RWR Advisory Group

May 2019

ASSESSING HUAWEI RISK

How the Track Record of the CCP Should Play into the Due Diligence of Huawei's Partners and Customers

Introduction

Despite the discomfort that may exist around drawing sweeping conclusions about Chinese companies, the primary risk involved in doing business with Huawei – and certain other Chinese technology firms – is that they operate under the jurisdiction of an authoritarian Chinese government that has an abysmal track record in the cyber domain. Indeed, the Chinese government's track record in this domain is marked by repeated, credible and well-documented cases of using cyber-espionage and hacking to steal intellectual property and to advance the global, strategic interests of the Chinese Communist Party.

Accordingly, although Huawei has been assertive in trying to defend its reputation from allegations that its equipment and technology could be used for malevolent purposes, the track record they are defending is arguably the wrong one. Ultimately, although Huawei has its own history of abuses to reckon with on these same topics, it is not the company specifically that foreign officials and security experts should be – and in many cases are – most concerned about. It is the long and established behavioral pattern of cyber abuses committed by the Chinese government and their use of corporate entities to carry out this activity.

Huawei Risk is China Risk

Unfortunately for Huawei, addressing the concerns of their critics requires significantly more than demonstrating, in technical terms, that their hardware and software is free of backdoors or malware. Rather, Huawei will have to persuade risk managers that:

1) the Chinese government does not aggressively use cyber means to engage in espionage, including corporate espionage and intellectual property theft; and

2) that Huawei would not be responsive to the Chinese government if instructed to assist with their cyber-related operations.

Secondarily, some – not all – of these same risk or threat managers around the world contracting for information and communications technology (ICT) have a mandate to consider more than just the economic and data security consequences of falling victim to Chinese cyber intrusions. Some governments and companies also place importance on whether, by integrating the ICT solutions of Huawei or other Chinese technology companies, they are enabling the advancement of China's strategic objectives at the expense of their own, and even making themselves susceptible to coercion and influence on topics fundamental to their core principles and values.

For liberal democracies that value their form of governance, free markets, intellectual property human rights, press freedom, and free speech, opening up one's information network to an entity that is beholden to a Chinese government with very different views on these core principles should raise red flags. These red flags signal non-monetary costs that should properly be appended to any strictly financial figures being calculated in ICT procurement or partnering decisions.

"Some governments and companies also place importance on whether, by integrating the ICT solutions of Huawei or other Chinese technology companies, they are…making themselves susceptible to coercion and influence on topics fundamental to their core principles and values."

"For liberal democracies that value their form of governance…opening up one's information network to an entity that is beholden to a Chinese government with very different views on these core principles should raise red flags."

This risk was emphasized in a report, entitled, "Authoritarians Advance," published by the Mercator Institute for China Studies (MERICS) and the Global Public Policy Institute, which noted,

> "…China's political model is based on an authoritarian regime intent on strengthening a deeply illiberal surveillance state at home while also exporting – or at least trying to popularize – its political and economic development model abroad."[1]

"…the repressive values of authoritarian systems – which encourage top-down authority, censorship, and the monopolization of power – are projected outward."

The sentiment was also expressed by Chris Walker of the National Endowment for Democracy, who observed,

> "Through [the use of] sharp power, the repressive values of authoritarian systems – which encourage top-down authority, censorship, and the monopolization of power – are projected outward."

Identifying and Evaluating the Ultimate Risk/Threat Actor

In the end, when dealing with Huawei and other Chinese technology entities, the companies themselves are not the ultimate and only threat actors behind efforts to steal information and compromise foreign companies and countries in the cyber domain. They are not the ultimate and only threat actors seeking to advance Chinese Communist Party (CCP) leadership, influence and illiberal governing principles on the world stage, including a vision for how the internet and state surveillance should operate. The Chinese government is the primary concern in these areas, often using companies as their vehicles.

"It is the CCP that is behind this [abusive cyber] behavior, often using companies as their vehicles…and their track record of abuses on these issues is available to those performing their diligence."

