HIGH SCHOOL EDITION
Journal of Student Research
Volume 11 Issue 4 (2022)

# Huawei: Caught in the Whirlwind of the U.S. & China High-Tech War

Qixin Zhang[1] and Stacy von Winckelmann[1#]

[1]St. Margaret's Episcopal School, USA
[#]Advisor

## ABSTRACT

Founded in Shenzhen, China in 1987, Huawei was Ren Zhengfei's startup that first served as a rural sales agent for network-based corporations. Now, Huawei identifies as a leader in the information and communications technology (ICT) sector that strives to create an increasingly connected, digitalized, and intelligent environment for all. Three core components of Huawei's early success are open innovation, tactful international strategy, and customer-centricity. Huawei's heavy investments in open innovation and R&D allow it to achieve extraordinary industry breakthroughs. By debuting in developing regions such as Africa first, Huawei builds the necessary skills needed to tackle developed regions such as Europe. Additionally, Huawei continuously adapts through customer feedback, thus providing superb customer service. Because of the escalating tensions between China and the United States since the Trump administration, the U.S. sees Huawei as part of the Chinese government's agenda to extend its influence over the digital world. As such, the U.S. declared Huawei a national security hazard because of its potential to be used for espionage and sabotage. It also embarked on a global campaign to strongly advise its European allies to refrain from using Huawei's services and products. Though European countries have responded on a continuum from avoidance to compliance, all took measures to strengthen their telecom policies explicitly or implicitly. In response to the accusations, Huawei has remained firm in denying ties to the state Communist Party, promising never to disclose private customer data to outside parties for any reason.

## Introduction

Founded in 1987 by 44-year-old Ren Zhengfei in his small apartment in Shenzhen, Huawei Technologies was among many startups seeking a foothold amidst China's transition from a state socialist economy to a more market-based and globally integrated economy. Unlike most other entrepreneurial ventures at the time, Huawei grew to be the world's largest telecommunications hardware manufacturer (Chang et al., 2017). It is also the second best-selling smartphone seller after Samsung, surpassing Apple in Quarter 1 of 2019 (Eadicicco, 2019).

With over 195,000 employees and activities in over 170 countries, Huawei is committed to building an intelligent and fully interconnected world (Huawei, 2021). But *how* did Huawei carve its own path? When Huawei was born on the cusp of 1990, the Chinese telecom equipment market had been dominated by foreign powers, including Sweden's Ericsson and France's Alcatel. Moreover, Huawei had limited capital, obsolete technologies, and no financial support from the state government (Wen, 2020). Between fierce domestic competition, established multinational corporations, and meager available resources, Huawei was in grave danger of being marginalized.

### Open Innovation

Huawei's success depended on three major factors: heavy investments in open innovation and R&D, laser focus on unexplored markets and opportunities, and its philosophy of prioritizing the customers.

Huawei utilized open innovation through collaboration across organizations on the management of knowledge flows and the development of innovative processes (Yan & Huang, 2022). Though Ren Zhengfei was well aware of the high risks associated with supporting R&D because of how fast the pace of technological advancements was, he still made the executive decision to invest 100 million yuan, the equivalent of approximately $12 million, to fund the development of Huawei's own set of technologies when the company was still in its infancy (Luo et al., 2011). This stands in stark contrast to most other Chinese companies' strategy of forming joint ventures with foreign enterprises to facilitate knowledge transfer (Yan & Huang, 2022).

Huawei started collaborating with top universities in mainland China as early as 1999 through the Huawei Science and Technology Fund. In 2004, Huawei outsourced industry projects to the Hong Kong Institute of Science and Technology (HKUST), its first of many research partners. A decade later, the Huawei Innovation Research Program (HIRP), a systemic way of managing research projects from initiation to completion, was launched (Yan & Huang, 2022).

