Huawei is a...

- ○ A. 5G pioneer
- ○ B. Nightmare for Apple
- ○ C. Threat to America
- ○ D. Trump scapegoat
- ○ E. All of the above

The Chinese tech company is growing so powerful that Washington killed somebody else's $117 billion deal to hold it back

By Max Chafkin and Joshua Brustein

On March 12, fresh off his Twitter proclamation that "trade wars are good and easy to win," President Trump issued an executive order blocking the biggest tech merger in history. The plan had been for Broadcom Ltd., a Singaporean chipmaker, to acquire San Diego's Qualcomm Inc., the leading maker of cellphone modems, for $117 billion. Trump said he canceled the deal for fear that Broadcom "might take action that threatens to impair the national security of the U.S."

The move deflated even the characteristically fiery Hock Tan, Broadcom's chief executive officer. Trump had praised Tan at the White House months earlier. Moreover, Broadcom looks in most respects like an American company. Tan is a U.S. citizen and resident, the company's employees are mostly in California, the deal was underwritten by American private equity firms, and Broadcom had promised to relocate its headquarters back to California as part of the deal. What more could American national security interests want? Almost immediately, however, the conversation shifted from Broadcom to Washington's real concern: Huawei.

Huawei Technologies Co. is China's biggest tech company by revenue, with sales 60 percent greater than those of the runner-up, JD.com Inc. Huawei is one of the world's biggest producers of telecommunications networking equipment, despite a de facto ban that prevents America's four principal wireless carriers—AT&T, Verizon, T-Mobile, and Sprint—from using its gear. The company also makes an ever-growing share of the world's smartphones. These two factors have rendered it terrifying enough to many American policymakers that they're willing to leave Broadcom the loser in a bigger game.

Chuck Grassley of Iowa, one of the longest-serving Senate Republicans, says he's worried about the prospect of American telecommunications companies becoming dependent on a Chinese manufacturer whose motives he finds suspect. "I can't pronounce their name," Grassley says, "but it starts with an H and ends with a W-E-I. Whenever they're involved, it scares the devil out of me."

This fear, which Trump's executive order did little to soothe, stems partly from Huawei's wild success. Besides growing faster than Apple Inc. and Samsung Electronics Co., the only phone makers with more global market share, the company now has the production capacity and technical know-how to rival Qualcomm in the race to develop the fifth generation of wireless equipment, which promises to make possible superfast smartphone data connections, self-driving cars, and remote-controlled medical devices and industrial equipment.

A Huawei with greater sway over the 5G market could stand to sap billions of dollars from U.S. rivals and charge other companies pricey fees on any patents it enjoys. But hawks such as Grassley say the bigger problem is security—that the Chinese government could slip through backdoors into Huawei's networking hardware and software, enabling it to spy on Americans' phone calls, texts, and emails.

Trump's case against Broadcom's acquisition of Qualcomm rested on a peculiar bankshot between these two points. The White House argued that Tan, who tends to slash expenses wherever he goes, would likely cut Qualcomm's spending on research and development, indirectly giving Huawei a greater advantage in the race to develop 5G wireless standards and equipment. In a letter dated March 5, the Committee on Foreign Investment in the United States, or CFIUS, warned that the potential deal would lead to "a weakening of Qualcomm's position," leaving "an opening for China to expand its influence on the 5G standard-setting process." Because, the letter continued, of the "well-known U.S. national security concerns about Huawei and other Chinese telecommunications companies, a shift to Chinese dominance would have substantial negative national security consequences."

In early January, Mike Conaway, a Texas Republican, introduced a House bill that would ban the federal government from doing business with any entity that relies on Huawei equipment. Two weeks later, a leaked U.S. National Security Council draft memo on 5G networks described the progress of Chinese technology companies as a threat to American security. The memo mentioned two by name: Huawei and the smaller ZTE Corp. It called for the government to make a national 5G network an investment akin to President Eisenhower's interstate highway system.

Huawei dismisses American fears about its intentions as nationalistic fearmongering. It says it has no more connection to the Chinese government than Apple or Google and that installing backdoors for spies in its network hardware or software would be tantamount to market suicide. "We're 30 years in this business, and there hasn't been a single security issue," says Joe Kelly, the company's vice president for international media affairs. "Should America have anything to fear from us from a cybersecurity perspective? The answer is no."

The NSC memo damaged Huawei, even though the carriers initially laughed it off and the U.S. Federal Communications Commission disavowed it. Within a day, Verizon Communications Inc. reversed a plan to sell Huawei's phones in its stores. AT&T Inc. had already abandoned a similar partnership under pressure from Congress.

Two people familiar with the memo's creation say the White House is worried that U.S. wireless carriers lack the financial muscle to build four separate networks and that China will beat the U.S. to deploying the new technology unless Washington takes drastic action. In this context, the Broadcom deal's scuttling stands as an escalation of hostilities between the two countries that some have compared to the beginning of the Cold War. "This is a major concern," says a senior U.S. telecom executive involved in 5G policy discussions. "This is the new battleground, not F-35 fighters."