Accordingly, it is the CCP's track record of abuses and governance system for controlling Chinese entities and persons, including private sector companies, that is relevant in the analysis of risk. This track record is available to those performing their diligence – and is summarized in this report.

[1] "Authoritarian Advance: Responding to China's Growing Political Influence." Mercator Institute for China Studies. February 2018.

The Components of the Risk

In the case of Huawei, to believe that even a clean track record or lack of technical vulnerabilities (neither of which is in evidence) can mitigate exposure to cybersecurity risk – when there is broad, international agreement that the Chinese government is a notoriously bad actor on these issues – requires risk managers to subscribe to the following beliefs:

1) that China does not have a worrisome track record in the cyber domain on state-sponsored corporate/economic espionage, intellectual property theft, surveillance, censorship and other areas of cyber concern;

2) that China's technology companies do not have to obey the orders of the Chinese government (i.e., the CCP);

3) that the strategic objectives outlined above to project the values and core principles of the CCP do not accurately reflect the global aspirations of the Chinese government; and

4) that China does not use the leverage it has in the economic domain for coercion or to exert unwanted influence on the political positions of other countries, and that it will not use the dependencies gained through a subsidized, low-cost position in another country's ICT infrastructure for this same purpose.

This report uses public information to spell out why each of these statements are refuted by the evidence, interspersing into each of the four sections that cover these topics how they relate specifically to Huawei.

For those countries and stakeholders that are not deterred by the four categories of risk described above or that believe the benefits of cheap, capable ICT equipment and services are worth the risks documented in this report: with eyes wide open, they move forward hoping that what China has done in the past is simply not a reflection of what they will do in the future.

If they are wrong, the risks are more significant and broader in scope than they have ever been before. The urgency that is evident in the debate taking place on 5G is not just due to some new U.S.-led anxiety about the rise of China. 5G will ultimately –

For those countries and stakeholders that are not persuaded by the four conclusions above or that believe the benefits of cheap, capable ICT equipment and services are worth the risks documented in this report: with eyes wide open, they move forward hoping that what China has said and done in the past is simply not a reflection of what they will do in the future.

"If the growing connectivity is due to Chinese financial largesse … foreign leaders could become politically dependent on the continuation of that assistance, just as countries in Europe have been vulnerable to the whims of Russian pricing on natural gas."

for those positioned to capitalize on it – connect to the internet all facets of daily life, including medical devices, automobiles, appliances, homes, and security cameras. A compromised system not only puts personal data and intellectual property at risk on an unprecedented scale, but also human lives.

Even for governments that do not see China's track record on intellectual property and hacking to be a problem – or who view its governance practices and values to be benign – there are other categories of risk to consider.

Low-Cost Technology Trap Diplomacy

As populations in the developing world gain access to improved internet services, any roll-back in their newfound connectivity will be deeply unpopular. If their growing connectivity is due to Chinese financial largesse – i.e., due to subsidized prices or low-interest export financing – foreign leaders could become politically dependent on the continuation of that assistance, just as countries in Central and Eastern Europe have been dependent on the whims of Russian pricing on natural gas. Rather than "debt trap diplomacy," accepting subsidized Chinese ICT solutions introduces the prospect of "low-cost technology trap diplomacy."

A scenario of actual or perceived dependency opens the door to pressure not to offend, including on issues such as disputed territorial claims, criminal prosecutions (such as allegations of bribery and corruption), votes at the United Nations, human rights, press freedom, censorship, and other hot button topics, such as Tibet and the plight of the Uighurs in Xinjiang.

Rather than "debt trap diplomacy," accepting subsidized Chinese ICT solutions introduces the prospect of "low-cost technology trap diplomacy."

Just as foreign governments, when taking positions on issues of strategic importance to China, already have to factor in their interest in preserving access to the Chinese market, so too will governments have to consider the risk of losing access to low-cost ICT equipment and services and underperforming on the rising expectations of their citizens.

