April 5, 2019

The US Case Against Huawei: Where's the Beef?

Is there a high-technology competitor that prompts as many questions and raises as many suspicions as Huawei Technologies Co. Ltd.? We doubt it.

But much of what is said and believed about China's globally competitive telecoms company is rooted in misperceptions and inflated assessments of risk, in our view.

As US–China trade frictions persist, and as Washington presses Europe to avoid Huawei products on national security grounds, it's time to clear the fog surrounding a leader in the fast-emerging market for 5G telecommunications networks. The Huawei controversy raises questions of free trade, market access, and reciprocity that can't be ignored or deferred. Are the Trump administration's aggressive moves against Huawei in part an effort to keep China out of the global 5G competition? A lot of prominent technologists think so. If that's even partially accurate it merits caution, given that the Administration is pressing its global case for an America First trade strategy on the principle of reciprocity.

Following is a look at the more common misconceptions propagated about Huawei, what it is, and what it does and doesn't do:

Huawei is a tool of the Chinese government. The company was founded in 1987 by Ren Zhengfei, a technology engineer who reportedly received his early IT training in the People's Liberation Army. Huawei is private and employee-owned, with headquarters in Shenzhen, the industrial city in Guangdong Province just opposite Hong Kong. To date, there is no evidence that the government, the ruling Chinese Communist Party, or the People's Liberation Army has ever sought or gained access to Huawei's telecom networks.

Beijing has a "back door" into Huawei's systems; the company was complicit in creating it. No cyber-security inspection of Huawei's networks has ever revealed any evidence of this charge. The only known "back door" into Huawei systems was created by the National Security Agency, which hacked its Shenzhen servers at some point between 2010 and 2012. The breach was revealed in the documents Edward Snowden made public in mid–2013. "On this point," a former NSA director tells us, "Washington is simply accusing Beijing of doing what we've already done."

Huawei is obligated by law to turn over data to the Chinese government. US officials and members of Congress made this allegation to justify a ban on federal agencies' purchases of Huawei equipment imposed earlier this year. Washington's China hawks are in full exaggeration mode, in our view. China's laws governing data

access are little different from those of numerous other countries, including the US and Australia. The latter passed such legislation last December. In the US, the government can obtain a court order requiring access to telecoms data. The NSA's extra-legal PRISM data-collection program, as also revealed in the Snowden documents, passed into law in January 2018.

Huawei is stealing its way to success via thefts of intellectual property and trade secrets. Charges of IP theft are not uncommon in high-tech industries. Those brought against Huawei have been few, modest in magnitude, and appear to reflect individual misjudgments, not corporate policy. "These kinds of cases are often at least partially business tactics," an experienced technologist tells us. "They can slow defendants' development processes and damage reputations." In our view, Huawei's competitive edge derives not from IP pilfering but from its patent portfolio, which grows like a weed: From 1,500 patents in 2012, Huawei owned 11,000 at end–2018; all but 300 of these were on products or processes the company developed.

Huawei is a Trojan horse intended to infiltrate the West and will spy, eavesdrop, sabotage networks, and crash systems when Beijing orders it to do so. This argument doesn't stand up to the simplest logic. Any such move on Huawei's part would amount to corporate suicide, given no one would ever again trust it. The only plausible circumstance in which Huawei would take malign action against another country's networks would be during an openly declared war.

In our view, these and various other misperceptions about Huawei reflect the inappropriate risk-assessment model the US uses to gauge the potential for security breaches via Huawei's networks and products. It ignores past or present practices or events and looks solely at capabilities assuming Huawei has become party to a hostile nation.

"None of this is about what Huawei has done," an American source in Beijing points out. "It's about what it could do—the future, not the past." We question the fairness of this standard, especially given Huawei's leading position in emerging 5G technologies and the Trump administration's running battle to gain greater access to Chinese markets.

* *

Last week was especially eventful for China's high-tech champion. On Thursday Britain's cyber-security oversight panel issued its annual report on Huawei, saying it doubts the company can remedy flaws in its development processes that leave its software products vulnerable to security risks. The following day, Huawei reported a 25% increase in its 2018 net profit, to a record $8.8 billion. It forecast double-digit growth in 2019 revenues, which topped $100 billion last year for the first time.

