Huawei and ZTE:

Huawei: A history
Huawei Shenzhen Technology Company. Huawei was founded in 1988 by Ren Zhengfei, a former director of the PLA General Staff Department’s Information Engineering Academy, which is responsible for telecom research for the Chinese military. Huawei maintains deep ties with the Chinese military, which serves a multi-faceted role as an important customer, as well as Huawei’s political patron and research and development partner. Both the government and the military tout Huawei as a national champion, and the company is currently China’s largest, fastest-growing telecommunications-equipment manufacturer.

Huawei and the Chinese military
Despite denials the Chinese military is a key customer of Huawei. According to Timothy Heath, Senior International Defense Research Analyst at the RAND Corporation:

Huawei continues to receive contracts from the Chinese military to develop dual use communications technologies. As of January, 2018, Huawei remained active in the 863 funding program. In particular, it is helping develop 5G networks with military applications in mind.

Chinese law compelling espionage
Chinese law compels companies such as Huawei and ZTE and their Chinese citizen employees to engage in intelligence gathering on behalf of the Chinese government regardless of their location. This requirement is consistent across several laws on the protection of China’s state security. For example, according to China’s 2015 State Security Law, ‘Citizens of the People’s Republic of China, every state organ and the armed forces, each political party, the militia, enterprises, public institutions and social organisations, all have the responsibility and obligation to maintain state security.’

Furthermore Article 7 of the National Intelligence Law states:

Any organisation and citizen shall, in accordance with the law, support, provide assistance, and cooperate in national intelligence work, and guard the secrecy of any national intelligence work that they are aware of [emphasis added]. The state shall protect individuals and organisations that support, cooperate with, and collaborate in national intelligence work.

---

It is also important to recognise that the Chinese policy of ‘intelligence work’ is significantly different to western concepts. The concept of ‘intelligence work’ from a Chinese perspective is not tied to specific legislation (which is usually vague and non-descript) but rather is defined on an ad-hoc basis as to whatever is beneficial to the Chinese government, and particularly the Chinese Communist Party at any particular moment; in effect a ‘rule by law’ rather than ‘rule of law’ approach. This was of significant concern to the Australian security services and a major factor in their ban of Huawei and ZTE in the roll-out of 5G networks in the Commonwealth. As Huawei’s 5G footprint expands, the ability for Chinese intelligence to leverage its infrastructure for espionage will only increase.

Concerns of global security services
Security services around the world have raised red flags about the use of Huawei and ZTE equipment in 5G networks. 5G will see an explosion of data devices which will eclipse the amount of devices currently connected to 4G networks. Data processing will also be different to the traditional methods and RAN architecture will reflect this. Network Cores will not be responsible for the bulk of the processing, instead devices on the edge will be able to process data – and it is these devices that are the major security concern. Traditional methods of cybersecurity are simply not good enough. Coupled with recent Chinese legislation compelling companies and Chinese citizens to engage in espionage when directed to do so it is clear a manufactured ‘perfect storm’ for Chinese espionage has been created for the 5G ecosystem.

Australia
In August 2018 the Australian security services recommended the banning of Huawei as a vendor for 5G networks; a recommendation accepted by the Australian government. Without actually naming Huawei or ZTE the Australian government stated that:

The involvement of vendors who are likely to be subject to extrajudicial directions from foreign governments that conflict with Australian law, may risk failure by the carrier to adequately protect a 5G network from unauthorised access or interference.

Canada
Canadian intelligence sources have expressed concerns about allowing Huawei and ZTE participate in 5G network builds, but those concerns have not yet resulted in Government action. However the Government minister responsible has expressed his concern. Ward Elcock, former head of the Canadian Security Service has also echoed the concern:

---

12 Financial Times. (2018, August 23). Australia bans China Huawei’s 5G rollout over security fears. Link: https://www.ft.com/content/c5f24650-a66b-11e8-8ecf-a7ae1beff35b
I think we should be very careful about using Huawei equipment extensively\textsuperscript{13}.