These potential risk factors go beyond the traditional national security concerns usually attributed to the United States. In a way that has broader relevance to the stability and independent decision-making ability of world leaders, these issues present risk factors that have national consequences.

1) China's Track Record on Cyber-Espionage, Economic Espionage and Intellectual Property Theft

In Coordination with 11 Other Countries, U.S. Government Alleges Chinese Government's Complicity in Hacking Campaign and Intellectual Property Theft, December 2018

In December 2018, in a sweeping set of official statements from the U.S. Department of Justice, operating in coordination with eleven other countries (including the United Kingdom, Japan, Germany, France, Canada, Brazil, Finland, India, Sweden, Switzerland and the United Arab Emirates), two Chinese nationals working for a Chinese company were charged with being complicit in a global hacking scheme to steal business secrets at the direction of the Chinese government.[2]

The individuals were alleged to be part of a group referred to as Advanced Persistent Threat 10 (APT 10) and, in coordination with China's Ministry of State Security, were accused of hacking more than 45 companies in the U.S. and elsewhere.[3]

According to the indictment, one of the charged individuals worked for a company, Huaying Haitai Science and Technology Development Company, demonstrating the willingness of Chinese security services to use a corporate vehicle to carry out cyber espionage and hacking. The indictment alleges the two Chinese nationals engaged in technology theft that began in 2006 and efforts steal intellectual property and other

"…in a sweeping set of official statements from the U.S. Department of Justice, operating in coordination with eleven other countries…two Chinese nationals working for a Chinese company were charged with being complicit in a global hacking scheme to steal business secrets at the direction of the Chinese government."

[2] "Deputy Attorney General Rod J. Rosenstein Announces Charges Against Chinese Hackers." The United States Department of Justice. December 20, 2018.

[3] "Deputy Attorney General Rod J. Rosenstein Announces Charges Against Chinese Hackers." The United States Department of Justice. December 20, 2018.

data from remote-access client-management companies starting in 2014. The targeted companies were from at least 12 different countries.[4]

This was not a U.S.-alone operation. When the indictment was announced several other countries made simultaneous statements of support, including with regard to the complicity of the Chinese government working collaboratively with these nationals under the cover of a corporate entity.

- "Along with its allies, the UK has announced that a group known as APT 10 acted on behalf of the Chinese Ministry of State Security to carry out a malicious cyber campaign targeting intellectual property and sensitive commercial data in Europe, Asia and the US."[5]

  The United Kingdom Foreign and Commonwealth Office

- "The Government Communications Security Bureau (GCSB) has established links between the Chinese Ministry of State Security (MSS) and a global campaign of cyber-enabled commercial intellectual property theft."[6]

  The New Zealand National Cyber Security Center

- "Today, the Australian Government joins other international partners in expressing serious concern about a global campaign of cyber-enabled commercial intellectual property theft by a group known as APT10, acting on behalf of the Chinese Ministry of State Security."[7]

  Australia's Minister for Foreign Affairs Marise Payne

- "Today, many of Canada's allies and partners have made statements concerning the compromise of several Managed Service Providers. CSE also assesses that it is almost certain that actors likely associated with the People's Republic of China (PRC) Ministry of State Security (MSS) are responsible for the compromise of several Managed Service Providers (MSP), beginning as early as 2016."[8]

  Canadian Communications Security Establishment

- "In this context, from December 20 to 21, the United Kingdom, the United States and other countries issued a statement on a group conducting cyberattacks based in China known as APT10. Japan has, with deep concern, been paying close attention to these attacks by APT10 which threaten the security of cyberspace, and strongly supports the determination

---

[4] "Deputy Attorney General Rod J. Rosenstein Announces Charges Against Chinese Hackers." The United States Department of Justice. December 20, 2018.

[5] "UK and allies reveal global scale of Chinese cyber campaign." UK Foreign & Commonwealth Office and UK National Security Centre. December 20, 2018.

