The company that spooked the world

The success of China's telecoms-equipment behemoth makes spies and politicians elsewhere nervous

Banbury, a little English town best known for a walk-on part in a nursery rhyme and as the eponymous origin of a fruitcake, is an unlikely fulcrum for the balance of power in the world of telecoms. But the "Cyber Security Evaluation Centre" set up there by Huawei, a Chinese telecoms giant, in 2010 marks a new way of persuading purchasers, and the British government, that equipment from the manufacturer that runs it can be trusted. It operates in close co-operation with GCHQ, Britain's signals-intelligence agency, located conveniently just over the Cotswolds in Cheltenham. Its security-cleared staff, some of whom used to work for GCHQ, are responsible for making sure that the networking equipment and software that the Chinese firm wishes to sell to British telecoms companies are reliable, will only do what customers want them to do and cannot be exploited by cybercriminals or foreign spies—including Chinese ones.

Over the past ten years or so, Chinese telecoms firms such as Huawei and ZTE, another telecoms-equipment provider, have expanded from their vast home market to become global players. This is a worry not just for the rich-world incumbents under threat but also for those responsible for the integrity of critical infrastructure such as phone systems. They fear that the companies' networking gear and software could be used by China's spooks to eavesdrop on sensitive communications, or that it might contain "kill switches" which would allow China to disable the systems involved in the event of a conflict. "I think it's ridiculous to allow a Chinese company with connections to the Chinese government and the People's Liberation Army (PLA) to have access to a network," says Dmitri Alperovitch of CrowdStrike, a web-security outfit.

Several big Chinese firms, including ZTE and China Mobile, a giant mobile operator, have attracted scrutiny. But thanks to its size and its international reach it is Huawei that gets most attention. This July the firm's revenues outstripped those of Ericsson, for some time the world's largest supplier of telecoms equipment; Huawei clocked up 103 billion yuan ($16 billion) in the first half of 2012 (see chart 1) compared with the Swedish firm's SKr106 billion ($15.5 billion). Because Huawei's sales as one of the world's ten largest mobile-phone manufacturers (a business Ericsson has left) account for about a quarter of that income, Ericsson is still the biggest supplier of network infrastructure. But probably not for long.

The question of whether to trust this new giant divides the world. In Africa Huawei is everywhere, and welcome almost everywhere; in India it has found itself under attack by government and media as both a security threat and an unfair competitor. In Canada and New Zealand it has won meaty contracts for work on big new networks; in Australia in March the government blocked it from taking part in a new national broadband system.

The doubts run deepest in America. Huawei has worked on networks for a number of smallish mobile operators there, but its repeated attempts to buy American tech firms have been scuppered by official opposition. The Intelligence Committee of the House of Representatives is taking an interest in both Huawei and ZTE. Last year the Committee on Foreign Investment in the United States, chaired by the treasury secretary, Timothy Geithner, opposed Huawei's purchase of assets from 3Leaf, a server-maker that had gone bankrupt, on the basis of unspecified security concerns. Huawei abandoned the attempt.

Even in America, though, opinion is divided. One former member of the joint chiefs of staff dismisses the fears about Huawei as China-bashing; another says, "We'd be crazy to let Huawei on our networks, just crazy."

