

Wall Street Journal (2.28.11)

Huawei's Bid to Crack Market, U.S. Sees a Threat From China Inc.

By JOHN BUSSEY

The Chinese opera starring Huawei Technologies Co. and Washington regulators hit another high note Friday when a spurned Huawei issued a public plea for understanding, fairness—and access to the rich U.S. telecom market.

Why has Washington repeatedly said no to Huawei as the China telecom giant tries to tap into the lucrative U.S. market? The Journal's John Bussey and Simon Constable discuss.

There are two lessons to draw from all the yodeling:

First, this drama isn't just about the Chinese suitor Huawei. It's about China Inc. and cybersecurity in the U.S. Because of that, Huawei may not be getting into the U.S. market in a big way anytime soon.

And second, Huawei—one of the biggest suppliers of telecom equipment in the world—may be the least of America's problems when it comes to thwarting aspiring cyberspies.

Huawei's latest travails stem from a tiny deal the company struck in California. It bought some patents and hired some employees from an outfit called 3Leaf Systems that did work in cloud computing. The Pentagon demanded Huawei retroactively seek approval of the transaction from a secretive panel called CFIUS, which reviews foreign investment that might threaten national security.



Sen. Jon Kyl and other U.S. lawmakers have likened Huawei to a dangerous arm of communist China intent on snatching U.S. secrets.

Huawei cried foul and said the deal didn't merit review because it wasn't an outright acquisition. Sens. Jim Webb and Jon Kyl and other U.S. lawmakers fired back, likening

Huawei to a dangerous arm of communist China intent on snatching U.S. secrets. This month, CFIUS essentially ordered Huawei to unwind the purchase. As the dust settled, a Chinese government spokesman condemned the decision and, in an ironic footnote, grumbled that the U.S. should be "more transparent" in how it treats foreign investors.

Then on Friday, Huawei publicly challenged the U.S. to investigate the company and clear the air.

"Huawei is Huawei," says Bill Plummer, the company's spokesman. "It's a multinational company. It isn't China. It shouldn't be held hostage to the tense relationship between the two governments." Huawei's supporters say U.S. companies are missing out on quality Huawei gear that's safely sold to virtually every major phone company in the world.

Maybe so, but a range of intelligence agencies that sit on CFIUS, or the Committee on Foreign Investment in the U.S., appear to feel differently. Huawei's plea "seems disingenuous," says an individual familiar with the government's thinking. "Why come out with that offer publicly? We've been asking for transparency" from the company for years.

The problem is that Huawei lives in a certain context. Its founder served in the People's Liberation Army. The company has prospered greatly in its home market and has grown almost overnight into a global giant. And while Huawei insists it is entirely independent of the Chinese government, the company thrives in an authoritarian country where success on so large a scale is usually carefully observed, and carefully prescribed. There are few subjects of greater interest to Beijing than telecommunications and technology—and creating national champions in both.

Rightly or wrongly, Huawei to many people in Washington is a proxy for China. They fear the company's equipment may contain bugs that could spy on American industrial secrets, shut down communications during a conflict, or make networks easier to hack. Huawei says that's nonsense.

CFIUS proceedings are secret, and a spokeswoman declined to comment on the Huawei case. But actions speak loudly. The committee, which includes the departments of Homeland Security and Defense, has blocked Huawei's access to the U.S. repeatedly, including Huawei's bid to buy electronics maker [3Com Corp.](#) in 2008, its effort to upgrade [Sprint Nextel Corp.](#)'s network in 2010, and now the [3Leaf](#) deal.

Noting the importance of context, a former intelligence official says: "You have senior officials in Washington going to work every week and their assistants telling them, 'Sir, the Chinese have hacked into your system and are reading your email again. We're trying to get them out. Don't use your computer.' China is contemptuous when we complain about this, and that probably deepens the reaction toward Huawei," he says.

Even Washington knows that at the end of the day Huawei is but a blip on a much larger radar screen of worry. Virtually every technology company is plugged into a global supply chain and gets its products from multiple sources. A given piece of consumer or industrial

electronics can cross borders dozens of times as it is designed, coded and assembled before landing in the U.S. The rogue might be anywhere: in China, or in the piece of equipment stamped INDIA that was preassembled in China.

"The cyber side is where the real national-security issues are growing exponentially, the vulnerabilities created by the global supply chain," says Nova Daly, a consultant with Wiley Rein in Washington who previously managed the CFIUS program at the Treasury Department. "We need clear cyberpolicy from the administration and Congress."

That effort is under way, there are some early steps to better vet the source of key electronics distributed in the U.S. Scrubbing software and hardware before it crosses the border is a tricky business. Experts say it's almost impossible to find every bug.

So trusting the source of origin becomes all the more important.

And that's the hill Huawei must climb.