Introduction

Based on an in-depth review of the global business transactions carried out by Huawei over the past decade as well as the company’s associations inside China, RWR Advisory Group (RWR) highlights in this report the risk factors present when doing business with the company. The intent is to present in one place a holistic view of the various ways in which Huawei’s transactions and business practices have undermined their value proposition. In the course of this research, a number of themes emerge regarding Huawei that raise serious concerns.

What differentiates this report from others examining Huawei is its granular, transactional level analysis. The report leverages RWR’s IntelTrak tool that tracks daily the international operations of not just Huawei, but a broad spectrum of Chinese state-owned and private enterprises.

Huawei’s risk profile is broadly defined by: 1) its alleged connections to China’s People’s Liberation Army ( PLA) and the Chinese Communist Party (CCP); 2) evidence of an ongoing, close business relationship with that state or state-backed entities; 3) the track record of the Chinese government engaging in cyber espionage and cyber-attacks against government, corporate and industrial targets, including through the use of external entities; and 4) the risk of Huawei being used as one such external entity or tool. This risk has been deemed sufficiently acute in the United States that legislation was even introduced in the U.S. Senate (SB 2391) on February 7, 2018 that ...
A Summary of the Different Risk Factors Faced by Huawei’s Partners and Customers

... would prohibit all U.S. government agencies from both purchasing and leasing any hardware from Huawei for reasons of national security.

Beyond these four foundational reasons for caution when doing business with Huawei, the company’s global track record at a transactional level demonstrates a range of other risk factors, including: disputes over copyright infringement; allegations of overpricing or reneging on contracts; labor disputes; performance problems; and allegations of bribery, corruption and the pursuit of foreign political interference.

This report includes summaries of those specific transactions where these various concerns have emerged most significantly. These transactions show that, when doing business with Huawei, the risk associated with protecting proprietary information and intellectual property, network security, and national security is only part of the problem.

In documenting these issues, this report goes beyond the fundamental questions concerning the company’s trustworthiness. It seeks to illuminate the transactional risk that Huawei customers and partners have taken on when working with the company.

<table>
<thead>
<tr>
<th>Most Frequent Risk Factors Encountered by Huawei Partners and Customers (by Count, 2012-2018)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Concern Raised About Cyber Security</td>
</tr>
<tr>
<td>Delayed or Canceled Transaction</td>
</tr>
<tr>
<td>Local Political/Regulatory Opposition</td>
</tr>
<tr>
<td>Cost Inflation and Company Reneging on Contractual Commitments</td>
</tr>
<tr>
<td>Accusation of Military Influence, Dual Use Potential</td>
</tr>
<tr>
<td>Non-Competitive Tender Process, Lack of Transparency</td>
</tr>
<tr>
<td>Dispute over Failure to Perform, Quality Control and Safety Problems</td>
</tr>
<tr>
<td>Bribery &amp; Corruption Allegations</td>
</tr>
<tr>
<td>Local Disputes, Labor Protests and Allegations of Fraud</td>
</tr>
<tr>
<td>Strategic Gains, Non-Commercial Terms (Risk of Asset Capture)</td>
</tr>
</tbody>
</table>
Background

Over the past two decades, Huawei has rapidly risen through the ranks of leading telecommunications and information technology equipment companies, assisted at times by the availability of cheap, subsidized financing from the state and an ability to undercut its competition on price. Since its early days, Huawei’s products and solutions have become significantly more advanced and popular in global markets. Concern the company is susceptible to having its equipment and technology exploited by Chinese intelligence services, however, has had a damaging effect on the company’s reputation and business prospects in certain markets. This fear, however, does not represent the full extent of the risk brought by the company to its partners and customers.

The primary problem inhibiting any near-term repair of Huawei’s reputation is the lack of trust in the Chinese government. It is widely believed that the Chinese government retains the ability and the authority to weaponize Huawei’s assets, access and market position at the time and place of its choosing. Michael Hayden, former Director of the Central intelligence Agency and National Security Agency, for example, offered,

“I stand back in awe at the breadth, depth, sophistication and persistence of the Chinese espionage campaign against the West...God did not make enough briefing slides on Huawei to convince me that having them involved in our critical communications infrastructure was going to be okay. This is not blind prejudice on my part. This was my considered view based on a four-decade career as an intelligence officer.”

The nature of the technology involved and the value of the data flowing through it creates a tempting, attainable target. Accordingly, the motivation of the company’s leadership and management, even though it is highly suspect, may practically be irrelevant.

The primary problem inhibiting any near-term repair of Huawei’s reputation is the lack of trust in the Chinese government...The nature of the technology involved and the value of the data flowing through it creates a tempting, attainable target.

Accordingly, the motivation of the company’s leadership and management, even though it is highly suspect, may practically be irrelevant.

The nature of the technology involved and the value of the data flowing through it creates a tempting, attainable target for the Chinese government. Accordingly, the motivation of the company’s leadership

---

and management, even though it is highly suspect, may practically be irrelevant. In the meantime, the track record of the Chinese government in the cyber realm is bad and getting worse.

Summary Findings

Based on RWR’s review of the company’s global business transactions and associations (provided below), the following is a short summary of the company’s most significant risk factors.

- The leadership of Huawei appears to have past connections to the PLA, the CCP and to China’s Ministry of State Security (MSS), the country’s intelligence services.

- Huawei claims the Chinese state has no influence over its activities, but the company is treated as a state-owned enterprise and has benefited from state procurement funds, subsidized financing from state-owned policy banks and state funding for research.

- Despite its professed distance from the Chinese government, numerous reports have alleged close working relationships between Huawei and some of China’s most notorious state-backed hackers and cyber bad actors, including Boyusec and APT3.

- Many governments (including the United States, Australia, India, Germany, Denmark, Uganda and others) have, at times, raised concerns about the national security risks of contracting with Huawei and blocked – or set strict conditions on – Huawei participating in public tenders.

- The NSA as well as alleged third-party intermediaries have reportedly been able to manipulate and exploit flaws in Huawei’s network and handsets, suggesting other actors – such as the Chinese state – are very likely able to do so as well.
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.

Huawei has also had high-profile failures in the fulfillment of its contractual obligations, triggering political and regulatory blowback, including contract cancellations. Huawei’s reputation has also created challenges and disruptions for the company’s customers.

Among the business risks present in Huawei’s global footprint, are the transaction costs associated with allegations of bribery, allegations of rewarding political parties responsible for contract awards, disputes over employment laws in foreign countries, and being accused of copyright infringement and intellectual property theft by its partners and customers.

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.

Huawei has failed to meet its own standards of adhering to business ethics, international conventions, national laws and regulations, including rules about providing support to foreign political parties and officials (with allegations of such support linked to contract awards).

---

Like other Chinese companies increasingly paying a price for their lack of transparency, Huawei’s opaque governance structure has contributed to its failure to penetrate certain markets. Despite publicly avowed corporate objectives to be more open and improve trust, the company has not satisfied the inquiries of some market players and government regulators. As a private entity, Huawei does not face the same accounting and disclosure standards and requirements as do publicly-traded companies.

The risk and threat profile represented by these bullet points has implications across most of Huawei’s growing locations of operation, including a notably large number of transactions in Europe (i.e., Germany, Russia, the United Kingdom, the Netherlands, and Spain) as well as South Asia (i.e., India and Malaysia). In terms of project values, Huawei’s highest value projects are located in Africa (i.e., Kenya, Ethiopia, and Zimbabwe) and South Asia (i.e., India, Malaysia, and the Philippines). Interestingly, even in the United States, where the federal government has taken a tough position on Huawei, the company is still highly active in relation to its activity elsewhere.