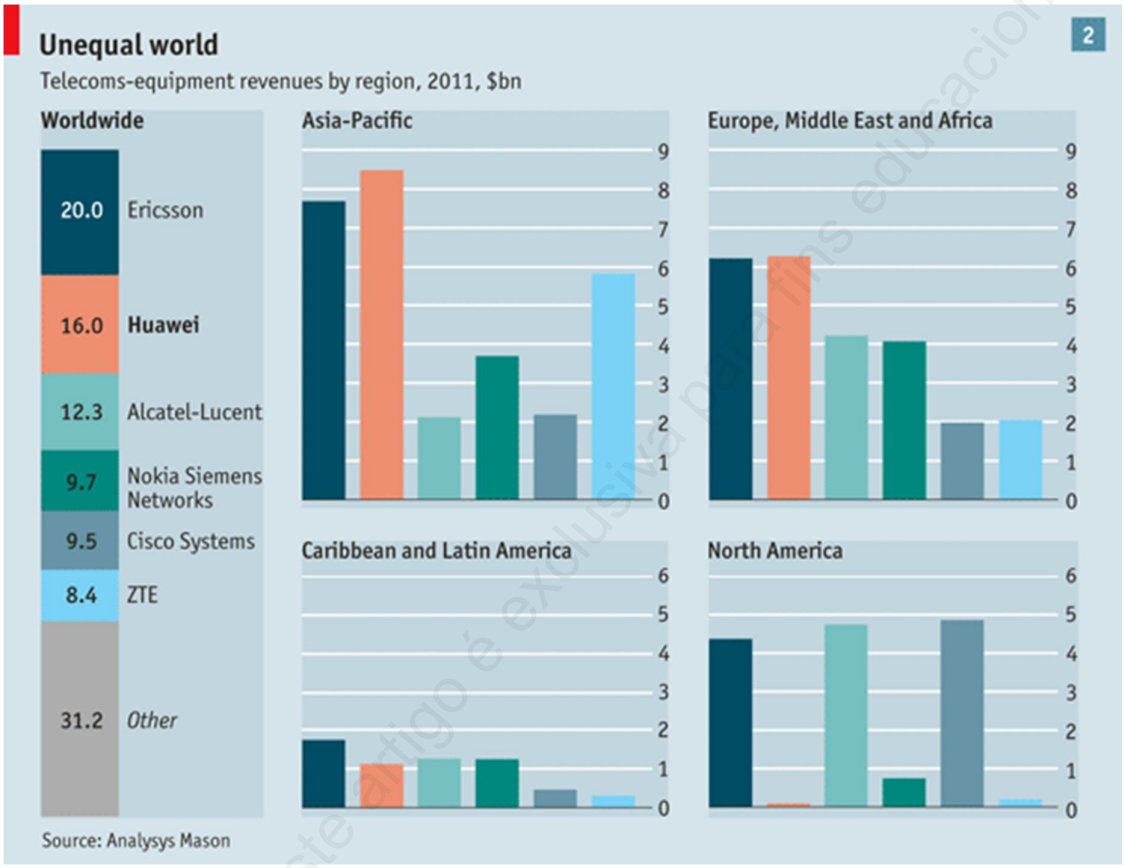
A Maoist approach to markets

The giant causing all this angst rose from humble roots. Although the company is not as forthcoming as it might be about the background of Ren Zhengfei, its founder, he is not the princeling scion of an elite family. He attended the Chongqing University of Civil Engineering and Architecture in the 1960s and served in the PLA's engineering corps, reportedly in its information-technology research unit. Huawei says he rose to the position of deputy director, but did not hold military rank. After cuts to the armed forces he left the army in 1983 and moved to Shenzhen, a boomtown near Hong Kong.

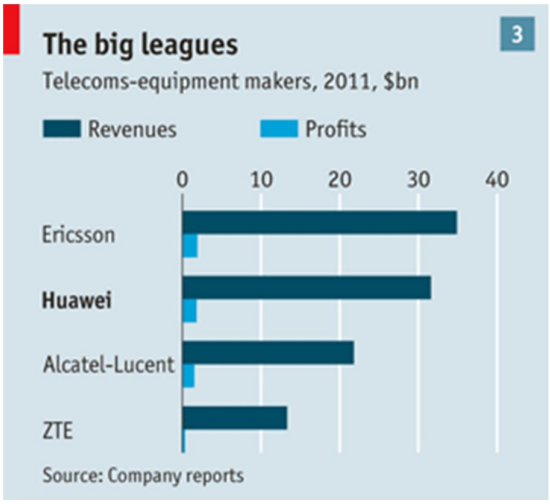
Mr Ren set up Huawei in 1987 with just 21,000 yuan, a bit more than $5,000 at the time. It mostly sold telephone-exchange equipment imported from Hong Kong. Five difficult years later, the firm made its first breakthrough with its C&C08 digital telephone switch, which had a

greater capacity than any other on the Chinese market. That positioned Huawei perfectly to ride the wave of China's telecoms-infrastructure boom of the 1990s.

Excluded from China's lucrative coastal markets, which were reserved for the better-connected, Mr Ren put to new purpose Mao's strategy of using the countryside "to encircle and finally to capture the cities." He encouraged his salesmen to undercut competitors in markets deemed minor. Huawei went on to use a similar approach overseas, initially targeting peripheral markets. It priced competitively: in Africa it undercut Ericsson and Nokia by 5% to 15%, according to a report by Wharton Business School. It also showed tenacity and daring. Its engineers soldiered on through civil wars and natural disasters; by 2006 sales in Africa were over $2 billion.