It's tough to see this conflict happening from inside the U.S., where the only mainstream phones are Apple's and Samsung's and existing networks are plenty fast for regular Facebooking. In China, the U.S. government's moves are considered the latest in a string of outrages. In the days ▶

Ren (right) with Chinese President Xi Jinping

◀ following the killing of the Broadcom deal, a hashtag that translated roughly as "Huawei banned in the U.S." appeared tens of thousands of times on Weibo, China's equivalent of Twitter. And on Feb. 1, the WeChat account of the *People's Daily*, the official Communist Party news outlet, published a post decrying American protectionism. "The robust rise of Huawei and the robust rise of China and the Chinese internet tech companies may have left the U.S. worried," the paper wrote. The post was later removed.

Of course, it's not easy these days to permanently hobble Huawei, which has grown into one of China's so-called national champions with the aid, critics say, of government contracts and near-unlimited lines of credit. The company has 180,000 employees, most of them engineers, and sells its products in 170 countries. Though it's privately held, Huawei reports earnings twice a year as part of a larger transparency effort designed to persuade foreign governments to contract with the company. It says it booked about $92 billion in revenue in 2017, up from $35 billion just five years earlier, and aims to top 12 figures in 2018.

And Huawei has lots of room to grow, especially if it takes a strong hand in developing 5G standards. The March CFIUS letter noted that Huawei has about 10 percent of the 5G patents so far, and the company says it has 300 of its best engineers working full time to develop more, with help from thousands of others. Huawei says it's spent $600 million on 5G research and expects to lay out an additional $800 million this year to bring the technology to market. It already has about 50 contracts with wireless carriers to test its equipment. Overall, it spent about $12 billion on R&D in 2016, compared with $5.1 billion for Qualcomm and $4.9 billion for Finland's Nokia Corp.

Huawei's headquarters, a sprawling, serene campus with low office buildings, a dozen cafeterias, and immaculately landscaped palm and banyan trees, would fit nicely in Silicon Valley. The one obvious flourish: a large man-made lake inhabited by a flock of black swans, which reclusive founder Ren Zhengfei is said to have imported from Europe as symbols of Huawei's uniqueness. There are other idiosyncrasies. The company is run by a trio of CEOs who serve rotating six-month terms, and it may be the world's largest business that's structured as an employee stock ownership plan.

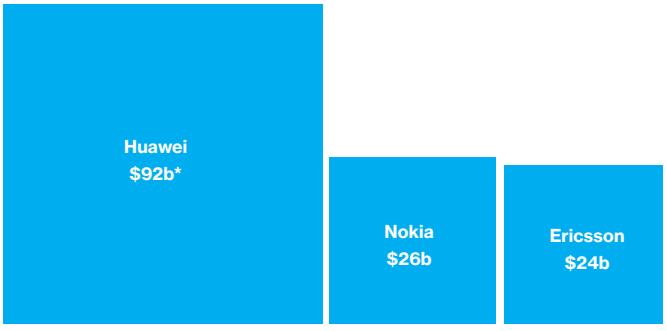
More familiar is the role of Ren, who grew up in a poor part of Southwest China. He owns a mere 1 percent stake but has veto power over major decisions, and his companywide emails betray his past as an engineer in the People's Liberation Army. A 2017 memo urged employees to adopt 21 distinct "military disciplines," axioms such as: "Company secrets are always sold along with your soul."

Ren has also rigidly enforced the company lore. The official story goes like this: In 1983, he lost his army job, a casualty of nascent privatization efforts, and wound up working at a small, state-owned oil company in the future tech hub of Shenzhen. While he struggled to get by on his government salary, he learned about business and became interested in the idea that China might one day manufacture its own technology equipment. So he was more or less ready in 1987, when Shenzhen, designated a "special economic zone" years earlier as part of Beijing's gradual embrace of private enterprise, began allowing entrepreneurs to start tech companies.

Ren quickly started Huawei with roughly $3,000 in capital from five investors and no obvious plan. "It was not as romantic as you imagined," he recalled in an interview at the annual World Economic Forum in 2015. "Neither was it so wonderful." In its early years, Huawei imported equipment from Hong Kong and sold it on the mainland, but before long Ren's engineers were developing their own crude, fridge-size switches for phone networks, the first items in what would become a massive catalog of computing and networking hardware.

In 2001, once it had become a cheaper alternative to American networking leader Cisco Systems Inc. in its home market, Huawei made landfall in the U.S., setting up 30 employees in a 24,000-square-foot facility in Plano, Texas. By the company's account, it was a humble operation: Workers had trouble with the language and didn't sign up a single American customer for more than three years. Support from the Chinese government, however, allowed it to spend heavily on R&D (including developing its own mobile chips) and to undercut competitors. "It was lower interest rates, deferred payments, don't pay anything now," recalls Anthony Lacavera, the CEO of Canadian wireless carrier Wind Mobile, which bought Huawei gear in 2009. "It felt like a retail promotion."