The second map shows this same footprint, but with regional (rather than country) markers sized showing how the dollar value of Huawei’s business compares as a percentage of that region’s GDP. The map shows where Huawei’s footprint likely carries the greatest relative influence or significance to the local economy.
China’s Role in Cyber Attacks and Espionage

In 2015, the Chinese government acknowledged for the first time the existence of cyber warfare divisions within the PLA consisting of: 1) specialized military forces trained in defensive tactics and offensive attack; 2) groups of experts from civil society (including at MSS and the Ministry of Public Security); and 3) private, external contractors or entities.3, 4

These external entities – operating under various names – have been accused many times over the waging of cyber warfare against leading multinational corporations and banks and stealing sensitive information about critical infrastructure and high-end intellectual property.5 China’s admission to specialized units devoted to hacking computer networks should properly focus attention on those Chinese entities building and managing such networks. This announcement came in sharp contrast to repeated PLA denials in previous years that it had ever supported any cyber-attack or hacking activity.6

...in May 2014, an indictment released by the U.S. Department of Justice... alleged that the specific PLA unit where these hackers worked had been hired in the same window by Chinese companies that stood to benefit from the stolen information.

The targeted industries of Chinese operations are significant. In the well-known case of Unit 61398, a Shanghai-based group outed as a cyber warfare arm of the PLA, the group allegedly targeted companies whose databases contained vast and detailed information about critical U.S. infrastructure, including pipelines, transmission lines and power generation facilities.7 The targeting of economic assets for intelligence purposes is especially prevalent in government-led economies, like China, where the interests of business and the state merge.8, 9

---

6 “China (Finally) Admits to Hacking.” The Diplomat. March 18, 2015.
Indeed, in May 2014, an indictment released by the U.S. Department of Justice accusing five Chinese military hackers of computer hacking, economic espionage and other offenses directed at six victims from U.S. industry alleged that the specific PLA unit where these hackers worked had been hired in the same window by Chinese companies that stood to benefit from the stolen information. This confluence of events introduced interesting questions about who was the initiator in these espionage operations: the Chinese state or the companies themselves. Reports such as this provide insight into how these efforts are organized and why companies like Huawei are suspect.

There are many examples of Chinese corporate espionage to draw from. As recently as January 25, 2018, a major Chinese wind power company, Sinovel, was found guilty in a U.S. court of “conspiracy to commit trade secret theft” against a former U.S. partner. In April 2017, PwC issued a comprehensive report detailing the hacking activities of the China-based (and likely state-backed) APT10 against a number of managed IT service providers (MSPs) in a cyber espionage campaign described as “Operation Cloud Hopper.” The target of this sustained campaign was, in large part, intellectual property.

Additional incidents around the world attributed to the Chinese state are listed below, underscoring the danger China is broadly believed to represent in this domain.

- In 2013, Unit 61398 first came under the spotlight as an offshoot of the PLA for attacks against U.S. firms and the theft of hundreds of terabytes of data from at least 141 organizations across 20 industries around the world. While China has previously denied state ties to cyber-attacks, China Telecom, a state-owned enterprise, is alleged to have supplied Unit 61398 with special fiber optic communication infrastructure in the name of national defense.
- In 2014, the U.S. Department of Justice unsealed an indictment targeting five members of the PLA for hacking into the networks of Westinghouse Electric, the United States Steel Corporation and other companies. The move was an important escalation in terms of U.S. government willingness to attribute malevolent cyber activity directly to the Chinese state.
- In 2014, Chinese investors froze financing for infrastructure projects in Vietnam after Hanoi’s criticism of Beijing over its South China Sea island-building.

---

14 “What we know about the Chinese army’s alleged cyber spying unit.” CNN. May 20, 2014.
17 “What we know about the Chinese army’s alleged cyber spying unit.” CNN. May 20, 2014.
airports were hacked showing messages criticizing Hanoi’s stance, demonstrating the vulnerability of Chinese-built digital infrastructure to cyber-attack from Chinese sources.19

- In 2015, Australian officials claimed that a cyber-attack on the Bureau of Meteorology was committed by Chinese actors. The attack was expected to cost the Australian government millions of dollars to fix after the breach of one of the country’s largest supercomputers holding sensitive government information, including that of the Department of Defense.20

- In 2017, Chinese cyber spies broadened their attacks on official and corporate targets in Vietnam during a time of raised tensions over the South China Sea. The hackers were identifiable due to the reuse of an earlier infrastructure design.21

Despite differing perceptions of the risk associated with Huawei, China’s aggressive use of the cyber domain, and the threat it represents, is well understood across different governments as well as private sector experts and companies.

- In June 2017, Germany’s BfV domestic intelligence unit reported that one of the priority areas of focus of Chinese intelligence is German businesses and acquiring technical know-how.22

- Danish intelligence sources recently said, “China uses its cyber capabilities for obtaining information of economic, political and military importance.”23

- The Netherlands, home to one of the world’s largest internet exchange points, has warned that, “some of the companies that operate in the Netherlands as suppliers originate from high-risk countries and that some have past or present links with foreign intelligence services...This provides an increased risk of espionage.”24

- The Danish Defense Intelligence Service offered that “China has advanced cyber capabilities, which it uses for defensive and offensive purposes alike. China has just concluded a major military reorganization of its cyber capabilities, likely allowing Chinese actors to conduct more sophisticated cyber espionage campaigns that are harder to detect.”25 The Chief of the Danish

---

25 “Intelligence Risk Assessment 2017.” Danish Defense Intelligence Service.
Defense Intelligence Service, Lars Findsen, added that China was specifically focused on industrial espionage and targeting Danish high-tech companies.”26

- Australian Attorney General George Brandis made it a priority to pursue an aggressive new legal framework that would set new rules for who can lawfully influence government politicians. Fairfax Media reports described intelligence briefings received by Mr. Brandis regarding efforts by Chinese Communist Party-affiliated lobbyists and business people to influence local, state and federal government officials. In the context of these efforts, leaked parliamentary briefing papers, according to reporting by the Sydney Morning Herald, noted “initiatives such as the ‘Torch’ program, which links Australian universities with Chinese companies and China’s technology ministry, have triggered concerns about ‘Chinese companies [co-opting] … Australian research’ and ‘diverse security challenges to Australian high tech industries.’”27

- Michael Hayden, former U.S. Director of the Central Intelligence Agency and National Security Agency, made a number of salient points during an interview with the Australian Financial Review28, stating,

  “I stand back in awe at the breadth, depth, sophistication and persistence of the Chinese espionage campaign against the West...God did not make enough briefing slides on Huawei to convince me that having them involved in our critical communications infrastructure was going to be okay. This is not blind prejudice on my part. This was my considered view based on a four-decade career as an intelligence officer.”

  “China does not confine itself to espionage against what you or I would call ‘state secrets.’ They have a much broader definition of legitimate espionage to include intellectual property, commercial trade secrets, and the negotiating positions of private entities. In other words, they don’t limit themselves in the way we do in the English-speaking community.”

  “Finally, as highlighted wonderfully in the [Permanent Select Committee on Intelligence of the House of Representatives] open hearings with Huawei officials last year, these guys are not even transparent to themselves. There’s no transparency around who appoints the board of directors or controls the ownership of the business. And there’s no independent Chinese government oversight committee that could give us continuing confidence that Huawei or ZTE would not do what they promised not to do.”

