

Red Herring or Real Threat? Security Gets Political

By Becky Bracken

Is it mere coincidence that Chinese gear manufacturers ZTE and Huawei have become the focal point of what essentially looks to be a public relations feeding frenzy for members of the U.S. House Intelligence Committee at the very same time election season has reached its full-fevered, sweaty, smelly peak?

Politicians running for everything from local city councils to even the most politicized, publicized national contests regularly, angrily demand “fairer” trade with China as a tool to create jobs and bolster a struggling economy. Keynes-versus-Hayek debates about economic theory aside, it’s a narrative that resonates with everyday struggling folk looking for someone, anyone to be pissed at about the whole mess.

Last month the House Intelligence Committee published its “Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications

Companies Huawei and ZTE,” which calls for U.S. telcos to boycott Huawei and ZTE based on concerns the companies are participating in state-sponsored espionage that poses a direct threat to U.S. national security. The report adds that executives from ZTE and Huawei failed to provide the committee with sufficient evidence to convince them they were not engaging in spying and other nefarious activities, and therefore must be up to something. Hardly the burden of proof most companies would be able to shoulder.

“Neither company was willing to provide sufficient evidence to ameliorate the Committee’s concerns,” the committee wrote in its report. “Neither company was forthcoming with detailed information about its formal relationships or regulatory interaction with Chinese authorities. Neither company provided specific details about the precise role of each company’s Chinese Communist Party Committee.”

The U.S. isn’t the first government to investigate Chinese



telecommunications equipment manufacturers. Earlier this year Australia barred Huawei from its National Broadband Network. Canadian officials have opened investigations into ZTE and Huawei. And the European Union has placed a similar investigation on hold, reports say, because of fears of upsetting the

critical free-trade agreement it has in place with China, the EU’s second largest.

Although the House Intelligence Committee report itself is light on evidence or specifics as to why so many lawmakers are convinced there’s something fishy going on,

there’s no denying the Chinese government has its fingerprints all over both companies. But is that really surprising given the nature of the communist state? And because telecommunications networks are of such vital government interest, governments all over the globe have made broadband buildout their business (see: exhibits one and two, Australia’s National Broadband Network and the House Intelligence Committee).

Huawei, which recently overtook Ericsson as the largest telecommunications equipment manufacturer in the world, was founded by the somewhat mysterious ex-military officer Ren Zhengfei, regularly cited by Forbes and other organizations as one of the richest and most influential people in China. Huawei is privately owned by its employees and not publicly traded on any exchange, nor is it subject to the transparency rules required for a publicly traded company. ZTE, the world’s fifth-largest equipment manufacturer, on the



Not for distribution or reproduction.

other hand, is publicly traded in notoriously regulation-light Hong Kong, but that hasn't done much to help its lackluster image. ZTE was founded with close ties to the Chinese Ministry of Aerospace.

The U.S. market for both ZTE and Huawei for their network equipment is fairly small — low single digits for both. Instead, handset sales through U.S. mobile carriers are what make up the current bulk of the companies' stateside action. Both had big plans for expansion in this country but will have to kiss them goodbye.

ZTE was recently investigated by the U.S. Department of Commerce for selling American-manufactured equipment to Iran, in violation of ratcheted-up sanctions against the Middle Eastern regime. Worse, the marked-up equipment is alleged to have been used by the Iranian government to suppress protest and censor content unfriendly to its current leadership; Reuters reported that after the sale of the equipment to Iran, the repressive government was "far more capable of monitoring citizens" than before.

Things went from worse to really worse after ZTE's Texas-based attorney Ashley Kyle Yablon turned whistle-blower and the investigation was handed over to the FBI, which found evidence of obstruction and a cover-up in relation to ZTE's dealings with Iran. (Not exactly something a company wants to brag about in a press release to the investment community.) And in mid-October ZTE announced brutal losses totaling as much as \$280 million over the last nine months.

Huawei has also lost opportunities in the U.S., not the least of which was a partnership with Symantec because the security organization feared losing access to classified information about cybersecurity threats if it continued to deal with the Chinese company. Symantec moved to sell off its 49 percent stake in Huawei, thus ending a four-year relationship.