In accordance with Huawei's core belief that the best means of making technological progress in the digital sphere is to focus on open innovation, 48% of all Huawei employees are classified in the research and development department. In addition, the global telecom giant has reinvested over 10% of its total sales revenue annually into R&D, the intensive spending unheard of in other companies (Zhang, 2013). Nevertheless, Huawei has consistently reaped the fruits of its labor in this arena. It consolidates external technologies and builds its own set of internal networks through cross-disciplinary knowledge flow between its 50 R&D and joint innovation research centers (Huawei) all over the world (Chang et al., 2011). Through R&D, Huawei has been able to maximize production efficiency and consumer satisfaction. In Huawei's newest 2021 Annual Report, Huawei states that it is continuing to fund research in cloud computing, communications, and AI, among other fields. They also published their vision for the next generation of wireless cellular networks–6G–proving, once again, that they are at the forefront of the newest and most innovative technological developments.

## From Developing to Developed Countries

In addition to a relentless pursuit of open innovation, Huawei's entrepreneurial success also depended on its ability to integrate wielding resources domestically with overseas exploration and breakthroughs. The company applied its homegrown approach of "encircling cities from rural areas" internationally with auspicious results (Zhang, 2013). It first expanded to emerging markets such as Russia, Africa, and Latin America, then to developed countries in Europe and the U.S. (Luo et al., 2011). By starting in developing nations whose technical requirements and thresholds are relatively low, Huawei has been able to gradually–and with heavy R&D investments–build technology products and services up to the standard demanded by more advanced countries. Huawei's case in West Africa exemplifies this strategic plan.

In 1999, Huawei founded Huawei Technologies Company Nigeria Limited with headquarters in Lagos (Agbebi, 2018). The success of Huawei in the African telecommunications sector can be attributed to its capacity to provide inexpensive technologies that are affordable and accessible to all. In this region, Huawei has played an integral role in upgrading the information and communications technology (ICT) infrastructure to enhance digital connectivity as well as in contributing to human capital development (HCD) to spur humanitarian and economic growth (Agbebi, 2018). For over 20 years, Huawei has benefitted from its operations in the African sector by making significant breakthroughs that equipped it with the might to venture into Western markets (Zhang, 2013).

## Customer-centric Focus

Huawei's sole purpose of existence is to serve its customers, and customer-centricity is entrenched in its corporate culture (Huawei, 2021). Deputy chairman Xu Zhijun speculated that one of the main reasons Huawei was able to not only catch up to but also surpass global competitors such as Ericsson and Motorola is that they are significantly more

people-oriented and comparatively less profit-driven (Tian & Wu, 2015). Huawei strives to provide superb customer service by proactively adapting through customer feedback. Feedback is collected via both direct and indirect means. Direct means include open-ended, face-to-face interviews. This allows Huawei researchers to gain insight into the perspectives of customers from target markets. The information gained includes commentaries on Huawei products, interpretations of the current business environment, and suggestions for improvements. Indirect means include methodically examining sales data and sales call reports (Fu et al., 2018).

## Huawei in the U.S.

### The Beginning: 2001 – 2012

Since establishing its first offices in the U.S. in 2001, Huawei has been met with obstacle after obstacle in the telecom market. In 2003, it signed an opportunistic contract with 3Com, a U.S.-based anti-hacking software provider. In the same year, it was sued by Cisco based on intellectual property theft claims. After 20 months of back-and-forth negotiations, the charges were dropped (Liu, 2021). The case achieved the opposite of what it was meant to do: instead of taking Huawei down a notch as Cisco intended, it actually helped Huawei garner the attention it needed to kick off its business journey in the U.S. Indeed, Huawei secured its presence as an emerging telecom competitor that could challenge established giants such as Cisco in Americans' eyes. While public scrutiny increased, so did opportunities to expand and grow.

Huawei's overseas revenue exceeded its domestic revenue for the first time in 2006, solidifying it as a truly global enterprise. In 2008, Huawei's deal with 3Com collapsed after it became clear that lawmakers in Washington D.C. were set on blocking the transaction out of perceived security concerns. The Chinese government accused the U.S. of its inability to deliberate commercial matters independently of political interests (Tang, 2020). In an effort to clear its name, Huawei invited the U.S. government to conduct a thorough investigation of the company in 2011. In October 2012, the House Permanent Select Committee on Intelligence released a formal report on its results, stating that though no wrongdoing could be proved, a full and fair investigation could not be carried out. Therefore, Huawei's provision of technology equipment to the U.S. could jeopardize its critical infrastructure (Rogers & Ruppersberger, 2012). The leap of logic from no wrongdoing found to labeling Huawei as a national security threat could be seen as far-fetched. The antagonist undertone throughout the report serves as a possible reflection of the U.S.' attempt to ward off China-affiliated influences from taking root in the state as part of a broader anti-China agenda.