More recently, Accenture Security’s 2017 Cyber Threatscape Report offered the following set of bottom-lines on China’s objectives in the cyber domain.

“After observing a downturn of activity in China, iDefense expects China's cyber-espionage activities aimed at technology transfer to regain historic levels. China’s 13th Five-Year Plan (FYP), which is now underway, may prompt the targeting of companies active in the areas of cyber-security, cloud computing and big data, new energy automobiles, high-performance computing, biomedical materials, repair and replacement of tissues and organs, deep sea key technology and equipment, and smart grid technology and equipment. Historically, Chinese cyber-espionage operations have heavily targeted foreign technologies that overlap with FYP goals. Newly created after a military-wide restructuring, the Strategic Support Force of the People’s Liberation Army (PLA) is also tasked with supporting innovation and military development, including support through cyber-espionage means, and many FYP projects will likely reinforce this mission.”

Huawei’s Alleged PLA and CCP Connections

A wide spectrum of analysts, experts, journalists and U.S. and other government agencies have detailed the alleged links between Huawei, the CCP and the PLA, and enumerated the aspects of these links that Huawei refuses to clarify. Despite the company’s dismissal of these associations, Huawei appears to have a close relationship with the state (receiving $228.2 million in government grants between 2008 and 2011 and some $9 billion in financing from state-owned banks for overseas projects since 2012 as well as millions of dollars of government research funding), which, if nothing else, is evidenced by the extent of government-backed loans and research contracts reportedly won by the company.

---

Like other high-profile Chinese companies that have come under increasing and damaging push-back from government regulators – such as HNA, CEFC, Anbang Insurance and Ant Financial – Huawei has similarly been criticized for its lack of transparency.

One of the primary conclusions of the investigation into the company carried out by the Permanent Select Committee on Intelligence of the U.S. House of Representatives in 2012 was that the company refused to answer certain important questions about its governance and decision-making processes and the role of the Chinese state in those mechanisms.  

It is worth noting that HNA, another major Chinese conglomerate, has come under mounting pressure over just the past six months regarding its refusal to answer adequately questions about its ownership and governance. This has led directly to deals being blocked by the United States, New Zealand and Switzerland. Huawei has an even longer track record of failing to answer these questions adequately and operates in a far more sensitive industry.

Part of the challenge encountered by Huawei is the lack of faith in Chinese institutions when it comes to there being distance between the state and the companies it oversees. In other words, it is assumed that the state exercises a significant degree of control and influence over Chinese companies. China’s new National Intelligence Law, enacted on June 27, 2017, validated this concern. According to the law’s Article 7,

“All national bodies, military forces, political parties, social groups, enterprise and undertaking organizations, as well as citizens, shall support, cooperate with and collaborate in national intelligence work, and maintain the secrecy of national intelligence work they are aware of.”

“Relevant departments in all levels of People’s Governments, enterprise and undertaking work units, other organizations and citizens shall provide the necessary assistance to national intelligence work organs lawfully carrying out their work, and maintain secrecy.”

And Article 11 specifies that the law’s powers are not limited to Chinese soil.

Article 9: “National intelligence work organs launch intelligence work inside and outside of the borders on the basis of work requirements, and by using the necessary methods, means and channels according to the law.”

As Article 28 makes clear, those failing to meet the requirements of the law will face repercussions:

“Those violating the relevant provisions of this Law and impede national intelligence work organs and their personnel from carrying out intelligence work, will be punished by relevant work units on suggestion of the national intelligence work organ, or be subject to a warning of administrative detention of less than 15 days by the national public security body, or public security bodies; where it constitutes a crime, legal liability will be prosecuted according to the law.” 34, 35

While the language of the law is broad and vague, it appears to create sweeping obligations for otherwise private citizens and companies to the state. The power of the law hinges on what – and who – are considered to be “national intelligence work organs.” An expansive reading of Article 6 could be interpreted to mean that private parties qualify – and without any requirement that such person be on Chinese territory.

In terms of basic corporate governance and decision-making, Huawei states that the company’s shares are owned by its employees, but Ren Zhengfei (Huawei’s founder and CEO) confirmed to the Permanent Select Committee that the company’s shareholder agreements give him ultimate veto authority over the company’s material decisions. This disclosure has brought even more scrutiny to Mr. Ren’s personal profile and background.

Ren Zhengfei and Sun Yafang

Huawei’s CEO, Ren Zhengfei, is believed to have served as a Director of the PLA’s Basic Civil Engineering Corps. Huawei describes Mr. Ren as a former soldier who worked for the PLA’s engineering corps, denying he held any senior-level position. According to reports, Mr. Ren left the PLA in 1983 to establish the Liao Yang Chemical Fiber

---


Factory, a state-owned enterprise he was tasked with establishing by the PLA, and, in 1987, under unclear circumstances, he reportedly left to form Huawei.\(^{36}\)

Huawei has never described in detail the transition of Mr. Zhengfei from his time at the state-owned enterprise to Huawei, leading to speculation about a possible agreement that would have a lasting impact on the government’s ties to the rising tech giant. These questions tie into others about any responsibility the state may have had – and may still have – in Huawei’s success and emergence as a “national champion.” An early U.S. government report, produced by the Pentagon in 2009, refers to Huawei as being one of several Chinese technology companies that maintains “close ties to the PLA and collaborates on R&D.”\(^{37}\)

Mr. Ren also sat on the 12\(^{th}\) National Congress of the Chinese Communist Party (CCP), but refuses to disclose any information about his activities during this period.\(^{38}\)

Sun Yafang, the Chairwoman of Huawei and Mr. Ren’s closest advisor, also has reported connections to the PLA. According to U.S. intelligence, Ms. Sun previously worked for the Ministry of State Security (MSS) in the Communications Department. MSS has close ties and sits above (in the organizational chart shown to the right) external entities used by the state for cyber-attacks and espionage (such as the notorious Guangzhou Boyu Information Technology Company, aka. Boyusec). Ms. Sun is alleged to have used her connections to secure funding for Huawei when the company was first founded in 1987.\(^{39}\)

Huawei, a Military Contractor

Although Huawei should not technically be eligible to supply the PLA due to procurement regulations prohibiting the acquisition of sensitive equipment from non-government companies, Huawei is allegedly a significant PLA contractor, managing to circumvent this rule.\(^{40}\) It has been reported, for example, that Huawei and ZTE are working together on a project, called PLA-863, to provide the military with switches, routers and mobile and fiber networks.\(^{41}\) While this does not mean that Huawei is state-owned, it does

---


suggest Huawei has special status with the PLA, which, at minimum, distinguishes the firm from being an ordinary private sector entity.

Huawei’s Alleged Ties to Cyber Attack Groups

Boyusec and APT3

A variety of reports emerging over the past several years, including a 2016 intelligence report by the Pentagon and research published by an anonymous group, Intrusion Truth, as well as 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.42

Boyusec’s website listed Huawei as a cooperative partner, per the image below. In addition, the chart shown above has Boyusec essentially responsive to Chinese intelligence (i.e., MSS).43 Boyusec is either working closely or may even share owners/actors (i.e., “command and control”) with APT3 (also known as Gothic Panda, TG-011 or UPS)44, another sophisticated threat actor linked to MSS with a track record of targeting critical industries and government agencies.45

A report by cybersecurity firm Recorded Future alleged that APT3 was directly tied

45 “APT3 is Boyusec, a Chinese Intelligence Contractor.” Intrusion Truth. May 9, 2017.
to the MSS and recommended that any companies or government agencies that believe they may have been targeted by APT3 to reexamine those instances, needing to realize “their activities support China’s political, economic, diplomatic and military goals.” The entity’s targets have focused on market players in the defense, telecommunications, transportation and advanced technology sectors.