Furthermore, two separate Canadian government memoranda from the Department of Public Safety (which oversees Canada’s spy agency, CSIS) outlined security concerns about Huawei. In 2016, Canada rejected the immigration applications of two Chinese employees from Huawei, based on espionage concerns surrounding the company.

**Germany**

Germany has a strong record of previous opposition to Chinese technology in their networks. In 2012, Germany excluded Huawei from bidding on tenders at Deutsches Forschungsnetz (DFN), Germany’s national research and education network. While the DFN network has been using Huawei equipment since 2005, Huawei and other Chinese vendors are not being considered to upgrade DFN’s network due to security concerns. The German security services are currently reviewing the threat of Huawei and ZTE to national security and a number of individuals have expressed their concern.

“There is serious concern. If it were up to me, we would do what the Australians are doing,” one senior German official involved in the internal 5G debate in Berlin told Reuters\textsuperscript{14}.

In Germany, officials said that the mood in government was growing increasingly wary of Huawei’s potential involvement in building the country’s 5G network. While it is too early to say if Berlin will ban the Chinese company from participating, concerns in some parts of the government, including the foreign and interior ministries, is deepening, officials said\textsuperscript{15}.

**India**

Whilst India had initially excluded Huawei and ZTE from participating in 5G network builds\textsuperscript{16} it later sent a letter of invitation to the companies to participate in testing after significant pressure from the Chinese Government. Telecom secretary Aruna Sundararajan has initially told the *Economic Times of India* that:

We have written to Cisco, Samsung, Ericsson, Nokia and telecom service providers to partner us in 5G technology-based trials, and


\textsuperscript{14} Silicon. (2018, November 14). *German Officials Urge Huawei Ban For 5G Rollout.* Link: https://www.silicon.co.uk/networks/carriers/german-urge-huawei-ban-5g-238861?inf_by=5c047e19671db89d0d8b4de1

\textsuperscript{15} The Financial Times. (2018, November 29). UK and Germany grow wary of Huawei as US turns up pressure. Link: https://www.ft.com/content/6719b6b2-f33d-11e8-9623-d7f9881e729f

have got positive response ... we have excluded Huawei from these trials (when asked if it was due to security reasons).\(^\text{17}\)

The pressure may have related to the desire by the Chinese government to begin processor chip manufacturing in India – and to knowledge-share from existing manufacturing engineers based in India.

**New Zealand**

To much media coverage, the GCSB (New Zealand’s intelligence agency) also refused to approve Huawei 5G hardware in the proposed network of Spark citing “significant national security risks”.\(^\text{18}\)

**United Kingdom**

In November 2018 Matthew Gould, the head of digital policy at the UK Department for Digital, Culture, Media and Sport, and Ciaran Martin, the head of the National Cyber Security Centre, wrote to several telecoms companies warning them that their 5G supply chain may be affected by a review of the UK’s telecoms infrastructure.\(^\text{19}\) In July a report by The NCSC stated that it was concerned over “shortcomings” in Huawei’s engineering processes that expose British telecoms networks to “new risks”, including a cyber-attack. The report could not give 100% assurance that Huawei technology was secure:

Due to areas of concern exposed through the proper functioning of the mitigation strategy and associated oversight mechanisms, the Oversight Board can provide only limited assurance that all risks to UK national security from Huawei’s involvement in the UK’s critical networks have been sufficiently mitigated.\(^\text{20}\)

It should also be noted that prior to Huawei reaching an agreement in the United Kingdom to vet its hardware and software for cybersecurity concerns after disclosure of the company’s growing relationship with BT Group, Britain’s Joint Intelligence Committee warned that, in the event of a cyber-attack, it “would be very difficult to detect or prevent and could enable the Chinese to intercept covertly or disrupt traffic passing through Huawei-supplied networks.”\(^\text{21}\)

