburn University's Center for Governmental Services
- Loma Linda University, School of Allied Health Professions
- Loma Linda University, School of Public Health
- Nash Community College
- Northwestern University
- University of Cincinnati
- University of Nevada, Las Vegas
- West Texas A&M University
- Western Carolina University

More Companies »

Calendar

Oct 24 Washington, DC	2012 Government Workforce: Learning Innovations Conference
Oct 25 - 31 Miam, FL	Hacker Halted USA 2012
Oct 26 - Nov 1 Orlando, FL	IAEM Annual Conference & EMEX Expo
Oct 26 Orlando, FL	Countermeasures 2.0
Oct 29 - Nov 2 San Diego, CA	HALO Counter-Terrorism Summit
Oct 30 - 31 Ottawa,	SECURETECH 2012
Nov 7 Washington, DC	Symantec Government Symposium

More Calendar »

Poll of the Week

Al Qaeda Central may be operationally diminished, but it's global, ideological kindred franchises and followers are very active and breed lone wolves and independent cells. Do you believe this metamorphosis represents an AQ 2.0 threat?

The challenge of detecting these so-called “deep contamination” threats is well known in defense and intelligence circles. But most private companies and civilian government agencies rely on commercial security products that are largely incapable of detecting threats embedded in the chipsets or firmware.

According to Lewis, the Department of Defense (DOD) and some contractors working on sensitive programs will actually x-ray newly purchased hardware to study it at the schematic level. “They’ll take it apart and put it back together again to see if there is anything out of the ordinary,” Lewis said.

Sumit Agarwal, vice president of product management at Mountain View, Calif.-based Shape Security said DOD will do even more to ensure their most sensitive networking and security equipment is secure. "They will actually insist on trusted provenance, making sure items are manufactured in the US and they will check it from time of assembly to time of delivery," said Agarwal, who is also the former head of Google’s mobile product management and an advisor for cyber innovation and executive at DOD.

In addition to the threats at the firmware and chipset level, there is the danger of manipulation at the network level. And while you may stop the most brazen attacks by preventing those you don’t trust from providing technologies to US critical infrastructure, it doesn’t solve the entire Chinese espionage problem,” said Lee. “If they already built the chipsets and firmware that operate the networking gear, then we really haven’t solved the problem. The one thing I would not do is become sanguine about our network security because we kept Hawei out of the business. That would be a bad call.”

In a statement issued after the release of the House intelligence committee report, a spokesperson for Huawei said the committee’s investigation relied on “many rumors and speculations to prove non-existent accusations,” and added that Huawei “is no different from any start-up enterprises in Silicon Valley.”

Lewis said he believes the House intelligence committee's recommendations to bar Huawei and ZTE from acquisitions and mergers in the US telecommunications industry is the prudent and cautious approach. “I don’t think I would purchase anything from Huawei,” he said. “But the reality is that I’m using a MacBook Pro right now and if you look on the bottom it says ‘Made in China.' The reality is everything is made in China.”

<--Return to Listing

○ Yes
○ No

Vote Now

Click Here for Poll Archives

HSTODAY.US

About Us | Contact Us | Advertise | Subscribe to Magazine | Privacy Policy | Site Map
Briefings | Blogs | Channels | Focused Topics | Media Library | Resources | Newsletters | Events & Awards | Magazine | Industry News