In this context, reports that Huawei is working closely with Boyusec are particularly troublesome. Huawei does not deny these reports, but claims it has merely used Boyusec’s security services to evaluate its internal corporate intranet.” Yet, according to November 2016 reporting by Bill Gertz at the Washington Free Beacon,

> “According to an internal report by the Pentagon’s Joint Staff J-2 intelligence directorate, Boyusec and Huawei are working together to produce security products that will be loaded into Chinese-manufactured computer and telephone equipment. The doctored products will allow Chinese intelligence to capture data and control computer and telecommunications equipment, said Pentagon officials familiar with the report.”

Gertz also quotes a Boyusec official, who reportedly added,

> “It’s closely connected to the [Ministry of State Security] and Huawei and they are developing a start-up program that will use malware allowing for capturing and controlling devices.”

Huawei denies these reports, with their U.S. spokesperson, William Plummer, saying

> “No solution or service from [Boyusec] has ever been incorporated into any Huawei product or service offered to any Huawei customer.”

The 2012 report by the Permanent Select Committee on Intelligence appears to support these allegations, although without naming Boyusec or APT3. Investigators claim to have seen,

> “internal Huawei documentation from former Huawei employees showing that Huawei provides special network services to an entity the employee believes to be an elite cyber-warfare unit within the [People’s Liberation Army].”

According to the report,

> “the documents appear authentic and official Huawei material, and the former employee stated that he received the material as a Huawei employee. These documents suggest once again that Huawei officials may not have been forthcoming [with the Committee] when describing the company’s R&D or other activities on behalf of the PLA.”

---


Pre-Installed Malware

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.\(^49\) According to the *New York Times*, U.S. authorities were not clear on whether this was the result of some sort of private intermediary with profit-based motives or if it was the result of a Chinese government effort to collect intelligence.

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 products.\(^50\)

The Vulnerability of Huawei Equipment and Technology

A report by the security services of the Dutch government aptly summarized the intelligence risks associated with using the telecommunications hardware and software of foreign providers.

“Computers and other equipment are often bought from a foreign country, because a foreign company has been awarded the tender. In addition, keeping complex hardware and software running is frequently left to the specialists of the company that has designed it or to a specialised third party. Due to the specialist knowledge that is required to produce and maintain these products, it is difficult for the organisation to keep a close eye on what is exactly happening in and on its own systems, and on who has access to specific information...Core interests could fall into the hands of another country in this way.”


“Even renowned companies, which have a good reputation as regards their protection against industrial espionage, cannot always or do not always want to offer protection against the activities of an intelligence service, for example because the company in question has been established by an intelligence service with the very objective of obtaining information in this way. Furthermore, a state may put pressure on a company located within its borders to cooperate with its intelligence service. Threats to refuse permits, charges for breaching national security or withholding lucrative government orders are instruments that companies can be extremely sensitive to...The bottom line is that there is a good chance that it is difficult for companies physically located abroad, no matter how reliable they tend to be, to refuse an ‘invitation’ to cooperate with their national intelligence service.”

51

The question of how susceptible Huawei’s equipment and technology is to Chinese hacking looms over the discussion about the material risk associated with doing business with the company. While Huawei argues that the lack of evidence of the company engaging in espionage or deliberately compromising its equipment should absolve them of risk, top experts firmly believe for some of the reasons described above that the inherent vulnerabilities in these systems together with the track record of the state on cybersecurity issues – as well as the way the state intervenes with Chinese enterprises – together constitute a major threat.

- In a Financial Times article, Robert Bebber, an information warfare officer at U.S. Cyber Command, commented on the risks associated with Huawei’s significant subsea fiber optic cable business, “Ownership in the undersea cable system, as well as leverage over its installation and maintenance, presents significant strategic opportunities for the People’s Republic of China.” He added that control over undersea cables could enable China to access nearly all communications traffic worldwide, including that of the U.S. military.

52

- Anthony Ferrante, a former advisor to President Obama on cybersecurity at the National Security Council, said “Network equipment is


a backdoor.” Managing the infrastructure provides a company direct access to whatever crosses through its system.  

During the aforementioned interview with the *Australian Financial Review*, Michael Hayden said, “I recognize the danger of implants and backdoors in telecommunications networks. [But] beyond that, just a foreign firm gaining the intimate knowledge they would get by helping build a telecommunications network is a sufficient ‘first-principles’ national security problem to give you serious pause before you even consider the presence of backdoors.”

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.”

When asked if he believed it was reasonable to assume that hard evidence exists showing that Huawei engaged in espionage on behalf of the Chinese state, Mr. Hayden answered, “Yes, that’s right. And, at a minimum, Huawei would have shared with the Chinese state intimate and extensive knowledge of the foreign telecommunications systems it is involved with. I think that goes without saying. That’s one reality.”

The perceived links between Huawei and the government are worrying given the intent of the state, not necessarily the company.

When certain observers question the level of concern about Huawei when there is so little hard evidence of actual espionage and compromised equipment, it is because of broad agreement within the international intelligence community that China is one of the leading state-sponsors of cyber-attacks and cyber-espionage for economic gain. The perceived links between Huawei and the government are worrying given the intent of the state, not necessarily the company.

---

Huawei as a “National Champion”

In another contradiction, despite Beijing’s denials of any undue influence over Huawei’s operations, the Chinese government has reportedly proclaimed the company as a “national champion.” This term has primarily been reserved for state-owned enterprises and used to describe companies used in a manner that shows “the fullest expression of state capitalism – the global face of China, Inc.” In other instances, “national champions” have been described as “…companies which help further the government’s strategic aims and in return, the government supports these companies by providing easier access to financing, giving preference in government contract bidding, and sometimes oligarchy or monopoly status in protected industries, giving these companies a number of advantages over their competitors. The [company’s] mission is to support China’s rise as a global super power.”

Again, per Michael Hayden,

“I understand the theory of Chinese state capitalism where the government classifies specific private companies as ‘national champions.’ Their success is strategically important to the state. It is well known Huawei falls into that camp.”

Although China reportedly provided government grants to Huawei in 2016 of $190 million (continuing a trend that saw the company receive some $228.2 million from the state between 2008 and 2011, according to earlier reports), the role of government support has been most prevalent in the state-backed financing provided for Huawei’s projects abroad. RWR research identified 32 cases since 2012 where Huawei projects were funded by Exim Bank of China ($2.8 billion) or China Development Bank ($7 billion). The Bank of China and the Industrial and Commercial Bank of China have also provided financing to Huawei, among a number of other smaller Chinese institutions.

These subsidies have been the subject of intense European Commission (EC) scrutiny and the topic of negotiations with Beijing. The EC pointed to credit lines from state banks that included a $30 billion loan facility provided by China Development Bank as an example of state support. In 2009, ZTE allegedly received credit lines of up to $25 billion from China Development

---

57 “We are the (National) Champions: Understanding the Mechanisms of State Capitalism in China. Li-Wen Lin and Curtis J. Milhaupt.
Bank and Exim Bank on revenues of just $8 billion, numbers out of sync with market norms. Although dated, research by Milhaupt and Zheng concluded that China Construction Bank provided financing to Huawei buyers totaling some 3.9 billion RMB (approximately $471 million) in 1998, a remarkable 45% of the total credit it extended that year.