---


\(^\text{18}\) Financial Times (2018, November 28). New Zealand blocks Huawei 5G bid on national security concerns. Link: https://www.ft.com/content/7387411a-f2bd-11e8-ae55-df4bf40f9d0d

\(^\text{19}\) Financial Times. (2018, November 6). UK warns telecoms groups to check security of 5G suppliers. Link: https://www.ft.com/content/29eb5d28-e10d-11e8-8e70-5e22a430c1ad


Huawei implicated in espionage

There are a number of examples of Huawei being directly implicated in espionage against other countries. Huawei attempted in each case to deny its culpability and refused to cooperate fully with investigations.

**Example 1: The African Union headquarters hack**

In January 2018, France’s Le Monde newspaper published an investigation, based on multiple sources, which found that from January 2012 to January 2017 servers based inside the AU’s headquarters in Addis Ababa were transferring data between 12 midnight and 2 am—every single night—to unknown servers more than 8,000 kilometres away hosted in Shanghai. Following the discovery of what media referred to as ‘data theft’, it was also reported that microphones hidden in desks and walls were detected and removed during a sweep for bugs. Huawei was the main provider of ICT for the AU and the project. Huawei also provided cloud computing to the AU headquarters and signed a MoU with the AU on ICT infrastructure development and cooperation. It also trained batches of the AU Commission’s technical ICT experts. The AU had to subsequently acquire its own servers at significant cost.

Whilst Huawei deny involvement in the data transfer it was also discovered that ZTE had its own contract with the AU which may have allowed it to access the data and engage the transfer.

*Note:* Huawei is increasingly involved in managing and storing the sensitive information of foreign governments and private citizens as well as equipping critical infrastructure projects. These are end uses that can have severe consequences when corrupted with weak security or back doors. State-backed cyber actors from both China and Russia have been detected mapping the critical infrastructure networks of other countries, specifically targeting these industries with espionage efforts.

**Example 2: India projects**

Significant distrust of Chinese telecoms companies exists in India, as evidence by the initial excluding of Huawei and ZTE from 5G trials. In 2010, India blocked for several months domestic carriers’ imports of Chinese telecoms equipment over suspicions that it might have spying technology embedded to intercept sensitive conversations and government communications.

---


24 Financial Times (2018, January 29). *African Union accuses China of hacking headquarters.* Link: [https://www.ft.com/content/c26a9214-04f2-11e8-9650-9c0ad2d7c5b5](https://www.ft.com/content/c26a9214-04f2-11e8-9650-9c0ad2d7c5b5)

communications. The unofficial ban was lifted after the Chinese makers, who had said their equipment was safe, agreed to new equipment rules with tougher checks.\(^{26}\)

Huawei was implicated in the hacking of Indian carrier Bharat Sanchar Nigam (BSNL) in 2014. Responding to a parliamentary question Killi Kruparani, junior minister for communications and information technology, said, “An incident about the alleged hacking of Bharat Sanchar Nigam Ltd network by M/S Huawei ... has come to notice”\(^{27}\).

In July 2015 the Indian Home Ministry approved a Huawei project to set up an electronics and telecommunications device manufacturing factory in Sriperumbudur. The contact was only awarded after a myriad of cybersecurity concerns led the Indian government to issue various amendments to the contract, such as requiring Indian nationals fill critical positions at the factory\(^{28}\).

**Example 3: South Sudan**
In 2014, Huawei entered into an agreement with UNESCO to improve internet connectivity in South Sudan’s schools. While this project, which was expected to finish in 2016, appeared to be assisting in the state’s development, issues surrounding Huawei’s presence in the country soon arose. In October 2014, the head of South Sudan’s Ministry of Information and Broadcasting agency accused Huawei of hacking government e-mail and falsifying and forging documents on behalf of the senior government officials. He also accused Huawei of forging a letter to the President of the Exim Bank of China under his name\(^{29}\).

