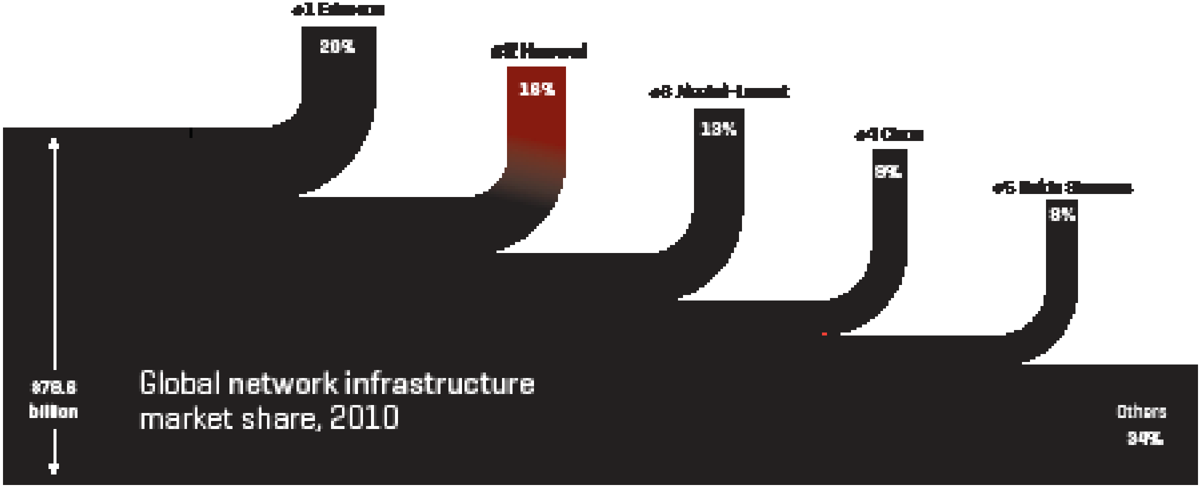
WHAT MAKES THIS CHINESE TELECOM SO SCARY?

It could soon be the world's biggest maker of network gear, but Huawei still can't conquer the U.S. The reason? **Widespread fear that it's here to spy for Beijing.**

By Sheridan Prasso · *Illustration by Alex Varanese*

RISING POWER Huawei now has customers in 130 countries around the world, and its sales are on pace to grow 10% this year.



Touch the yellow box for company info.

XXX XXX XXX XXX XXX

Huawei, the world's second-largest supplier of telecom and Internet gear, has little trouble garnering business around the globe. The Chinese company has customers in 130 countries, sells equipment to 45 of the world's top 50 telcos, and brought in $27 billion in revenue in 2010—enough to rank No. 352 on *Fortune*'s Global 500 list. With sales on pace to grow another 10% this year, it's likely that Huawei (pronounced "HWAH-way") will soon race past Sweden's Ericsson and take over as the globe's No. 1 manufacturer of communications equipment. ¶ Yet success in the world's biggest telecom market, the U.S., has been hard to come by. Despite bidding again and again since it first entered America a decade ago, the company has yet to win a single big contract from the top-tier U.S. carriers, AT&T, Sprint, T-Mobile, and Verizon. →

There are some good reasons for that. U.S. telecom companies have long relationships with homegrown suppliers like Lucent (now part of France's Alcatel), Motorola, and Cisco. It's also true that for many years Huawei's gear just wasn't that good—fine for emerging markets, perhaps, but not for the 24/7 service and reliability required by U.S. networks. Today, however, Huawei is building some of the best, most innovative, and fastest equipment in the industry. Quality is no longer an issue. Über-tech investment banker Frank Quattrone recently cited Huawei as one of the industry's new leaders in remarks to a conference crowd.

But Huawei is facing resistance that goes beyond pure competition with its peers. Several members of Congress, joined by Gary Locke—the U.S. Commerce Secretary soon headed to Beijing as the next U.S. ambassador—have lobbied hard against Huawei. Meanwhile, U.S. regulators have blocked it from three acquisitions, and earlier this year forced it unravel its purchase of a defunct California cloud-computing company called 3Leaf.

What's behind the groundswell of public and private opposition? In a word, fear.

As one of the first Chinese companies to emerge as a global powerhouse, Huawei contends that it's a punching bag, a victim of worries about an ascendant China and growing concerns about cybersecurity and intellectual-property theft. This concern is deepened by American anxieties caused by the Great Recession and the accompanying mood of U.S. declinism. For politicians, hitting out at an increasingly assertive China taking on new prominence in the world—and at Huawei as its proxy—is

Touch the yellow box for company info.
S ALU CSCO MSI ERIC T VZ

an easy way to score political points. Another factor is protectionism by entrenched players that fear having their margins pinched, as happened in Europe when Huawei entered the market there.