In defense of these loans, Mr. Plummer argued, according to the Wall Street Journal, that “the government loans were given to foreign companies to help finance the purchase of Huawei products, not Huawei itself.” Although he also argued such support was for only a fraction of Huawei’s global sales, this distinction is unimportant in terms of establishing the government’s role in “championing” (read: subsidizing) the company and its international growth.

The reality is that the problem with Huawei’s receipt of subsidies from the Chinese state is not necessarily that it distorts markets and puts its competitors at an unfair disadvantage (which have long been legitimate complaints), but the evidence such support provides of the closeness between the company and the state.

It is this relationship that underscores the most consequential concerns in foreign markets about data security, cyber-espionage and the integrity of national networks.

Huawei’s Ties to High-Risk Countries

Based on RWR’s research from publicly available information, Huawei’s business transactions show a high concentration of activity in countries that are high on internationally recognized corruption indexes as well as those that are of low creditworthiness, according to the ratings of leading credit agencies. Below are visuals and statistics taken from RWR’s IntelTrak tool of the company’s footprints in these countries, based on transactions found in public reports since 2012.

---

61 “We are the (National) Champions: Understanding the Mechanisms of State Capitalism in China. Li-Wen Lin and Curtis J. Milhaupt.
Activity in High Corruption Risk Countries

The visuals below (from RWR’s IntelTrak tool) show that approximately 51% of Huawei’s transactions since 2012 (by value) have taken place in countries that score high on the corruption risk scale.

![Global Activity in Corruption Risk Countries by Value](image)

Activity in Low Creditworthy Countries

The visuals below – also from RWR’s IntelTrak tool – show that approximately 37% of Huawei’s transactions since 2012 (by value) have taken place in countries that are of low creditworthiness.

![Global Activity in Low Creditworthiness Countries by Value](image)
Recurring Risk Factors in Huawei Transactions

Beyond the fundamental cybersecurity questions raised above, Huawei’s specific business transactions have triggered important questions about the company’s trustworthiness and ability to deliver on the promises made to clients on performance and overall value proposition. Similar to above, much of the research below was compiled in the course of RWR’s maintenance of its online IntelTrak tool.

Concerns Associated with Espionage, Copyright Infringement, Intellectual Property Theft, and Cybersecurity

Below is a partial list of transactions or instances that saw Huawei partners and customers pulling back from the company over concerns about espionage risk and cyber threats.

- In 2008, Motorola, filed a lawsuit in the United States against Huawei for stealing and using its technology. After investigation, Motorola alleged Huawei not only used stolen technology, but had a scheme to steal additional specific information about a 3G base station called the SC300.63

- In 2010, Hibernia Networks announced it would build a transatlantic submarine cable network to be completed in 2013, linking Halifax, Nova Scotia to Slough, United Kingdom and Cork, Ireland. The contract stipulated that Huawei would be the main technology and deployment services provider. In January 2011, Hibernia received $250 million in financing from Huawei Marine Networks Co., Ltd.64 The total cost of the project was expected to be $300 million. In February 2013, Hibernia halted work on the project after becoming embroiled in rising tensions over the associated cyber threats.65 In 2014 the contract was cancelled, with TE SubCom taking over Huawei’s role. In September 2015, Hibernia Networks announced that the cable was ready for service, two years behind schedule.66

- In February 2011, the Committee on Foreign Investment in the United States (CFIUS) blocked Huawei from acquiring 3Leaf Systems. Huawei divested its assets in 3Leaf after CFIUS suggested the company do so voluntarily. Huawei initially acquired 3Leaf’s assets for $2 million in May 2010. It did not self-report the acquisition even though CFIUS had previously objected to Huawei’s involvement in the acquisition of 3Com in February 2008.67

64 “Huawei Marine Networks Finances Project Express Trans-Atlantic Cable.” Submarine Cable Networks. February 13, 2011.
In 2012, Symantec dissolved its joint venture with Huawei after four years of cooperation developing computer network security products. It has been reported that Symantec ended the venture over concerns its involvement with Huawei would prevent the company from obtaining U.S.-supplied warnings about cyber threats.68

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.69

Huawei contracted to build a $100 million communications cable between Sydney and Auckland. The project was supposed to be completed by 2013, however, in March 2012, it was announced that the Australian government was investigating Huawei over another proposed cable between Perth and Singapore. The investigation examined security and cyber concerns on national security grounds. This ultimately led to both deals being blocked.70

The 2012 employment of Huawei by India’s Bharat Sanchar Nigam Limited (BSNL) to modernize its national communications network, which in two phases replaced 4 million telephone lines, was criticized due to perceived cybersecurity threats. In February 2014, Huawei’s engineers were blamed for the hacking of a mobile tower in Andhra Pradesh.71 Both BSNL and the Indian Parliament are investigating the incident, although this has not stopped the network upgrade.72

In 2012, Huawei was banned by the Australian government from bidding for state tenders due to security concerns. The decision was upheld in 2013 after a change of government.73 In October 2016, the government infrastructure minister Paul Fletcher was challenged after a Huawei smartwatch was listed as a gift on his declaration of interests. There was concern about the smartwatch’s connection to the parliamentary network, which manages extremely sensitive information.74

---

72 "BSNL starts migration to IP-based Huawei NGN switches to reduce Opex." Telecom Lead. February 14, 2014.
after he admitted he had not disclosed a visit to China with Huawei. Liberal MP Steve Ciobo also failed to disclose that he participated in the Huawei sponsored visit.\textsuperscript{75}

- In 2012, Canada's National Surveillance and Cryptology Agency banned Huawei from bidding on a major telecommunication project in Ottawa. The Assistant Director of Intelligence argued that the ban was used to protect significant and long lasting Canadian infrastructure from Huawei espionage.\textsuperscript{26}

- In October 2012, the Canadian government invoked its national security exception, which allowed it to “discriminate without violating international trade obligations, against companies it deems to be too risky” to exclude Huawei from helping to build the government communications network.\textsuperscript{77} Two separate Canadian government memoranda from the Department of Public Safety (which oversees Canada’s spy agency, CSIS) outlined security concerns about Huawei.\textsuperscript{78} Later, in 2016, Canada rejected the immigration applications of two Chinese employees from Huawei, on the basis of espionage concerns surrounding the firm.\textsuperscript{79}

- In May 2013, it was announced that Huawei was under investigation by Indian intelligence agencies. According to a 2010 report, titled “Shadows in the Cloud: Investigating Cyber Espionage 2.0”\textsuperscript{80}, a Chinese “spy ring” had stolen more than 700 documents from India’s Ministry of Defense.\textsuperscript{81} The resulting elevated security concerns led Indian officials to ban telecommunications providers from importing Chinese manufactured components from companies, including Huawei and ZTE.\textsuperscript{82}

- In the summer of 2013, controversy erupted in Denmark over a contract awarded to Huawei to service the IT network of the country. The Danish Defence Intelligence Service (DDIS) warned against the entrance of such Chinese telecom companies into the country’s critical infrastructure.\textsuperscript{83} That opposition was reversed after a deal was reached to permit the country’s Center for Cyber Security (CFCS) to monitor Huawei’s work, only allow individuals with security clearances into the Network Operation Center (NOC), and ensure that all to-be installed Huawei hardware be screened by “The Cell,” as the Danish refer to the mechanism set up in the UK to vet Huawei equipment.