**Example 4: Supplying technology to rogue states**
Huawei has been investigated for allegedly circumventing official sanctions in the sale of products to Iran, Sudan, Cuba and Syria, including possibly re-exporting U.S. technology illegally. Moreover, when the U.S. Department of Commerce announced an investigation into fellow Chinese telecom giant, ZTE, in March 2016, it released a document showing ZTE executives mapping out a plan for how to get around U.S. export controls. According to the New York Times, the document said the strategy came from a company, referred to as F7, that closely resembled Huawei\(^{30}\).

---


\(^{27}\) Financial Times (2014, February 7). *India: Huawei investigated over alleged BSNL hack*. Link: [https://www.ft.com/content/aabe2d64-d1e6-33d4-8371-48231e327ba0](https://www.ft.com/content/aabe2d64-d1e6-33d4-8371-48231e327ba0)


Example 5: Boyusec and APT3
A 2016 intelligence report by the Pentagon and research published by cyber-security firm, Recorded Future, have documented the cyber espionage activities of Guangzhou Boyu Information Technology Company (Boyusec) and its ties to China’s MSS intelligence services. Corroborating these allegations, in November 2017, Boyusec co-founder Wu Yingzhuo, Executive Director Dong Hao, and employee Xia Lei, were indicted by the U.S. Department of Justice for hacking and stealing materials from Moody’s, Siemens, and Trimble. Boyusec’s website listed Huawei as a cooperative partner. According to the Pentagon’s Joint Staff J-2 Intelligence Directorate both Boyusec and Huawei work to produce security products that will be loaded into Chinese-manufactured computer and telephone equipment - allowing Chinese intelligence to capture data and control the infected hardware31.

Example 6: Pre-installing unremovable malware on devices
In 2015 and 2016, reports emerged from cybersecurity groups, including G DATA and Kryptowire, that smartphones sold by Huawei, Lenovo and Xiaomi were being sold with preinstalled, un-removable malware on them that enabled third parties to listen to calls, track users, download contact lists and call logs, see users’ texts, make online purchases and extract other personal data. The Chinese company, Adups, that developed the software said it was not intended for American phones, indicating it was written at the request of an unidentified Chinese manufacturer. Both Huawei and ZTE are listed on the company’s website as customers of its products32.

*It should be noted that Huawei deny all of the above examples.*

Case Studies: How Huawei and ZTE technology can be utilised for Chinese espionage

Chinese tech companies and 5G reliant technologies: Case Study: Connected Vehicles

Huawei has also engaged a number of European car manufacturers to explore rolling out Huawei GPS technology for both autonomous vehicles, connected vehicles and GPS assisted navigation. In 2016 French car manufacturer Groupe PSA33 signed a deal with Huawei called "Push to Pass" strategy for 2016 to 202134. If implements with Huawei technology car manufacturers will be able to track, in real-time, the location of a vehicle, and retain the data. Generally this data is not collected in real-time by car manufactures and this would be a significant departure from the status quo. In 2018 the Chinese government directed all Chinese car manufacturers to integrate such surveillance into their vehicle tracking systems35. In October 2018 Huawei also signed a research partnership agreement with Audi to collaborate on "intelligent connected vehicles"36.

The French security services, the SGDSN, and the National Cybersecurity Agency of France – ANSSI, have both raised concerns over the growing dominance of Chinese connected vehicles systems, especially those that will be paired to 5G networks with Chinese hardware and the deal with Groupe PSA. Specifically the various agencies are concerned that cars using this technology and paired with any network run with Chinese hardware would be make vehicles susceptible to espionage; with the ability for Chinese spy agencies to hack the software to allow them use the voice recognition features to listen in on conversations of persons of interest such as CEOs, politicians and high ranking civil servants37.