Particularly vexing for Huawei is the suggestion that the company could be used to spy on behalf of the government in Beijing. Unverified assertions that the company is “linked” to the Chinese military appear regularly in news articles. The charges are largely based on the fact that Huawei’s media-shy founder and CEO, Ren Zhengfei, once served in the People’s Liberation Army as a telecom technician, and that the company (like AT&T, Sprint, and Verizon in the U.S.) is a military and government contractor in its home country. “The context of all this is, China is very active in espionage, as are we,” says James Lewis of the Center for Strategic and International Studies (CSIS) in Washington, D.C. At a minimum, says Lewis, Huawei has an image problem in cyber circles. “The national security community in the U.S. is united in its opposition to Huawei,” he says.

“It was a serious mistake for America not to [have had Sprint award Huawei the business],” says Bill Owens of Amerilink Telecom. “This is so compellingly wrong.”

Certainly there are very real security concerns to consider—a fact that virtually everyone in the cybersecurity world is quick to state and that Huawei itself concedes. In a world in which hacking is proliferating, no company or government agency wants to risk giving potential enemies the means to access its network by buying vulnerable equipment. But is the security risk really greater if the network's parts were sold by a Chinese company? Huawei argues that it's a multinational just like GE or IBM, and is only as vulnerable to intrusion as any other private corporation. It also points out that most equipment made by its main competitors—Ericsson, Alcatel-Lucent, and Nokia Siemens—is manufactured in China. What's to stop Chinese spies from infiltrating those operations?

Despite those barriers, Huawei shows no sign of giving up on its efforts to win over U.S. customers. To build relationships with carriers and develop products for the U.S. market, it has hired a slew of executives from Western companies such as Cisco, Ericsson, Intel, Nortel, and Sun. Matt Bross, Huawei's global chief technology officer and the first Westerner to reach Huawei's c-suite, joined from British Telecom. To work on its image in Washington, it engaged the lobbying firm of former Defense Secretary William Cohen. And in February, Huawei published an open letter inviting anyone, including the U.S. government, to investigate its business practices.

Rather than jump through hoop after hoop, wouldn't it be easier for Huawei just to retreat and be happy with its impressive growth everywhere outside America? Perhaps. But U.S. companies spend some $30 billion a year on telecom equipment, a figure that is set to rise as an industrywide network upgrade to 4G technology continues. If Huawei can convert its doubters, there are huge profits to be made in America. Give up? No way.

William Plummer, Huawei's point man in Washington, has developed a mantra for his meetings with politicians: "Huawei is Huawei, not the Chinese government."

WILLIAM PLUMMER, Huawei's trim and very polished government-relations point man, is an avid runner. Since he joined the company last year, the 47-year-old father of eight, who spent 12 years in a similar role at Nokia Siemens, has had ample opportunity to demonstrate his endurance. Plummer has been meeting with virtually anyone in government willing to listen to Huawei's side of the story (bolstered by a 17-slide PowerPoint pitch). He's also developed a mantra that encapsulates his message: "Huawei is Huawei, not the Chinese government."

This past March, just after regulators forced Huawei to unravel its 3Leaf acquisition, Plummer met with a half-dozen stern-faced members of a congressional committee focused on national security. Recounting the episode, Plummer gets visibly agitated as he recalls how the staffers suggested that Huawei was beholden to the wishes of Beijing. "Well, no," Plummer says he told them, emphasizing that Huawei is not a state-owned enterprise. "This year GE sold 150 locomotives to Pakistan. Following that logic, if the U.S. went to war with Pakistan, then GE would derail the trains? That's just silliness. That's not how a multinational company would want to risk its future."

Huawei's rise from startup to international powerhouse happened remarkably fast. Ren, the founder and CEO, served for 10 years in China's equivalent of the Army Corps of Engineers. In 1983 the corps was disbanded, and he was let go as part of a mass demobilization. The company says Ren founded Huawei in 1987 with $2,500 in savings plus funds collected from family members. (Ren almost never gives interviews and would not comment for this article.)

Huawei argues that it has no ties to the Chinese government. As Plummer likes to point out, the company is headquartered in Shenzhen, across the border from Hong Kong and far from Beijing. Huawei derives just 36% of its revenue inside China. The government has never taken any ownership stake, says Huawei, and the company is 100% employee-owned; Ren holds 1.42%. Huawei says it cannot launch a public stock offering because of Chinese rules that prevent companies with large employee ownership from going public. An IPO would also make much of the company's top management instant billionaires, points out

As one of the first Chinese companies to emerge as a global powerhouse,Huawei contends that it's a punching bag, a victim of worries about an ascendant China and growing concerns about cybersecurity.