The House Intelligence Committee's report cites concern that Chinese spies would use ZTE and Huawei's gear to gather intelligence or even unleash malware with the intent to cripple the U.S. telecommunications infrastructure. But the problem remains: of the five major telecommunications equipment providers — Huawei, ZTE, Alcatel-Lucent, Ericsson, and Cisco — all of them source some components from China, so if the argument is one of national security it's going to be difficult to build out a 21st-century broadband network without a little help from the country.

A request to the largest gear manufacturer in the world, Ericsson, for comment on how it can guarantee security with sourced components from China remained unanswered by press time.

Politicians running for everything from local city councils to even the most politicized, publicized national contests regularly, angrily demand "fairer" trade with China as a tool to create jobs and bolster a struggling economy.

Huawei and ZTE have proposed contracting with organizations like Electronic Warfare Associates that are trusted by the U.S. government to test high-tech gear. But the House Intelligence Committee report seems to dismiss that approach.

The Chinese are apoplectic about the report and subsequent U.S. ban and have signaled they aren't ruling out some sort of trade-ban retaliation. ZTE and Huawei remain indignant about what they see as unfair treatment from the U.S.

In a recent editorial published in a Communist Party tabloid, Commerce Ministry spokesman Shen Danyang said the congressional committee's report "violated [the U.S.'s] long-held free market principles and will undermine cooperation and development between the two countries." Meanwhile, both ZTE and Huawei interpret the move as a way to lock them out of the most lucrative market on the planet.

"The report released by the Committee today employs many rumors and speculations to prove non-existent accusations," Huawei spokesman William Plummer said in a statement. "This report does not address the challenges faced by the ICT industry. Almost every ICT firm is conducting R&D, software coding and production activities globally; they share the same supply chain, and the challenges on network security is beyond a company or a country. The Committee's report completely ignored this fact. We have to suspect that the only purpose of such a report is to impede competition and obstruct Chinese ICT companies from entering the US market."

Nonetheless, the committee and the FBI are undaunted, and in fact are pushing ahead with a second phase of the investigation. A staff member of the House Intelligence Committee told Reuters it has received "dozens and dozens" of calls from current and former employees, not to mention customers, of the Chinese firms with reports of their nefarious activities.

"I don't think the companies should expect our attention to stop," said the staff member, who was

not authorized to speak publicly on the matter.

In a global market it would seem utterly impossible to lock an economy as large as China's out of U.S. telecommunications technology altogether. But as the House Intelligence Committee continues to investigate the activities of these Chinese companies — and either intentionally or unintentionally chooses the industry's winners and losers in the process — the U.S. government starts to look more and more like China's. There is no denying the national interest in building a secure, robust telecommunications infrastructure, but what is emerging is a stark politicization of telecommunications networking on a remarkable scale that will inevitably send shock waves through industries and economies around the world.

And you can be sure, as the political season reaches its inevitable boiling point leading up to the November elections, that this story will stay in the headlines. Unfortunately for the telecommunications industry as a whole, the aftermath may be confusion and chaos in a sector that should be focused on innovation and the customer experience rather than political theater.

The White House denies that the yearlong investigation and congressional report is aimed at specific businesses. "We have a process that is not aimed at one specific company, but, using all the assets and parts of U.S. government, aimed at protecting our telecommunications and critical infrastructure," a senior White House official said. But only time, and perhaps the pending election, will truly tell.

Huawei has also lost opportunities in the U.S., not the least of which was a partnership with Symantec because the security organization feared losing access to classified information about cybersecurity threats if it continued to deal with the Chinese company.

During the last presidential debate of the 2012 campaign, discussions about Chinese industry copyright and patent infringement, artificially suppressed prices, and of course, security were heated topics of discussion. Telecommunications is an industry that crosses all three of those areas of American interest and will remain a highly politicized and scrutinized sector as it relates to Chinese trade and competition. With both presidential candidates vowing an increasingly tougher stance on Chinese trade, regardless of the election's outcome, it's clear the eyes of America will remain fixed on China's every move, and with it, ZTE and Huawei will remain in the glare of the klieg lights of American politics.