\textsuperscript{75} “State Edition MPs’ lap of honour Pollies holiday before retiring.” Sunday Mail (South Australia). May 19, 2013.
\textsuperscript{77} “Huawei Faces Exclusion from Planned Canada Government Network.” Reuters. October 9, 2012.
\textsuperscript{78} “Huawei Makes Canada Nervous Too.” Motherboard. September 2, 2014.
\textsuperscript{79} “Canada Cites Espionage Risk from Two Huawei Employees, Saying it Plans to Reject Their Immigration Applications.” South China Morning Post. May 4, 2016.
\textsuperscript{81} “China Denies Hacking Indian Defence Documents.” Information Age. April 6, 2010.
\textsuperscript{82} “India Bans Chinese Network Equipment.” Information Age. April 30, 2010.
\textsuperscript{83} “China’s Overseas Investment In Critical Infrastructure.” DIIS Report 2016.
In November 2008, Japanese SoftBank Mobile selected Huawei as the primary supplier of its LTE mobile devices. Huawei has been marked as a cybersecurity risk to US companies because of alleged ties to the Chinese military, which complicated SoftBank’s acquisition of 80 percent of Sprint in 2013. As a condition to approving the acquisition of Sprint, the US government maintained the right to approve equipment vendors to the company. As a result, SoftBank and Sprint had to agree not to integrate Huawei equipment into U.S. operations.

In December 2013, Huawei won a contract to construct a 4G LTE network for South Korea’s LG Uplus (U+). The $232 million contract raised concerns for the U.S. Congress, which opposed the plans due to the risk it could present to the U.S. military presence in the country.

In August 2014, Taiwan’s Hon Hai pulled out of its contract with Huawei to provide 4G equipment after the Taiwanese government warned that Huawei’s involvement posed a national security threat. They argued that the deal, worth $178 million, would enable cyber espionage against the country.

In October 2014, Huawei signed an agreement with the Washington Redskins to become an official sponsor and technology partner for an undisclosed amount. The technological partnership meant Huawei would provide a Wi-Fi network at the 85,000-seat FedEx Field. In December 2014, the project was cancelled amid claims that the US government highlighted cyber security concerns of having a Huawei managed network.

In 2014, Huawei was accused of hacking into Indian state-run telecommunications systems, an allegation that Huawei denied.

In July 2015, the Indian Home Ministry approved a Huawei project to set up an electronics and telecommunications device manufacturing factory in Sripurumbudur. Cybersecurity concerns

---

86 "Korea deal sees Huawei back in U.S. sights; A HK$1.8b agreement with LG unit prompts warning from lawmakers in Washington that security ties with Seoul could be threatened." Bien Perez. South China Morning Post. December 5, 2013.
87 "U.S. concern over Huawei telecoms deal with South Korea." Reuters. December 4, 2013.
led the Indian government to issue various amendments to the contract, such as requiring Indian nationals fill critical positions at the factory.\footnote{"MHA clears Huawei’s proposal for manufacturing unit in Tamil Nadu." Economic Times of India. July 15, 2015.}

- In November 2015, State Grid Corporation of China (SGCC) and the Macquarie Group, Ltd. emerged as frontrunners to lease the fifth largest optical fiber network in \textit{Australia}, TransGrid from the New South Wales government.\footnote{"ACCC ticks off China deal with TransGrid as OK.” Australian Financial Review. October 26, 2015.} SGCC had agreed to use Huawei technology, which raised concerns about potential cyber-espionage. Concerns emerging about SGCC’s ties to the PLA– and Huawei, specifically – ultimately played a role in the deal’s collapse.\footnote{"NSW:Aust-led group wins NSW electricity lease." AAP Newsfeed. November 25, 2015.}

- In 2016, Huawei entered discussion with \textit{South Korea} regarding the installation of a 5G network throughout the country. This came following a 2014 agreement between Huawei and SK Telecom to supply wireless equipment for South Korea’s 4G network that was never consummated. The 5G plans were again opposed by members of the U.S. Congress.\footnote{“Senators Fear Chinese Role in Telecom of South Korea; Biden is Asked to Warn Seoul of Security Threat if Huawei Builds Network.” International New York Times. December 5, 2013.}

- In February 2016, Huawei and the Spanish National Institute of Cyber Security (INCIBE) signed a Memorandum of Understanding (MoU) outlining the promotion of cyber security collaboration in \textit{Spain}. This MoU established a collaboration scenario promoting best practices and information exchanges regarding cyber security actions and protection measures. This was the first such agreement of its type signed by Huawei in a European country and was to provide Huawei with knowledge of Spain’s cyber landscape.\footnote{“Huawei Spain, Spanish National Institute of Cyber Security Sign a Memorandum of Understanding for Development of Cyber Security.” South China Morning Post. February 26, 2016.} Some have argued it will leave Spain vulnerable to cyber threats.\footnote{"China’s ghost in Europe’s telecom machine.” POLITICO. December 11, 2017.}

- In August 2016, AT&T announced that it would be exploring the joint development of international 5G standards with a group of international telecommunications companies, including China Mobile and Huawei. On September 13, 2016, it was reported that the Federal Bureau of Investigation (FBI) and National Security Agency (NSA) were launching a formal review of Huawei, following AT&T’s announcement to examine the national security implications of Huawei constructing telecommunications networks in the \textit{United States}.\footnote{“U.S. Spies Think China Wants to Read Your E-Mail.” Eli Lake. Bloomberg. September 13, 2016.}

- On March 28, 2017, \textit{South Korea}’s largest telecommunications provider, SK Telecom, announced that it is reviewing an offer from Huawei among other bidders to procure equipment for the company’s new base transceiver stations. SK Telecom, however, is facing pressure from
conservative policy-makers in Seoul to remove Huawei from consideration due to cybersecurity concerns.\(^9\)

- In August 2017, a Huawei network equipment distributor in Seoul, Hyundai Information Technology, won a $6.19 million bid to supply telecommunications equipment to Seoul's metropolitan subway system. It was awarded the contract, as it was able to significantly undercut the competitor's price evaluations in the final bid. Skepticism has been raised about the bidding process and the "complacency" of authorities toward expanding Chinese business in South Korea. The system will also be able to connect to other transportation systems, raising questions about Huawei' control over critical infrastructure.\(^10\)

- Huawei's 2017 announcement, that it had entered a partnership with Global Switch led to the government of Australia terminating its relationship with Global Switch's Australian data center over security concerns. The files will be moved to a government-owned hub in 2020, with associated costs for the Australian government estimated at $200 million.\(^11\)

- In January 2018, AT&T reportedly walked away from a partnering arrangement with Huawei to sell its phones in the United States just prior to an important Huawei appearance at the CES conference in Las Vegas. The decision may have been influenced by a letter sent by Members of Congress to the Federal Communications Commission in December 2017 that, in the words of the New York Times, which reviewed the document, expressed "misgivings about a potential deal between Huawei and an unnamed American telecommunications company to sell its consumer products in the United States. [The letter] cited longstanding concerns among some lawmakers about what they said were Huawei’s ties to the Chinese government."\(^12\)

- Later in January 2018, reports emerged that Verizon had similarly dropped plans to partner with Huawei and sell its handsets in the United States, which, according to sources cited by Bloomberg, was also speculated to be the result of pressure from the U.S. government.\(^13\)

---

Accusations of Reneging on Contractual Obligations, Cost Inflation, Intellectual Property Theft and other Unethical Activity

While many transactions shown in this report relate to the cyber threat associated with Huawei’s activities, other problems with the company’s behavior and value proposition have also been prevalent in the company’s foreign transactions.