### Since the Sino-U.S. Trade Wars in 2018

When the Trump administration took over the White House in 2016, they adopted a decidedly anti-China stance. In July, the U.S. imposed tariffs and quotas against Chinese-imported goods on the grounds that China was responsible for the loss of American manufacturing jobs, initiating what became known as the Sino-U.S. trade wars (Hass & Denmark, 2020). At the same time, questions were raised regarding the hand-in-glove relationship between the Chinese Communist Party and Huawei, especially since Huawei has been designated as a "national champion" who has reaped significant financial benefits and backing from the Chinese government (McLure, 2012). As such, the U.S. accused Huawei's 5G technologies of being capable of acting as spy agents and infiltrators in Western intelligence services, which allegedly aligns with President Xi Jinping's broader, more ambitious plans to assume international cyberspace sovereignty (Friis & Lysne, 2021; Tang, 2020). Consequently, the U.S. banned the use of Huawei and ZTE, another Chinese telecom equipment manufacturer, in 2018. In 2019, Huawei was put on the "Entities List," which disallowed it from buying U.S.-made products such as chips which were essential to the company's automotive business expansion (Friis & Lysne, 2021).

The latest round of U.S. verdicts on Chinese telecom companies occurred when President Biden signed the Secure Equipment Act of 2021. The bipartisan legislation requires the Federal Communications Committee to no longer review applications for telecom equipment from companies that pose serious national security threats. This ensured that Huawei had no way of entering American communications networks. The impact of all aforementioned developments is this: as of 2020, Huawei's major markets are Europe, the Middle East, Africa, and Latin America. The others–including the U.S.–occupy less than 2.7% of Huawei's annual revenue (Tang, 2020). Further, this percentage point likely decreased in the past two years owing to the passage of the Secure Equipment Act and the deteriorating Sino–U.S. geopolitical ties.

## Huawei In Europe

### Early Developments

Huawei established its first European headquarters in Basingstoke, U.K. in 2001, the same year the company debuted in the U.S. But Europe's response to Huawei differed drastically from that of the U.S. For example, Huawei became one of the main suppliers of network gear–including 3G and 4G networks–to British service providers by 2010. When the U.S. raised security concerns in 2011, Huawei and the U.K. worked together to problem-solve suspected risks associated with U.K.'s critical infrastructure, resulting in improvements in Huawei's product quality and reliability (Liu, 2021). The success of Huawei in Europe is demonstrated by how, as of 2020, over half of Huawei's total 91 5G contracts are in Europe (Tang, 2020). This collaborative approach stands in stark contrast to the U.S.'s forceful attitudes toward Huawei since its entry into the market. While the U.K. was willing to take concrete steps that produced mitigated cybersecurity risks, the U.S. took preemptive measures to prevent the telecom supplier from developing domestically.

### Rising Security Concerns & U.S. Pressures

Unlike previous administrations, then-President Trump and his Secretary of State Mike Pompeo embarked on a global outreach campaign that aimed to ban Huawei technologies from actualizing implementation in regions worldwide. The warning was emphasized for the U.S.'s NATO (North Atlantic Treaty Organization) allies such as Italy, Germany, and the U.K. Perpetuating employment of Huawei telecom networks, the U.S. claims, could jeopardize information and intelligence sharing–and thus undermine the working partnership between their countries (Friis & Lysne, 2021). The underlying threat is clear: any nation that chooses to work with Huawei jeopardizes its alliance with the U.S.

However, researchers at the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) published an authoritative report titled *Huawei, 5G, and China as a Security Threat* in which they concluded that there is no evidence of significant vulnerabilities in Huawei's technology products (Kaska et al., 2019). Therefore, although the U.S. has reiterated that Huawei is a "national concern" purely because of suspected technical loopholes and security weaknesses, speculations could be made that the real agenda stems from a geopolitical basis, that the U.S.' persistent actions to stump Huawei's growth are part of a broader scheme to try and push Chinese 5G network suppliers out of the next phase of ICT development for fear that China will eventually dominate the technology and innovation hub for which the U.S. currently assumes command of. If so, this will not be the first time that the U.S. has leveraged its diplomatic superiority status to steer the structural decisions of its subordinates and impede forces, like Huawei, which it deems threatening to its position at the top of the global communications food chain from growing beyond its control (Tang, 2020).