[6] "Cyber campaign attributed to China." New Zealand National Cyber Security Centre. December 21, 2018.

[7] "Attribution of Chinese cyber-enabled commercial intellectual property theft." Australian Minister of Foreign Affairs. December 21, 2018.

[8] "Canada and Allies Identify China as Responsible for Cyber-Compromise." Canada Communications Security Establishment. December 20, 2018.

of the United Kingdom, the United States and other countries to uphold the rules-based international order in cyberspace."[9]

Japan's Ministry for Foreign Affairs

- "[Denmark] shares concern about commercial espionage, including from China, which goes against the rules-based international order and threatens to undermine our economy. We will continue to promote responsible state behavior in cyberspace."[10]

  Ministry of Foreign Affairs of Denmark

- "Referring to the statements today by the United States and the UK, Finland again reiterates her concern on continued activities in cyberspace undermining international law. We require responsible state behavior."[11]

  Ministry of Foreign Affairs of Finland

- "Norway shares the concern expressed by several countries over cyber operations directed at civilian infrastructure, including from China. Important that agreed norms for state behavior in cyberspace are upheld."[12]

  Ministry of Foreign Affairs of Norway

- "Partners attribute specific cyber operation to China. As mentioned in annual reports of AIVD/MIVD, [the Netherlands] acknowledges threat of financial-economic espionage emanating from China. [The Netherlands] calls upon China to respect international law and norms in the digital domain."[13]

  Ministry of Foreign Affairs of the Netherlands

- "[We] share concerns expressed about state-sponsored malicious cyber activities. Campaigns like the so-called Cloud Hopper erode trust in cyberspace and threaten the global connectivity which we all rely on."[14]

  Margot Wallstrom, Minister of Foreign Affairs of Sweden

---

[9] "Cyberattacks by a group based in China known as APT10." Ministry of Foreign Affairs of Japan. December 21, 2018.

[10] "DK shares concern about commercial espionage, including from China, which goes against the rules-based international order and threatens to undermine our economy." Denmark MFA Twitter. December 20, 2018.

[11] "FM #Soini: Referring to the statements today by the United States and the UL, Finland again reiterates her concern on continues malicious activities in cyberspace undermining international law." Ulkoministeriö Twitter. December 20, 2018.

[12] "Norway shares the concern expressed by several countries over cyber operations directed at civilian infrastructure, including from China." Norway MFA Twitter. December 21, 2018.

[13] "Partners attribute specific cyber operation to China." Dutch Ministry of Foreign Affairs Twitter. December 20, 2018.

[14] "Share concerns expressed about state-sponsored malicious cyber activities." Margot Wallström. December 20, 2018.

- "We have great confidence in the attribution of APT10 to Chinese government agencies by different partner countries. We expect all countries to refrain or stop cyber activities that violate internationally agreed norms and standards, such as the G20 Declaration of Antalya 2015, and in no way help promote such operations."[15]

  From Transcript of Q&A with German Deputy Government Spokesperson

U.S. Charges Chinese Businessman with Economic Espionage, April 2019

Another U.S. Department of Justice indictment unsealed on April 23, 2019 alleged a Chinese businessman (Zhaoxi Zhang), together with a former General Electric (GE) Engineer (Xiaoqing Zheng), conspired to steal turbine technology trade secrets from GE. The theft was allegedly used to advance their business interests in two Chinese companies involved in researching, developing and manufacturing parts for turbines. The indictment also specifically alleged that, through their companies, the two defendants,

> "…received financial and other support from the Chinese government and coordinated with Chinese government officials to enter into research agreements with Chinese state-owned institutions to develop turbine technologies."[16]

"…[the U.S. Department of Justice indictment charging a Chinese businessman of stealing turbine technology trade secrets from GE alleges that he and a co-defendant]…received financial and other support from the Chinese government and coordinated with Chinese government officials to enter into research agreements with Chinese state-owned institutions to develop turbine technologies."