Shang-Jin Wei, who chairs Chinese Business and Economy studies at Columbia Business School in New York. Those executives would likely leave, lopping decades of experience and expertise off the top of the company.

Huawei is often mentioned as having links with the People's Liberation Army (PLA). But Plummer says that it's a case of mistaken identity. He points to another Chinese company with a similar name which was in fact headed by a PLA officer and may have sold optical communications gear to Iraq under Saddam Hussein. The mixup, Plummer says, erroneously became part of a *Wall Street Journal Asia* article in 2001, then was referenced in a 2006 Rand Report—and has been falsely repeated ever since. "There was some confusion there," says Plummer. "Huawei has never delivered any military technologies at any time."

But the assertion of a complete separation between the Chinese government and private Chinese companies is not terribly convincing to the cybersecurity community, according to Adam Segal, a China expert and senior fellow for counterterrorism and national security at the Council on Foreign Relations. Beijing last year forced all government suppliers to turn over their encryption codes. Beijing also dangles the threat of corruption investigations to keep companies in line, even executing executives convicted of graft. "Private companies in China are always wondering what the government is going to want next," Segal says.

To alleviate security concerns, Huawei has volunteered to reveal its source code—as it has done with success in countries such as India and the U.K.—and allow ongoing monitoring through a company called Electronic Warfare Associates (EWA). The company has top security clearance with defense and intelligence agencies and therefore can stay abreast of all known cyber risks, says John Lindquist, president and CEO of EWA's infrastructure technologies group. Any Huawei customer can take advantage of EWA's vetting as part of a "trusted delivery" purchase of Huawei equipment. Still, Lindquist concedes, "nothing is 100% fail-safe." While security experts say the real vulnerabilities come not when the equipment is delivered but perhaps six months later when a patch or update is required, Lindquist says ongoing monitoring looks in on patches after the fact. "I'm very confident we'll find anything that's there," he says.

HUAWEI FIRST CAME to America on Valentine's Day in 2001. That's when a small group of Huawei employees led by Charlie Chen, a senior VP, arrived in Plano, Texas, to establish the company's first U.S. office. "I couldn't speak good English, didn't know how to drive," recalls Chen. "We started from our apartment, maybe four or five people, and we had no clue. To understand the market, to set up a strategy, was very hard."

Some three years later Huawei CEO Ren visited Texas to check on his emissaries. Huawei had yet to sign up a single U.S. customer, says Chen, and almost no one could pronounce its name. (The company had registered in the U.S. as "Futurewei" to make things easier, but that only caused confusion.) Ren had some advice for employees. "He said, 'We have to break through like a needle,'" says Chen. "'Put all the effort into one single product with one customer, break through, and then we can build up our recognition.'"

Huawei has continued to pour resources into the U.S. in the years since. The Plano office is now a 100,000-square-foot building and is the North

American headquarters. Huawei has set up 12 branch offices and seven R&D centers in the U.S., including a brand-new research center in Santa Clara, Calif., and now employs more than 1,100 people in the U.S., 75% of them Americans (some 200 Huawei employees in the U.S. have come from China). Huawei has the infrastructure to be a major telecom player in America.

But competitors have a compelling reason to shut Huawei out of the bidding for big contracts: margins. While U.S. operators do an estimated 15% of the global spending on telecom equipment, they account for up to 25% of the profit. That's because gross margins for telecom equipment in the U.S. are 45% to 50%. Before Huawei entered Europe in late 2004, margins for Ericsson and Alcatel-Lucent were that high too.

"The national security community in the U.S. is united in its opposition to Huawei," says James Lewis of the Center for Strategic and International Studies.

But they fell to 30% to 35% immediately after Huawei arrived and began bidding aggressively, according to a report titled "Chinese Water Torture" by analysts at Berenberg Bank in Hamburg. The gearmaker's new technology makes it an even more formidable competitor because it can create significant cost savings for customers. Its SingleRAN equipment, for example, can handle multiple types of signals—2G, 3G, WiMax, CDMA, GSM—on one box, freeing a carrier from building separate networks.

Last fall when Sprint Nextel solicited bids for a network upgrade, Huawei offered a deal that would have saved the carrier at least $800 million from its existing costs in its first year of operation alone, according to several industry sources. But members of Congress, led by Sen. Jon Kyl, Republican from Arizona, launched a letter-writing campaign urging Sprint not to include Huawei. And Commerce Secretary Locke reportedly called CEO Dan Hesse to convey his "very deep concerns" about national security. The $5 billion prize was split among Ericsson, Alcatel-Lucent, and Samsung. Kyl and Locke declined to comment on the matter.