In response to U.S. pressures, Western allies' responses have varied on a continuum spectrum from resistance and circumvention to absolute compliance. For example, the U.K. initially granted Huawei a role in the non-critical parts of its 5G infrastructure in early 2020. But in an abrupt 180-degree turnaround later in the year, the U.K. reversed

its decision and banned all present and future Huawei products from operating in the state. The officially cited reason was that because Huawei was put on the Entities List, it could no longer import software systems from U.S. suppliers, which significantly reduced the trustworthiness of Huawei's equipment (Friis & Lynse, 2021). However, political pressure from the U.S. likely pulled an equally important weight in the final verdict. The other European country that explicitly banned Huawei was Sweden. In contrast, Germany, France, and many others adopted a more conciliatory approach in the sense that though they refrained from using any direct references, new ICT security laws emphasize stricter control and screening mechanisms in choosing ICT suppliers as their service providers (Friis & Lynse, 2021).

## Huawei's Response

Amidst the nonstop torrent of accusations that have hit Huawei over the past two decades, Huawei has tried to defend its reputation time and again by striving to increase the transparency of its systems and operations. It has allowed government agencies such as the FBI in the U.S. and the National Cyber Security Centre in the U.K. to conduct multiple investigations, and the general ruling has always been that Huawei has the *potential* to interfere with core communications, never that it has found any concrete wrongdoings or even just suspicious activities that warrant further inspection.

An important point to note is that a "full" investigation–one that covers every area of concern–can not be completed simply due to the complex, technical nature of 5G networks. Thus, no matter how exceptionally transparent Huawei becomes, it remains insufficient to erase all doubts of insecurity (Friis & Lysne, 2021). It follows then that there must exist a certain degree of trust and cooperation between the tech vendor and the receiving nation. Unfortunately for Huawei, by default of being born in a non-Western and non-democratic country that also happens to be locked in a global high-tech rivalry with the U.S., its liability of foreignness (LoF) is likely high, and its chances of landing contracts are likely low.

On Huawei's part, its CEO Ren Zhengfei has publicly denied ties between his firm and the Chinese government, including claims that his company receives billions in funding from the state and claims that it shares private user data with the leading Communist Party (Cheslow, 2019). Huawei affirms in its 2021 Annual Report that moving forward, it will embrace transparency to an even higher degree to ensure that all of its stakeholders–governments, partners, researchers, experts, suppliers, and customers–can continue to see who Huawei portrays itself to be.

## Conclusion

The U.S. doubts about the security and reliability of Huawei's technology equipment are valid but to a limited extent. No glaring holes were found in any federal-led investigations, but, at the same time, it is impossible to check every aspect of concern given the complex scope of 5G networks. The White House's main argument is that Huawei serves as a channel through which the Chinese Communist Party Infiltrates Western intelligence services, a claim lacking concrete evidence. The U.S.'s anti-Huawei campaigns make sense when the situation is viewed in the context of the broader China-U.S. rivalry. 5G represents the future of wireless networks. If Huawei, a company with non-Western and non-democratic origins, succeeds in dominating the ICT sphere, the U.S.'s status as the shaping force of global communications systems is potentially jeopardized. In response to U.S. pressures, European nations have made corresponding adjustments to varying degrees of severity. While the U.K.–arguably the U.S.' closest ally–has promised to cut ties with Huawei completely, France, Germany, and others have refrained from name-dropping firms but have taken implicit measures to tighten telecom vendor control.

All in all, Huawei has suffered significant losses in brand image, revenue generation, and contract landings as a result of concerns surrounding its products' technical and security reliability. While Huawei perhaps could have taken measures to increase the transparency of its operations sooner and to a greater extent, its liability of foreignness

factor as China's "national champion" put it at an inherent disadvantage compared to its Western counterparts. This is the unfortunate and frustrating reality that Huawei will always have to confront.