This is Huawei: While Western intelligence agencies and cyber-security officials raise a plethora of doubts about the company, customers count it a leading high-tech innovator, and on price it can beat competitors by 50% to 70%. User satisfaction surveys rank Huawei products well above rivals such as Samsung and Microsoft. "In the 5G field," our source in Beijing tells us, "it would be hard to build a system without Huawei products."

Washington has made Huawei a defining issue in its broader trade offensive against China, to the extent of charging CFO Meng Wanzhou with financial fraud in an alleged attempt to circumvent U.S. sanctions against Iran. But Europe is also a key front in U.S. efforts to keep Huawei out of the 5G market. Trump administration trade officials and diplomats continue a vigorous campaign to stop Europeans from allowing Huawei a role in their 5G development plans. In a letter made public last month, for instance, Richard Grenell, Trump's outspoken ambassador to Berlin, warned that the US will limit its intelligence-sharing with Germany if it gives Huawei any part of its 5G program.

Europe has so far proven resistant to Washington's entreaties. It appears to recognize that weaknesses and "bugs" in Huawei software products are not much different from those in the output of many competitors, probably most. The challenge is to identify vulnerabilities and manage threats. Even the British report on Huawei made public last week stopped well short of Washington's demand for a ban on Huawei 5G products. For its part, Huawei committed $2 billion last December to repair flaws in its software development processes that are causing weaknesses in its products.

In proposals made public last week, the E.C. urged member states to conduct their own risk assessments of Huawei with a view to combining these in an E.U.–wide strategy to identify and manage any potential for security breaches. This is a sound approach, in our view. But as our Beijing source notes, "The US position is not to have that conversation."

This may finally be changing.

A Washington Post report published earlier this week quoted national security officials saying the U.S. is now "planning for a future in which Huawei will have a major share of the advanced global telecommunications market, and has begun to think about how to thwart potential espionage and disruptive cyberattacks enabled by interconnected networks." If this proves out, we endorse the government's belated acceptance of Huawei's inevitable place among the top 5G competitors.

The Europeans are well aware of another risk: Cutting Huawei out of their 5G programs would cause development delays that would put them at a competitive disadvantage and be "detrimental to Europe's GDP growth," as Simon Segars, CEO at Arm, the

British chip manufacturer, put it at a conference in late February. As if to underscore Segars's point, South Korea's three mobile carriers, including market leader SK Telecom, rushed out their first 5G offerings ahead of schedule this week.

* * *

Bretton Woods Research

Domestic Reports, Global Reports, and Supply-Side Portfolio (collectively referred to hereafter as "Bretton Woods Research"), is published as an investment newsletter for subscribers, and it includes opinions as to buying, selling and holding various securities. However, the publishers of Bretton Woods Research are not broker/dealers or investment advisers, and they do not provide investment advice or recommendations directed to any particular subscriber or in view of the particular circumstances of any particular person. The information provided by Bretton Woods Research is obtained from sources believed to be reliable but is not guaranteed as to accuracy or completeness. Subscribers to Bretton Woods Research or any other persons who buy, sell or hold securities should do so with caution and consult with a broker or investment adviser before doing so. Bretton Woods Research does NOT receive compensation from any of the companies featured in our newsletters.

The publishers, owner, agents, and employees of Bretton Woods Research, LLC, may own, buy or sell the exchange traded funds and other securities or financial products discussed in Domestic Reports, Global Reports, and Supply-Side Portfolio ("Bretton Woods Research"). Bretton Woods Research and its publishers, owners and agents, are not liable for any losses or damages, monetary or otherwise, that result from the content of Bretton Woods Research. Disclosure: The publisher and owner of Bretton Woods Research, LLC, may own, buy or sell the exchange traded funds currently listed in Supply-Side Portfolio's current list of recommendations and may purchase or sell some of the shares of the companies held by these ETFs. Bretton Woods Research and its publishers, owners and agents, are not liable for any losses or damages, monetary or otherwise, that result from the content of Bretton Woods Research.

Past results are not necessarily indicative of future performance. Performance figures are based on actual recommendations made by Bretton Woods Research. Due to the time critical nature of stock trading, brokerage fees, and the activity of other subscribers, Bretton Woods Research cannot guarantee that subscribers will mirror the performance stated on our track records or promotions. Performance numbers shown are based on trades subscribers could enter. The trade results posted for Bretton Woods Research are hypothetical but reflect changes and positions with the last available prices. Investors may receive greater or lesser returns based on their trading experience and market price fluctuations.