Although Huawei is often seen as a cheap alternative to their competitors, their reputation for low prices is not always deserved. First, these prices are usually greatly facilitated by state-backed financing. They also have a track record of exploiting situations with corrupt regimes to inflate prices and increase profits. This is especially prevalent in developing regions, where customers are choosing Huawei due to their low-cost reputation, rather than properly assessing the risk.

- In October 2009, Entel Bolivia signed a $120 million contract with Huawei to implement the construction of telecommunications infrastructure and supply services that would provide 1.5 million people in rural Bolivia with telephone service. In December 2010, Huawei was declared non-compliant in the fulfillment of the contract and fined $8 million by the Bolivian government.  

- 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. According to workers, the state-owned utility could have breached government procurement laws in awarding Huawei the tender. 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, and the Exim Bank of China took over funding. TelOne took over the construction of the project.

- In 2006, Huawei was contracted by the Ugandan government to construct a telecommunications backbone network. The construction was expected to last 27 months and cost $55 million. Instead, the project faced a number of delays and had a cost increase of $7

---

million. It was completed well behind schedule in October 2011.\footnote{107} In 2012, the government ordered an investigation into the project over claims of inflated prices and the use of inferior equipment. Further, the rising cost necessitated another loan, which Ugandan President Museveni asked Premier Ruhakana Rugunda to block. The Ugandan also noted Rwanda had 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.\footnote{108} Concerns were also expressed over the security of the network, which is used by five ministries including those of defense and foreign affairs.

- In December 2012, Huawei was awarded a contract to deliver service management and operations of telecommunications company Three’s core network in the United Kingdom under a 5-year, $192 million contract.\footnote{109} 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.\footnote{110}

- In 2013, Telecom Namibia purchased a billing system from Huawei against the advice of its employees. The equipment was purchased at around $7.1 million, over three times its estimated cost. The equipment proved to be faulty. The state-owned Telecom Namibia reportedly employed a questionable consultant to oversee the tender process, leading to Huawei being awarded the contract.\footnote{111} Huawei subsequently requested additional servers for the system, costing Telecom Namibia an additional $2.3 million. The equipment began servicing some 15,000 employees in November 2013, but was still not functioning properly.\footnote{112}

- In January 2014, 9Mobile (Etisalat Nigeria) and Huawei entered a partnership to improve information technology and telecommunications services offerings. Under the arrangement, Huawei was responsible for the operational management of 9Mobile’s IT services across technical infrastructure, application management and user support.\footnote{113} In July 2017, 100 Nigerian Huawei workers were fired overnight.\footnote{114} The lack of due process triggered political opposition to the move as well as protests by workers and the local community.\footnote{115}

- In March 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.\footnote{116} Mustek was selected for its expertise in logistics and, as part of the contract, to deliver the equipment.

\footnotesize
\begin{itemize}
\item \footnote{107} "Huawei delivers Uganda fiber Internet backbone." New Vision. October 10, 2011.
\item \footnote{108} "Uganda orders probe into Huawei’s fiber project." ZD Net. October 3, 2012.
\item \footnote{109} "Huawei wins Three network deal." Financial Times. December 9, 2012.
\item \footnote{110} "Huawei Loses Key Contract in £20m Blow." The Daily Mail. October 30, 2014.
\item \footnote{111} "Namibia; Telecom Ignored Workers On System." Africa News. September 2, 2014.
\item \footnote{113} "Etisalat, Huawei Ink Outsourcing Deal." Communications Week. January 2, 2014.
\item \footnote{114} "100 Nigerian Engineers Sacked in Etisalat Crisis." IT News Africa. July 20, 2017.
\item \footnote{115} "Over 100 workers sacked as Etisalat Nigeria rebrands." TV360. July 21, 2017.
\item \footnote{116} "Mustek in R128m Huawei deal." Tech Central. March 7, 2014.
\end{itemize}
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.

In May 2017, at least 12 former Huawei employees in South Africa were arrested after they – and some 200 other protesters – blocked the streets over a sudden termination they claimed they received by text message. The arrests followed police officers firing rubber bullets and lobbing stun grenades to disperse the crowd of upset former employees. The workers refused to leave until the company addressed them.

In September 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.

In March 2015, an audit of Uganda’s National Backbone Infrastructure (NBI) and Electronic Government Infrastructure (EGI) projects under Huawei recommended the projects be canceled due to cost overruns and price gouging. Huawei was originally awarded a contract in 2006 after the Ugandan government procured a $106 million loan from China to lay 211 km of optical fiber cable linking government offices. Initially, the four phases of the project were to only take 27 months, but only the first phase was finished by 2013. Early in 2015, Huawei sought an additional loan for the third phase when a second report recommending the contract be canceled was released. This second audit noted the contract was $41 million over budget.

Uganda’s government has yet to make a decision on the recommendation.

In November 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

---

119 "Zain South Sudan partners with Huawei and UNESCO to power Internet connectivity for schools." UNESCO. September 5, 2014.
121 "Govt may cancel Shs300b Internet deal to China firm." The Daily Monitor. March 8, 2015.
122 "Uganda’s USD $100 million Fibre Optic Project Halted by President." PC Tech Mag. January 4, 2015.
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.123

- In May 2017, Huawei was found guilty of stealing T-Mobile technology. An American court ordered Huawei to pay T-Mobile $4.8 million. The lawsuit which focused on events in 2012 and 2013, found that Huawei employees spied on T-Mobile’s smartphone testing robot, and used the information to improve their own version.124 In this instance, Huawei employees visiting T-Mobile’s lab reportedly photographed the robot and stole one of its “fingertips.”125

Allegations of Bribery and Corruption

Huawei’s Commitment to sustainability on its website points to the company’s signature at the World Economic Forum in January 2017 to the Compact for Responsive and Responsible Leadership. The company states,

“We will ensure that our company's strategic goals are aligned with the long-term goals of society as a whole. We are committed to sustainable value creation and will not sacrifice long-term economic prosperity and social welfare for our own short-term interests.”126

Below is a list of transactions afflicted with allegations of bribery, corruption and manipulation of local political processes.

- In June 2012, Algeria banned Huawei and ZTE from participating in any public tender ventures in the country for two years after a bribery scandal surfaced involving two ZTE employees and a Huawei staffer who allegedly gave $10 million in bribes to a former executive of the state-owned Algeria Telecom, Mohamed Bukhari, from 2003 to 2006. According to local Algerian reports, this was the first time the country had ever banned companies from their public tender process.127 In 2012, executives of the Chinese firms were sentenced in absentia to 10-year prison terms over these allegations.