It is essential to acknowledge that choosing 5G network vendors is a hefty task with long-term implications. Reversing such a decision is expensive and time-consuming. In addition, it cannot be denied that this is as much a technological choice as it is a strategic one (Kaska et al., 2019). Looking forward, Western countries should–instead of taking preemptive measures to block Huawei–give it the chance to prove itself as a capable and trustworthy partner.

## References

Agbebi, M. (2018). China in Africa's telecom sector: Opportunities for human capital development? A case of Huawei in Nigeria. *Human Resource Development International*, *21*(5). 532-551. https://doi.org/10.1080/13678868.2018.1512232

Chang, L.-C., Ho, W.-L., Tsai, S.-B., Chen, Q., & Wu, C.-C. (2017). Dynamic organizational learning: A narrative inquiry into the story of Huawei in China. *Asia Pacific Business Review*, *23*(4), 541–558. https://doi.org/10.1080/13602381.2017.1346910

Cheslow, D. (2019, January 15). *Huawei founder denies his firm spies for China*. NPR. https://www.npr.org/2019/01/15/685484428/huawei-founder-denies-his-firm-spies-for-china

Eadicicco, L. (2019, May 3). *Huawei, the Chinese tech giant embroiled in controversy, just overtook Apple to become the second-largest smartphone maker*. Business Insider. https://www.businessinsider.com/huawei-surpasses-apple-as-second-largest-smartphone-maker-2019-5

Friis, K., & Lysne, O. (2021). Huawei, 5G and security: Technological limitations and political responses. *Development & Change*, *52*(5), 1174–1195. https://doi.org/10.1111/dech.12680

Fu, X., Sun, Z., & Ghauri, P. N. (2018). Reverse knowledge acquisition in emerging market MNEs: The experiences of Huawei and ZTE. *Journal of Business Research*, *93*, 202–215. https://doi.org/10.1016/j.jbusres.2018.04.022

Hass, R., & Denmark, A. (2020, August 7). *More pain than gain: How the US-China trade war hurt America*. Brookings. https://www.brookings.edu/blog/order-from-chaos/2020/08/07/more-pain-than-gain-how-the-us-china-trade-war-hurt-america/

Huawei. *2021 annual report*. https://www.huawei.com/en/annual-report/2021

Huawei. *Huawei facts*. https://www.huawei.com/en/facts

Kaska, K., Beckvard, H., & Minárik, T. (2019). *Huawei, 5G, and China as a security threat*. NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/uploads/2019/03/CCDCOE-Huawei-2019-03-28-FINAL.pdf

Liu, X. (2021). Chinese multinational enterprises operating in western economies: Huawei in the US and the UK. *Journal of Contemporary China*, *30*(129), 368–385. https://doi.org/10.1080/10670564.2020.1827351

Luo, Y., Cacchione, M., Junkunc, M., & Lu, S. C. (2011). Entrepreneurial pioneer of international venturing: The case of Huawei. *Organizational Dynamics*, *40*(1), 67–74. https://doi.org/10.1016/j.orgdyn.2010.10.010

McLure, J. (2012). State capitalism. *CQ Global Researcher*, *6*(10), 229-256. https://library.cqpress.com/cqresearcher/document.php?id=cqrglobal2012051500&type=query&num=huawei&

Rogers, M., & Ruppersberger, D. (2012). *Investigative report on the U.S. national security issues posed by Chinese telecommunications companies Huawei and ZTE*. U.S. House of Representatives Permanent Select Committee on Intelligence. https://republicans-intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf

Tang, M. (2020). Huawei versus the United States? The geopolitics of exterritorial internet infrastructure. *International Journal of Communication*, *14*, 4556–4577. https://ijoc.org/index.php/ijoc/article/view/12624

Tian, T., & Wu, C. (2015). Common sense and truth: Customer centricity. In *The Huawei story*. SAGE Publications India Pvt, Ltd.

Wen, Y. (2020). March into the global north: Opportunity or peril? In *The Huawei model: The rise of China's technology giant*. University of Illinois Press.

Yan, X., & Huang, M. (2022). Leveraging university research within the context of open innovation: The case of Huawei. *Telecommunications Policy*, *46*(2), 1-11. https://doi.org/10.1016/j.telpol.2020.101956

Zhang, G. (Ed.). (2013). *Providing global IT solutions from China: The Huawei story*. Paths International, Limited.