As further noted,

> "The indictment also alleges that Zheng and Zhang conspired to commit economic espionage, as the thefts of GE's trade secrets surrounding various turbine technologies were done knowing and intending that the thefts would benefit the People's Republic of China

[15] "Regierungspresskonferenz vom 21. Dezember 2018." Die Bundesregierung. December 21, 2018.

[16] "Former GE Engineer and Chinese Businessman Charged with Economic Espionage and Theft of GE's Trade Secrets." The United States Department of Justice. April 23, 2019.

and one or more foreign instrumentalities, including LTAT, NTAT, Shenyang Aerospace University, Shenyang Aeroengine Research Institute, and Huaihai Institute of Technology."[17]

Norway's Visma Hacked by Chinese Intelligence, February 2019

On February 6, 2019, the cybersecurity firm, Recorded Future (in collaboration with cyber-security consultancy Rapid7), published research claiming that hackers working for Chinese intelligence had breached the network of Visma, a Norwegian software company, to steal data from its clients.[18] Recorded Future described the hack as a potentially catastrophic attack.

The malware, Cloudhopper, which intelligence officials have attributed to the same hacking group described above, APT 10, has been deployed against a variety of targets, reportedly including Hewlett Packard Enterprise Co. and IBM. Visma, with global revenues of $1.3 billion last year, provides business software products to more than 900,000 companies across Scandinavia and parts of Europe.[19] According to Recorded Future,

> "…hackers working for Chinese intelligence had breached the network of Visma, a Norwegian software company, to steal secrets from its clients."

> "Access to the networks of these third-party service providers grants the [Ministry of Security Service] the ability to potentially access the networks of hundreds, if not thousands, of corporations around the world. We assess that APT10 likely compromised Visma with the primary goal of enabling secondary intrusions onto their client networks, and not of stealing Visma intellectual property."[20]

[17] "Former GE Engineer and Chinese Businessman Charged with Economic Espionage and Theft of GE's Trade Secrets." The United States Department of Justice. April 23, 2019.

[18] "APT10 Targeted Norwegian MSP and US Companies in Sustained Campaign." Recorded Future. February 6, 2019.

[19] "China hacked Norway's Visma to steal client secrets – investigators." Reuters. February 6, 2019.

[20] "APT10 Targeted Norwegian MSP and US Companies in Sustained Campaign." Recorded Future. February 6, 2019.

Huawei Charged by the U.S. Justice Department of Theft and Trade Secrets Conspiracy over Theft of T-Mobile Technology; Huawei Accused of Issuing Special Bonuses for Intellectual Property Theft

In May 2017, Huawei was found guilty of stealing T-Mobile technology. A U.S. 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 such capability.[21] In this instance, Huawei employees visiting T-Mobile's laboratory reportedly photographed the robot and stole a piece of it.[22] According to one account, Huawei employees "illicitly photographed the device, tried to smuggle components out of T-Mobile's Bellevue lab, and — when banned from the facility — tried to sneak back in." The original suit alleged Huawei was "using T-Mobile's stolen robot technology to test non-T-Mobile handsets and improve return rates for handsets developed and sold to other carriers."[23]

On January 28, 2019, the U.S. Justice Department announced charges against Huawei Device Co., Ltd. and Huawei Device Co. USA for theft of trade secrets conspiracy, attempted theft of trade secrets, seven counts of wire fraud, and one count of obstruction of justice. The press release summarized the charges as such,

> "The alleged conduct described in the indictment occurred from 2012 to 2014, and includes an internal Huawei announcement that the company was offering bonuses to employees who succeeded in stealing confidential information from other companies…
>
> 'The charges unsealed today clearly allege that Huawei intentionally conspired to steal the intellectual property of an American company in an attempt to undermine the free and fair global marketplace,' said FBI Director Wray. '…We look forward to presenting the evidence of Huawei's crimes in a court of law, and proving our case beyond a reasonable doubt.'…

"The alleged conduct described in the indictment…includes an internal Huawei announcement that the company was offering bonuses to employees who succeeded in stealing confidential information from other companies…"

[21] "Jury awards T-Mobile $4.8M in trade-secrets case against Huawei." The Seattle Times. May 18, 2017.