Huawei's customers now serve several billion people in over 140 countries (see chart 2). Its revenues in 2011 topped $32 billion, up nearly 12% on the previous year and ten times what they were a decade previously. It is involved in over half the rollouts of super-fast 4G mobile networks so far announced in Europe. In the past few years, the firm has consistently been one of the world's leading generators of intellectual property, and has filed for some 47,000 patents. It led the way on "dongles" for connecting laptops to phone systems, and on software that allowed operators to run different wireless standards cheaply and flexibly. "The company's equipment is now world-class," says Jim Lewis of the Centre for Strategic and International Studies (CSIS), an American think-tank, who has studied Huawei's rise.



It has over 140,000 employees, and says 44% are in R&D, many of them in its shiny corporate campus in Shenzhen. The site boasts a buzzing "Tower of 10,000 engineers", meeting rooms designed as Zen gardens and an espresso bar with first-class baristas. Just across the road is the massive factory complex where Foxconn makes Apple's iPhones and iPads—and some of Huawei's equipment, too. Though it could manufacture its own kit in-house, Huawei, like the Western giants with which it now competes (see chart 3) outsources much of its manufacturing to specialists. It sees itself as the new face of Chinese technology: an innovator, a sales force and a global brand.

Back-door imbroglios

Critics are convinced that there is more to Huawei's rise than strategy, guts and Mr Ren's devotion to innovation. They think it has stolen vast amounts of intellectual property and that it has been heavily subsidised in its expansion by the Chinese government, eager to use it as a Trojan horse with which to infiltrate itself into more and more foreign networks. Huawei rejects all these allegations.

John Chambers, the boss of Cisco, an American supplier of network equipment, recently claimed that Huawei does not always "play by the rules" on intellectual property; many in America are convinced that Huawei stole the design of one of its early products from Cisco, though the Chinese company hotly denies this. Cisco settled a lawsuit it had brought against Huawei in 2004 in a way that both sides spun as vindication.

Then there is the question of whether China's government bankrolled Huawei's undercutting of its rivals. In 2011 Huawei acknowledged that its customers did benefit from access to $30 billion in potential "export financing", though apparently only a fraction of that has been used. Pressed for details, the firm says that "in 2011, the financial support that Huawei provided to customers came to 5.86% of total contract sales," a figure not specified.

At the end of June, Chinese and European officials met in a bid to avert a trade war over subsidies. Avoiding a formal confrontation may suit all concerned. Pierre Ferragu of Sanford C. Bernstein, an investment bank, reckons that Huawei's rivals have used the same sort of inducements. He adds that everyone will do it less in the future, because customers who can buy only if subsidised are poor prospects for future earnings: "You can't up-sell higher-margin follow-on work to them later because they can't afford it."

This leaves the most troubling criticism: that the firm might be a creature of China's security services. Mr Ren's past in the PLA fuels such suspicions, as does a reasonable perception that privately held Chinese companies are often in cahoots with the powers that be. The firm's dealings with unsavoury regimes such as Iran, where its salesmen boasted that their equipment makes it easier to spy on potential troublemakers, are taken as supporting this view.

Such dealings are not unknown in the world of telecoms. An investigation by *Wired* magazine found Cisco's salesmen making similar claims in efforts to win contracts with a repressive government—ironically, that of China. And American telecoms-equipment companies have a degree of cosiness with America's national-security apparatus; the former head of the National Security Agency, America's GCHQ, sits on the board of Motorola Solutions, a telecoms-equipment provider. But such symmetry hardly means there is no need to worry about Huawei. American fears may be based on the fact that its leaders know from experience that telecoms companies can be helpful espionage assets. American officials have in the past demanded the installation of "back doors" in some exports, through which the devices can be accessed on the quiet.

Huawei clearly might do such things; the question is whether it does. Evidence was presented at DefCon, a big hackers' convention held in July, of security vulnerabilities in a couple of Huawei's smaller routers. But such flaws are common. Several years ago, the American government gave warning of similar vulnerabilities found in kit made by Cisco and other Western firms. Years of intense scrutiny by experts have not produced conclusive public evidence of deliberate skulduggery, as opposed to mistakes, in Huawei's wares. BT, a British telecoms company that buys products vetted in Banbury, says it has not had any security issues with them (though it rechecks everything itself, just to be sure).