Huawei collaboration with manufacturers continues. In November 2018 Vodafone, Jaguar Land Rover and Huawei collaborated on a full Cellular Vehicle-to-Everything (C-V2X) system - such a system is capable of simultaneously undertaking both direct short-range communications and long-range communications over a live network. This included connecting to Huawei’s PC5-enabled roadside unit (RSU) for speed limit alerts38. Over-reliance of such RSU alert systems, if hacked, could be dangerous.

CCTV and Facial Recognition: Case Study: Social scoring of non-Chinese citizens

By 2020 the Chinese plans to roll out a ‘social credit’ system which will rank citizens allegiance to the state and allow them certain liberties based on their credit rating. Whilst this may

---

33 Groupe PSA manufacture the following: Citroën; DS; Ambassador; Opel; Peugeot; Vauxhall; Aixam
35 AP (2018, November 30). In China, your car could be talking to the government. Link: https://www.apnews.com/4a749a4211904784826b45e812cf4ca?utm_source=newsletter&utm_medium=email&utm_campaign=newsletter_axiosam&stream=top
sound like the preserve of the communist state access to 5G networks globally could allow the Chinese government to build similar ‘social credit’ scores on non-Chinese citizens; albeit less detailed.

In November 2018, speaking in front of business leaders in a held forum in Manila, a high-ranking Huawei official said the tech giant wants to install modern cameras all around the Philippines to ensure the ‘safety’ of Filipinos. The Huawei official also outlined the capabilities of their cameras, which, he claimed, have artificial intelligence and are equipped with machine learning39. Huawei currently have contracts with the two carriers, Smart and Globe, and China Telcom was recently awarded the third telco license for the Philippines – a license rushed through by the Filipino president.

A number of countries have expressed interest in developing Chinese-style systems to monitor their citizens and, in effect any citizen from other nations who happen to visit, be it for business or leisure. Chinese officials have held meetings with over 30 countries about the system, according to Freedom House’s 2018 report on digital authoritarianism40.

Background: Huawei and ZTE – Allegations of corruption and failures to deliver

Allegations of corruption

Algeria
In 2012, Algeria banned Huawei and ZTE from participating in any public tender ventures in the country for two years. They were involved in paying $10 million in bribes to a former executive of the state-owned Algeria Telecom, Mohamed Bukhari, between 2003 and 2006.\(^41\)

Ghana
In 2012 Huawei was selected to implement Ghana’s $127.5 million e-government project, improving online services for citizens. The project has been criticized due to an alleged $43 million tax incentive granted to Huawei. Evidence was later found that showed Huawei had materially supported the ruling party after the tax incentive was granted.\(^42\)

Nigeria
In 2014, Huawei and ZTE was contracted to build Nigeria’s National Rural Telephone Project for $200 million. They, however, only managed to build local exchanges, failing to meet their contractual obligations. As a result, the project was cancelled and awarded to other companies.

Pakistan
In 2013 Huawei was successful in tendering for a $124.7 million Islamabad Safe City Project. The project was financed by a $68 million short-term loan from the Exim Bank of China. The system was to be complete by 2015. It ran significantly over cost and was delayed by one year. Huawei was forced to renegotiate the contract by the Supreme Court and the chair of a Senate Standing Committee overseeing the project that had initially highlighted its inflated cost observed that Pakistan should blacklist Huawei over the controversies encountered in this project.\(^43\)

Solomon Islands
In 2017, the Solomon Islands government abruptly pulled a submarine fiber optic cable contract from a British-American contractor in favour of Huawei. The change was reportedly done without proper processes, even prompting the Asian Development Bank to withdraw its support on the basis that it had no information on other bidders. Allegations also emerged of a $5.25 million political donation by Huawei to the ruling party in Honiara.\(^44\)


South Africa
In 2013, Huawei was awarded a $27 million contract by the Gauteng Department of Finance (GDF) in South Africa to provide 88,000 tablets for a e-learning project. Huawei was later investigated for the manipulation of contract requirements.45