[22] "Jury awards T-Mobile $4.8M in trade-secrets case against Huawei." The Seattle Times. May 18, 2017.

[23] "T-Mobile sues Chinese telecom giant Huawei." The Seattle Times. September 5, 2014.

After T-Mobile discovered these criminal activities, and then threatened to sue, Huawei produced a report falsely claiming that the theft was the work of rogue actors within the company, rather than Huawei corporate entities in the United States and China. As emails obtained in the course of the investigation reveal, the conspiracy to steal secrets from T-Mobile was a company-wide effort involving many engineers and employees within the two charged companies.

"Huawei produced a report falsely claiming that the theft was the work of rogue actors within the company…as emails obtained in the course of the investigation reveal, the conspiracy to steal secrets from T-Mobile was a company-wide effort involving many engineers and employees…"

As part of its investigation, FBI obtained emails revealing that in July 2013, Huawei offered bonuses to employees based on the value of information they stole from other companies around the world, and provided to Huawei via an encrypted email address."[24]

Chinese Company Indicted on Economic Espionage, November 2018

On November 1, 2018, a Chinese state-owned enterprise (Fujian Jinhua Integrated Circuit, Co., Ltd.), along with a Taiwanese company and three individuals, were charged with "crimes related to a conspiracy to steal, convey, and possess stolen trade secrets of an American semiconductor company for the benefit of a company controlled by the PRC government." The target of the alleged conspiracy was Micron, a semiconductor company. As described by Attorney General Jeff Sessions at the press conference,

> "The worldwide supply for DRAM is worth nearly $50 billion; Micron controls about 20 to 25 percent of the dynamic random-access memory industry—a technology not possessed by the Chinese until very recently. As this and other recent cases have shown, Chinese economic espionage against the United States has been increasing—and it has been increasing rapidly."[25]

FBI Director Christopher Wray noted,

[24] "Chinese Telecommunications Device Manufacturer and its U.S. Affiliate Indicted for Theft of Trade Secrets, Wire Fraud, and Obstruction of Justice." The United States Department of Justice. January 28, 2019.

[25] "PRC State-Owned Company, Taiwan Company, and Three Individuals Charged with Economic Espionage." The United States Department of Justice. November 1, 2018.

"The Chinese government is determined to acquire American technology, and they're willing use a variety of means to do that – from foreign investments, corporate acquisitions, and cyber intrusions to obtaining the services of current or former company employees to get inside information."[26]

"The Chinese government is determined to acquire American technology, and they're willing use a variety of means to do that – from foreign investments, corporate acquisitions, and cyber intrusions to obtaining the services of current or former company employees to get inside information."

Chinese Intelligence Officer Charged with Economic Espionage, October 2018

On October 10, 2018, the U.S. Justice Department charged Yanjun Xu, an operative of China's Ministry of State Security, with "conspiring and attempting to commit economic espionage and steal trade secrets from multiple U.S. aviation and aerospace companies." The individual was extradited to the United States on October 9, 2018. According to the indictment,

> "Beginning in at least December 2013 and continuing until his arrest, Xu targeted certain companies inside and outside the United States that are recognized as leaders in the aviation field."

Assistant Director Bill Priestap of the FBI's Counterintelligence Division noted the role of the Chinese state in these activities.

> "This unprecedented extradition of a Chinese intelligence officer exposes the Chinese government's direct oversight of economic espionage against the United States," said Assistant Director Priestap."