- In August 2013, Huawei was awarded a $27 million contract by the Gauteng Department of Finance (GDF) in South Africa to provide 88,000 10-inch tablets for their new e-learning project in the Gauteng province.128 In October 2014, Huawei and a local internet services provider, CloudSeed, were being investigated for corruption and contract manipulation. The auditor general of GDF stated that the contracts were awarded “on points,” and it appeared that

---

contract stipulations were manipulated by the companies to increase their chances of winning. It was also deemed unusual that the company’s' services were not obtained through the State Information Technology Agency, which normally handles these kinds of deals.\textsuperscript{129}

- In September 2013, Huawei began implementing the $124.7 million Islamabad Safe City Project in Pakistan. Initially approved in 2009 and financed with the assistance of a $68 million short-term loan from the Exim Bank of China, the project would install 1,500 security cameras linked to an online security system and CCTV and a designated security force equipped with new vehicles and Chinese weapons. The security system was scheduled to be fully installed by the end of 2015. After finalizing the agreement, it was criticized for being overpriced, leading to a renegotiation of terms with Huawei (after intervention from the Supreme Court).\textsuperscript{130} The project was also completed two years later than expected. 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.\textsuperscript{131} In October 2016, however, the project was inaugurated, around a year behind schedule.\textsuperscript{132}

- In January 2014, Nigeria’s Ministry of Telecommunications announced that the National Rural Telephone Project (NRTP) would commence in April. Originally, the project was awarded to Huawei and ZTE Corporation for $200 million. These companies, however, only managed to build local exchanges, reportedly failing to meet their contractual obligations. As a result, the project was canceled and given to five new companies.\textsuperscript{133}

In defending the company against its critics, an official statement in August 2017, stated “As a global business entity, Huawei does not involve itself in politics. Huawei forbids all of its global subsidiaries from making any form of political donation, including in places where this practice is legal.”\textsuperscript{134}

- In 2012, however, 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 through the Social Democratic Administration of President Mahama.\textsuperscript{135} Various invoices have been uncovered, which show that Huawei materially supported the political party after the tax incentive was granted.\textsuperscript{136}

\begin{itemize}
  \item \textsuperscript{129} “Huawei responds to reports that Gauteng school tablet tender is being investigated.” htxt.africa. October 29, 2014.
  \item \textsuperscript{130} “Islamabad Safe City Project Goes Ahead.” Daily Capital. March 30, 2015.
  \item \textsuperscript{131} “Govt paying markup on $124m loan since 2011.” Imran Mukhtar. The Nation. September 18, 2013.
  \item \textsuperscript{132} “Punjab Safe City Project inaugurated.” Dawn (Pakistan). October 12, 2016.
  \item \textsuperscript{133} “Nigeria Hints At Reviving Rural Telephony Project.” Ventures Africa. January 22, 2014.
  \item \textsuperscript{135} “Ghana; Chinese Coy Granted $47 Million Tax Exemption Aiding NDC Campaign.” Africa News. October 17, 2012.
  \item \textsuperscript{136} “Huawei Technologies to implement e-government project in Ghana.” Human IPO. March 18, 2013.
\end{itemize}
In 2017, the **Solomon Islands** government abruptly switched a submarine fiber optic cable contract from a favored British-American contractor (already vetted by the Asian Development Bank that was backing the project) to a subsidiary of Huawei. The project was to lay a 4,500-km cable connecting Sydney to Honiara, bringing reliable internet to the country. The contract 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. More specifically, it is alleged that Huawei promised the Prime Minister these funds in exchange for award of the contract. An Australian committee report wrote,

“\[If true, this is a corrupt and criminal offence and the committee calls on the [Royal Solomon Islands Police] to conduct an urgent investigation into this...The committee is of the view that this is the main reason for the government to bypass procurement requirements in favour of the company Huawei.\]^139

Robert Bebber, an information warfare officer at U.S. Cyber Command described the threat, “Ownership in the undersea cable system, as well as leverage over its installation and maintenance, presents significant strategic opportunities for the People’s Republic of China.” He indicated control over the cable would allow China to access communications traffic, including that of the US military, as well as to disrupt communications. In January 2018, Australis denied landing rights for the Huawei-led project, committing to fund it independently using more trusted contractors.

It has also been reported in **Czech** news that Huawei supplied mobile phone devices to the staff of President Zeman in the Prague Castle worth approximately $100,000, reportedly in exchange for special advertisements and favorable rental access to the Castle for special events. This “barter” arrangement, as it has been described, has been going on since 2013, with nearly 400 mobile devices received for staff during this time. In exchange for these devices, the Castle provided an advertisement campaign for Huawei and supplied hundreds of free tickets for events and Castle tours. The Castle has argued that the value of what has been provided to Huawei is equal to what Huawei provided to the Castle. The Castle spokesman said, “The Prague Castle management received 390 mobile devices since 2014. The devices were used for its own needs, or they have been provided as a service to the President of the Republic Office, which complies with its (The Castle management) status.” It was pointed out that, with some

---

353 employees at the Castle as of April 2017, there was at least one Huawei device for each employee (when including gardeners, ticket sales assistants, Directors, etc.)

Chinese companies have established a notoriously close connection with the newly elected Czech president, with the Chairman of CEFC China Energy, Ye Jianming, serving as a formal economic advisor.

- Huawei was also accused of bribery within China. The Vice President of the Huawei Consumer Business Group in the Greater China Region (responsible for China, Macao and Hong Kong) was detained for bribery in December 2017. In 2014, China’s Caixin reported that 116 employees at Huawei had accepted or solicited bribes (mainly in the form of kickbacks). Another source cited by Telworld indicated that different departments at Huawei have had significant corruption problems, including at the research and development, procurement and sales divisions.

In January 2018, the company reportedly put in place a self-imposed fine on top executives – including the Chairman, Ren Zhengfei – for management oversight problems with regard to quality control. Mr. Ren was fined some $469,000. The fines were disclosed in a leaked internal company memo that admitted to “quality breach and business falsification.” The incidents driving the penalties were uncovered by an internal audit, with the decision motivated by Mr. Ren as a means to “encourage the management team to reflect on past management and decision-making gaps.”

### Huawei’s Future Goals

Some 63 percent of the company’s $33.2 billion in global revenue in 2016 came from selling telecommunications network equipment to manage mission-critical industrial operations (so-called operational technology). According to Huawei, it seeks to be one of the top five largest cloud networks in the world and has already won more than 300 contracts from global telecom operators and other industry customers to deploy All-Cloud

---

Among the company’s other stated goals are working with European policy makers on 5G, becoming the leader in the global mobile phone market by 2021\textsuperscript{147} and seeking to increase positive brand awareness at a rate of some 30\% per year overseas.\textsuperscript{148}

The risk factors described above create headwinds for each of these objectives, despite the company’s successful growth internationally thus far. Still, it seems the company’s greatest exposure from the point of view of cybersecurity concerns, lack of transparency and methods of doing business lie in its operational technology business or its core area of network equipment solutions.

With a reputation that does not appear to be on its way to rehabilitation and a government that is tightening control – including with regard to the internet, intrusiveness into the personal data of its population (and the client base of its leading tech companies, including Huawei) gaining enough traction in these market segments to keep up with the company’s internal expectations could be more difficult than it anticipates. This situation is not helped by the insertion of more influential Communist Party layers into the governance structures of its leading companies, including those in the supposed private sector.

Even if Huawei’s equipment and software does not have intentional back door access, the ability for other actors to access its systems shows some complacency at Huawei in providing sufficient security.

At best, Huawei seems ignorant to the company it keeps, rather than complicit in their indiscretions. At worst, the company is compromised by the Chinese state intelligence services. While the truth is probably somewhere in between, neither scenario is attractive for prospective partners and customers.


\textsuperscript{147} “Huawei plans to be global smartphone leader in five years. Sounds reasonable.” ZDNet. June 9, 2016.

\textsuperscript{148} “Chinese Telecommunications Giant Huawei- Strategies To Success.” Nanyang Technical University. 2015.
This document is intended for general informational purposes. RWR disclaims, to the fullest extent permitted by applicable law, any and all liability for the accuracy and completeness of the information in this document and for any acts or omissions made based on such information. RWR does not provide legal, regulatory, audit, or tax advice. Readers are responsible for obtaining such advice from their own legal counsel or other licensed professionals.

This publication is designed to provide accurate and authoritative information in relation to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering any form of professional or other advice or services. No person should rely on the contents of this publication without first obtaining advice from a qualified professional person.