Huawei seems open to such scrutiny, at Banbury and elsewhere. "Believe no one and check everything," is the right attitude for dealing with Huawei or anyone else, says John Suffolk, now Huawei's global cyber-security officer, previously the British government's chief information officer. Huawei equipment for America and Canada, he says, is independently vetted by Electronic Warfare Associates, an American defence contractor well supplied with security clearances and experience.

But absence of evidence is not evidence of absence; flaws in telecoms gear, whether put there deliberately or accidentally, are hard to find. "Most security problems we encounter are due to very subtle bugs in code that even the original programmers may miss," says Steven Bellovin of Columbia University. "Identifying back doors in hardware is also a really, really hard challenge." So doubts remain.

The charmless offensive

Part of Huawei's problem is that it gets lumped in with its rival, ZTE. America's FBI has investigated whether that firm illegally sold American technology to Iran and then lied about the matter, something Huawei is not accused of. Back doors that might have allowed remote access appear to have been found on some ZTE mobile-phone handsets. Huawei itself is suing ZTE for stealing intellectual property (perhaps with the caution of the poacher-turned-gamekeeper, it takes piracy very seriously now it is a technology leader).

Huawei is also in part the author of its own misfortune. The China head of a Western management consultancy insists that Huawei is not controlled by the PLA, and deserves to be treated as the private-sector firm that it is. But because of the secretive way Mr Ren has run it, it is hard for others to be so sure. Belatedly, and under pressure from outsiders, the firm is trying to modernise and open up, embarking on what it thinks is a charm offensive. It has hired lobbyists and public-relations consultants, and assembled well-paid advisory bodies of the great and the good in important countries. It is even publishing something resembling an annual report.

This has not yet paid off. The firm talks of corporate-governance reforms, for example, but remains murky to the core. Its handling of its leadership succession is revealing. Mr Ren reportedly wanted his son to take over from him, but in April he was forced instead to agree that three colleagues should share the chief-executive job with him on a rotating basis. The chairman of a big Western firm with intimate knowledge of Huawei quips, "it looks like how the Communist Party frequently rotates bosses among state-owned industries." The congressional committee has asked the company to clarify its links with the Chinese Communist Party—

including the role of an internal “party committee”. If Huawei wants to win America’s trust, argues Claude Barfield of the American Enterprise Institute, a conservative think-tank, it should list on an American stock exchange and embrace international guidelines on state aid and trade.

Moving towards openness would leave Huawei better positioned to work on a new set of international rules and guidelines for sourcing telecoms networking gear and code—something that many industry insiders think is sorely needed. In a paper published last year two Microsoft executives, Scott Charney and Eric Werner, called for governments and companies to come up with much better standards for supply chains, to mitigate all sorts of risks including some that pertain to security.

Mr Charney acknowledges that governments will not find it easy to trust stuff designed and deployed by firms from countries considered adversaries. But knee-jerk nationalism could have dire consequences. Simply banning stuff on the basis of a firm’s nationality “could blow global trade away and balkanise the world of IT,” he says.

Ross Anderson, a professor of security engineering at Cambridge University, points out that banning equipment from Chinese firms would give a false sense of security: equipment from everyone else has Chinese components anyway. Bryan Wang of Forrester, a consultancy, notes that Alcatel-Lucent makes nearly its full range of products in China, except for some high-end routers, and that Nokia Siemens Networks makes its mobile base stations and its switches there.

Greater international co-operation in another area could help to defuse the tension. One reason that Huawei and other Chinese firms are being scrutinised so closely is that study after study has shown that many of the cyber-attacks mounted on Western companies and government departments originate in China. If China’s government were to commit itself to identifying the perpetrators, and to confound sceptics by actually shutting hacking operations down, American attitudes towards firms such as Huawei might improve.

And it might be in China’s interests in other ways. The Chinese are as worried about digital Trojan horses as the Americans are. As a statement that came out of a recent meeting convened by CSIS, the American think-tank, and the China Institutes of Contemporary International Relations, an influential Chinese counterpart, put it: “Both [countries] believe that the other will seek to exploit the supply chain to introduce vulnerabilities into networks and infrastructures.”

“We need to drain the swamp,” says Mr Anderson. If China wants Huawei to become truly global it should take the lead on the clean-up effort. If it does so, America would have an incentive to welcome Huawei—and no more reason to vilify it.

Fonte: The Economist, London, v. 404, n. 8796, p. 19-23, 4-10 Aug. 2012.