U.S. Charges Five Chinese Military Hackers with Cyber Espionage, May 2014

On May 19, 2014, in what was the first instance of the U.S. Justice Department charging a state actor with hacking, five Chinese military hackers were indicted for "computer hacking, economic espionage and other offenses directed at six American victims in the U.S. nuclear power, metals and solar products industries." As noted in the associated press release,

[26] "PRC State-Owned Company, Taiwan Company, and Three Individuals Charged with Economic Espionage." The United States Department of Justice. November 1, 2018.

> "The indictment alleges that the defendants conspired to hack into American entities, to maintain unauthorized access to their computers and to steal information from those entities that would be useful to their competitors in China, including state-owned enterprises (SOEs). In some cases, it alleges, the conspirators stole trade secrets that would have been particularly beneficial to Chinese companies at the time they were stolen. In other cases, it alleges, the conspirators also stole sensitive, internal communications that would provide a competitor, or an adversary in litigation, with insight into the strategy and vulnerabilities of the American entity."[27]

Allegations of Chinese Government Officials Working Undercover at Huawei

Several allegations have been made referencing Chinese government officials working undercover at Huawei, either with or without the company's knowledge. The *Los Angeles Times* reported on April 10, 2019, that since 2012,

> "U.S. intelligence officials say they have continued to pursue leads that suggest Huawei is still gathering competitive intelligence and there are strong indications that the Chinese government, with or without Huawei's permission, has installed operatives with unofficial cover in some Huawei foreign offices."
>
> 'We have seen examples where Chinese spies have gone undercover with Huawei,' said one senior intelligence official. 'At the same time, we think that it is becoming increasingly tough to detect changes in software from Huawei and other Chinese companies.'"[28]

"…there are strong indications that the Chinese government, with or without Huawei's permission, has installed operatives with unofficial cover in some Huawei foreign offices."

Similar beliefs were later attributed, in the same article, to sources from within the company,

> "Interviews with Huawei employees and companies doing business with it reveal a widespread belief that the Chinese government has placed intelligence agents in Huawei offices around the world and that conversations are routinely monitored.

---

[27] "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage." The United States Department of Justice. May 19, 2014.

[28] "The man behind Huawei." Los Angeles Times. April 10, 2019.

'The state wants to use Huawei, and it can use it if it wants,' the staffer in Shenzhen said. 'Everyone has to listen to the state. Every person. Every company and every individual, and you can't talk about it. You can't say you don't like it. That's just China.'"[29]

"Interviews with Huawei employees and companies doing business with it reveal a widespread belief that the Chinese government has placed intelligence agents in Huawei offices around the world and that conversations are routinely monitored."

Huawei Official Urges "Comrades on the Hidden Fronts to Take the Risks"

Online reports emerged in April 2019 that a speech given by Huawei's Senior Vice President, Chen Lifang, at a meeting of the company's new employees urged them to "[rely] on comrades on the hidden fronts to take the risks" to obtain certain technologies on which the U.S. has imposed sanctions. She went on to say, "Why do we have to firmly study from the United States? How much do you understand about the real American manufacturing?" According to an analysis of these comments from *Chinascope*,

"She gave examples of technologies on which China is still falling behind after 30 years of hard work. She said that in the field of composite materials, the process data accumulated by DuPont is more than 25 times what China has collected. In the field of turbofan engines, the number of materials and process tests completed in China is only 5 percent of what GE has done.

Chen expressed the belief that a long list of equipment, including smart grid advanced measuring instruments, material analysis precision testing instruments, mechanical performance testing equipment, new types of non-destructive testing equipment, environmental and safety testing instruments, and special defense testing instruments, all rely on imports."

"…a speech given by Huawei's Senior Vice President, Chen Lifang, at a meeting of the company's new employees urged them to '[rely] on comrades on the hidden fronts to take the risks' to obtain certain technologies on which the U.S. has imposed sanctions."

[29] "The man behind Huawei." Los Angeles Times. April 10, 2019.

Chen reportedly said of such protected technologies,

> "For those technologies that are embargoed according to the Wassenaar Agreement (export controls for conventional weapons and sensitive dual-use goods and technologies), we can only rely on comrades working on the hidden fronts to take the risks to obtain them."