Sprint's senior vice president of network, Bob Azzi, who made the contract decision, wouldn't acknowledge that Huawei had been a bidder. He says there are many costs to consider in an upgrade—including transitioning to a new technology—but that a warning from the Secretary of Commerce wasn't one of them. "I was not told what to do," he insists. "The bottom line is we made the choice in the business context we had. We decide on the costs; we decide on the benefits. Period."

The Huawei team was crushed—having been almost sure it was going to nail Sprint as its first Tier 1 contract in the U.S. To boost its chances, Huawei had formed a partnership with a company called Amerilink Telecom, headed by the former vice chairman of the Joint Chiefs of Staff, Adm. Bill Owens, who also was once CEO of Nortel Networks. "In my view it was a serious mistake for America not to [have had Sprint award Huawei the business],” says Owens. “They’re opening all their source code to Sprint, to the U.S. government, to everyone. At Nortel, I never would have opened the source code to anyone, especially not the U.S. government. This is so compellingly wrong in the way this has happened.”

Huawei has set up 12 branch offices and seven R&D centers in the U.S., including a brand-new research center in Santa Clara, Calif., and now employs more than 1,100 people in the U.S.

IT MAY NOT HAVE broken through to big U.S. carriers yet, but Huawei has begun to pick up serious momentum selling to mid-tier telecoms—from core infrastructure to consumer devices. Last year Huawei tallied $765 million in revenue in North America, more than double its total from the year before. One important customer is Leap, a spinoff from Qualcomm whose Cricket is the seventh-largest U.S. wireless operator. Leap first purchased Huawei’s 3G equipment in 2006, then base stations in 2007, and modems in 2010. Currently it sells Huawei’s affordable Android-based smartphone, the Ascend. T-Mobile offers the Huawei Ascend as well. And Best Buy sells a seven-inch Android-based tablet from Huawei called the IDEOS S7, which at under $300 is aimed at consumers who don’t want to splurge for an iPad.

Touch the yellow box for company info.

BBY LEAP

Some of that new business has led down surprising paths. For instance, another large customer is Internet wireless provider Clearwire, which, ironically, is majority-owned by Sprint. And Clearwire has a partnership deal to carry Sprint's 4G traffic—on Huawei's equipment, as it turns out. Clearwire declined to comment except to confirm that Huawei was previously its WiMax supplier and is now a supplier for its 4G network.

Then there's Level3 Communications—which operates secure-channel communications for over 200 government agencies, is a U.S. defense contractor, and forms what is called the backbone of the Internet, an IP transit network across the U.S. and Western Europe. That Level3 has purchased Huawei equipment is confirmed by industry sources and analysts, even though neither company has ever announced any deals. "It's base stations, core switching equipment—the kind of stuff that really ought to keep people up at night," one source says. Level3 responds that customer confidentiality is its highest priority, but that it does not "comment further on network security" issues.

Perhaps because of the cybersecurity issue, most of Huawei's customers decline to be interviewed about the company. One customer happy to talk was Robert Parsloe, founder and CEO of the new Northeast Wireless Networks, which is installing equipment to provide better cellular access and wireless broadband in remote places like Maine and Oregon. He raves that Huawei's SingleRAN box can handle both Sprint's CDMA

Touch the yellow box for company info.

LVLT

CLWR

and AT&T's GSM technologies—along with microwave Internet connections from Canada. "That's the winning solution out here, and why I got so hooked on the Huawei equipment," says Parsloe, an ex-Lucent employee. "They're really industry leaders by far on the technology side."

Before he made the purchase, though, he worried about security concerns based on what he had read. So Parsloe went to Washington—once a week for 2½ months from January through March. "I had meetings in D.C., on the Hill with senators and congressmen, and I went to the security agencies," he says. "I was not about to make a decision that might impair our national security." But he heard nothing that convinced him that equipment from Huawei would constitute any kind of threat. "I walked away feeling very comfortable making the decision based on my meetings and the agencies I met," he says.

Winning converts has not been easy for Huawei. But the company is willing to keep slogging away to reach its long-term goals. "We just have to be patient," says Charles Ding, head of Huawei North America. Huawei's plans call for moving into cloud computing and the enterprise space—bringing it into competition with the likes of Oracle, Avaya, Hewlett-Packard, Cisco, and Amazon. Worldwide, Huawei forecasts that its revenue will triple by 2020, to more than $100 billion—an ambitious goal and one it's unlikely to reach unless it can land top-tier customers in America. But if Huawei can convince enough people in Washington that its intentions are pure, it just might succeed.

Touch the yellow box for company info.
ORCL HPQ AMZN