Examples of Huawei and ZTE failure to complete major projects

Bolivia
In 2009, Entel Bolivia signed a $120 million contract with Huawei to implement the construction of telecommunications infrastructure and supply services that would provide rural Bolivia with telephone service. In December 2010, Huawei was declared non-compliant in the fulfilment of the contract and fined $8 million by the Bolivian government.46

Kyrgyzstan
In 2015, the Kyrgyz State Committee for the Fight Against Economic Crimes announced that they were investigating claims that Huawei artificially increased the cost of a telecommunications project by over $1.55 million. They believe that $300,000 was spent on work that cost the Kyrgyz government $3 million. The original agreement is not in the public record. This resulted in Huawei’s Kyrgyz accounts and other property being seized by the government and a court ruling in absentia to take the culprits into custody.47

South Africa
In 2014, South Africa’s Mustek won a contract to supply $12 million worth of Huawei’s signaling and telecommunications equipment for railways to a consortium consisting of Zambia Railways, Huawei International, Bombardier Transportation and GMC Technologies. Mustek was selected for its expertise in logistics and, as part of the contract, to deliver the equipment from Hong Kong to Zambia. The consortium was previously contracted to upgrade Zambia’s railway for $51 million. Muyenga Atanga, CEO of Zambia Railways, was fired for awarding the contract. Zambia’s Minister of Communication and Transport, Kapembwa Simbao, cited the contract cost as excessive and overpriced. After it was completed, Zambia Railways only used a fraction of the installed infrastructure.48

South Sudan
In 2014, Huawei entered into an agreement with UNESCO to improve internet connectivity in South Sudan’s schools. While this project, which was expected to finish in 2016, appeared to be assisting in the state’s development, issues surrounding Huawei’s presence in the country soon arose. In October 2014, the head of South Sudan’s Ministry of Information and Broadcasting agency accused Huawei of hacking government e-mail and falsifying and forging

45 IT Web Online. (2013) "New service providers for Gauteng Online." Link: https://www.itweb.co.za/content/okYbe97XYJBMAMwpG
documents on behalf of the senior government officials. He also accused Huawei of forging a letter to the President of the Exim Bank of China under his name.

**Uganda**

In 2006, Huawei was contracted by the Uganda to construct a telecommunications backbone network. The construction was expected to last 27 months and cost $55 million. Instead, the project was delayed and costs increased by $7 million, necessitating another loan. In 2012, the government ordered an investigation into the project over claims of inflated prices and the use of inferior equipment. It was noted that Huawei spent $38 million on a similar project to cover a distance of 2,300 km, while, in this case, Uganda would spend over $62 million to cover 2,100 km.

In March 2015, an audit of Uganda’s National Backbone Infrastructure (NBI) and Electronic Government Infrastructure (EGI) projects under Huawei recommended the projects be cancelled due to cost overruns and price gouging.

**United Kingdom**

In December 2012, Huawei was awarded a contract to deliver service management and operations of telecommunications company Three’s core network in the UK under a 5-year, $192 million contract. In October 2014, it was announced that Huawei had missed the performance standards set by the contract with Three and forced the British company to complete the work in house. As a result, Huawei allocated $20 million as a voucher for Three allowing it to receive discounts on future work over three years.

**Zimbabwe**

In 2010, TelOne awarded a $98 million contract to upgrade and modernize Zimbabwe’s telecom network to Huawei. A delay in implementing the project meant that TelOne eventually resorted to using its own resources to fund the project. The lack of promised funding from Huawei led to delays and a reduction in the scale of the project. It was then alleged that Huawei’s project had been over-priced. In December 2015, the contract was cancelled with Huawei, delaying it for years.

---


52 The Daily Mail (2014) "Huawei Loses Key Contract in £20m Blow."

53 Newsday (2016) "TelOne to kick-start $98 million project - NewsDay Zimbabwe." Link: [https://www.newsday.co.zw/2016/03/telone-kick-start-98-million-project/](https://www.newsday.co.zw/2016/03/telone-kick-start-98-million-project/)