Who Can Compete With a National Champion?
Revenue, 2017



*COMPANY FORECAST; DATA COMPILED BY BLOOMBERG

Lacavera, like many customers, initially saw Huawei as a lower-end supplier. His impression changed partway through the negotiating process, when he visited its jumbo R&D lab in Shanghai's Pudong district. Sales reps led Lacavera through a conventional product presentation, but the real showstopper was the office tour. "It was rows of desks as far as you could see," he says. "It was a scale that I'd never seen before. They were there to compete." As China has grown into the world's largest semiconductor market, Huawei has grown along with it. Unlike most rivals, the company makes its own chips, cutting out Qualcomm.

Huawei's is one of the great success stories of modern China, but the tale can feel strangely incomplete. While Ren's official biography notes that in 1982 he attended the Chinese Communist Party's National Congress, the twice-a-decade meeting of the country's ruling elite, that honor seems hard to square with the fact that he was laid off a year later. A scathing Obama-era congressional investigation, prompted by Huawei's failed attempts to acquire American tech companies, alleged that Ren might have been a high-ranking Chinese spymaster and indeed may still be. The House report also included claims that Huawei's chairwoman, Sun Yafang, had worked for the Ministry of State Security. Huawei denies these allegations.

The company has also been repeatedly accused of more corporate-variety espionage. In 2003, Cisco sued Huawei, saying it had discovered its own source code, bugs and all, inside Huawei software. The Chinese company eventually conceded that a small portion of its router software had been copied from Cisco, but said the act had been inadvertent. In the end, the companies settled, with Cisco dropping its suit and Huawei tweaking its products.

In 2009, when Canadian networking giant Nortel declared bankruptcy, employees blamed a hack that they traced to China, one that for almost a decade had granted the attackers access to the CEO's emails and other company files. China denied any involvement, but Brian Shields, the security engineer who first noticed the hack, told the CBC that Huawei had been the intended beneficiary. "How can you survive when you have a competitor basically right there, knowing all your moves?" he asked.

Most U.S. allies still allow Huawei products into their wireless networks but scrutinize them for possible security vulnerabilities. In 2010, as part of a compromise with the U.K., Huawei opened what it calls its Cyber Security Evaluation Centre in Banbury, in Southern England. The office, more commonly known as the Cell, is staffed by Huawei employees but supervised by British intelligence officers, who examine the company's code for possible backdoors. The local officers have reported no security flaws, and Huawei has traded on that record to expand its operations throughout Western Europe.

The problem with the Cell, at least from the U.S. point of view, is that it's really hard to find a security hole unless you know exactly where to find it. A modern wireless switch might have millions of lines of code, and things can slip through in preproduction or be added on the factory floor or in a routine update. Hardware vulnerabilities, like the ones revealed in Intel chips earlier this year after more than a decade, can be almost impossible to anticipate or spot. In a nightmare scenario, a backdoor could be hard-coded into the silicon on a Huawei chip, then activated remotely, potentially opening with a few keystrokes the contents of an entire network to the Chinese military.

With a market share of about 11 percent, Huawei is the world's No. 3 smartphone maker, behind Samsung and Apple

One reason American policymakers are so mindful of this sort of scenario is that U.S. intelligence agencies have routinely exploited domestic companies for exactly the same purpose. AT&T so freely aided National Security Agency eavesdropping that the agency praised it for an "extreme willingness to help" in a document leaked by former contractor Edward Snowden and published by the *New York Times*. Suspicions of Huawei's ties to the Chinese government appear in the leaked Snowden files, but so do frustrations that Huawei encryption was too good for U.S. spies to crack. "The irony," a Huawei executive said at the time, "is that exactly what they are doing to us is what they have always charged that the Chinese are doing through us."

Silicon Valley's roots, like those of the internet itself, lie in technologies developed by or for the Pentagon. So China's blackout of Google and its temporary removal of Apple from a list of approved government suppliers make a certain amount of sense. A reckoning has been a long time coming, says James Lewis, a former U.S. State Department cybersecurity expert now affiliated with the Center for Strategic & International Studies, a Washington think tank. "China is deeply worried about this, and they have been for more than a decade," he says. "Their solution was, 'We'll build our own national champions.' That's kind of the genesis of Huawei."

Yet if the U.S. and China continue to escalate the stonewalling of one another's tech companies, they could slow the progress of innovation worldwide. Lewis thinks the U.S. has three options, none of them particularly good. Two are political suicide in America: Throwing vast sums of public money behind national champions to battle China's or subsidizing the only non-Chinese companies that can compete for big equipment contracts—Sweden's Ericsson AB and Finland's Nokia.

The third option is less realistic. Government researchers have been working for at least 15 years on a kind of unbreakable encryption meant to secure hardware that can't otherwise be trusted. It's not clear that's even possible. "I saw one of the people involved in the last couple of weeks, and I said, how's that going?" Lewis says. "They haven't been able to make it work." B

—*With Yuan Gao and Alistair Barr*

MATTHEW LLOYD/AFP/GETTY IMAGES