According to *Chinascope*,

> "She also said that as for equipment such as high-reliability and sensitive sensors, new composites, optical fibers, MEMS, biosensors, high-end (especially military-grade) electronic devices and variable frequency speed control devices, we can only rely on special means of importing goods to acquire them."[30]

Economic Espionage in Poland, Huawei Employee Arrested

On January 8, 2019, Poland's Internal Security Agency (ISA) charged with espionage a former Polish civil servant, Piotr D., and a Chinese national, Weijing Wang, also known as Stanislaw Wang, who was a sales director at Huawei at the time (and subsequently fired after the arrest). Interestingly, prior to joining Huawei in 2017, Wang was an attaché at the Chinese Embassy in Poland from 2006 to 2011. Piotr D. was a former employee of ISA, but, at the time of the arrest, worked for telecommunications company Orange Polska.

In statements made following the arrest, the spokesman for the ISA, Stanislaw Zaryn, said that the "matter has to do with [Wang's] actions, it doesn't have anything to do with the company he works for" in reference to Huawei. Several senior officials, however, have since made statements against the company. On January 13, Poland's Internal Affairs Minister, Joachim Brudziński, called for the EU and NATO to take a "joint stance" on Huawei in response to the arrest.

He stressed that Poland wishes to maintain "relations with China that are good, intensive, and attractive for both sides" but that "there are concerns about Huawei." Karol Okonski, a Deputy Digital Affairs Minister, also made public comments that Warsaw was analyzing any involvement by Huawei in building the country's 5G telecommunications infrastructure.

Alleged Chinese Hack of Dutch ASML Leads to Calls to Ban Huawei

In April 2019, two leading Dutch political parties, the People's Party for Freedom and Democracy (VVD) and the Christian Democratic Appeal (CDA) declared their support for banning Huawei from

[30] "Quote from Huawei's Senior VP – "Rely on Comrades on the Hidden Fronts to Take the Risks." Chinascope. December 30, 2018.

construction of the country's 5G network after news from semiconductor chip machine maker ASML that, in 2015, it had been the victim of corporate espionage from employees from countries, including China.

The response from VVD and CDA came after news of the theft broke in the Dutch daily newspaper *Financieele Dagblad*. GroenLinks, the largest opposition party on the left, had already called for this action in February. VVD MP Wybren of Haga offered the view,

> "It's very simple…if a party doesn't play by the rules in a game, then you shouldn't play with that. China is a country that clearly does not respect the rules of international trade and has no respect whatsoever for the intellectual property of Western high-tech companies."

"Poland's Internal Security Agency (ISA) charged with espionage…a Chinese national, Weijing Wang…who was a sales director at Huawei at the time… Interestingly, prior to joining Huawei in 2017, Wang was an attaché at the Chinese Embassy in Poland from 2006 to 2011."

CDA MP Joba van den Berg offered,

> "There are strong doubts about Huawei's independence from the Chinese government. You don't want a company like that in your core systems…When it comes to Huawei, we are very focused on their network equipment, such as routers and servers, but we also have to look at the operating systems that are being used and the service and maintenance contracts."

The Dutch security service AIVD has long warned officials about the dangers of Chinese corporate espionage in the country's high-tech sector. Most recently, on April 2, 2019, AIVD reportedly advised its government not to use technology from countries with active hacking campaigns targeting them, including China. Specifically, AIVD's annual report said,

> "It is undesirable for the Netherlands to exchange sensitive information or for vital processes to depend on the hardware or software of companies from countries running active cyber programmes against Dutch interests."[31]

[31] "Dutch security agency warns against using 'undesirable' Chinese, Russian technology, citing hacking risk." South China Morning Post. April 3, 2019.

Examples of Other Past Allegations of Huawei Hacking and Intellectual Property Theft

- In early 2004, Huawei was reportedly caught stealing trade secrets from Nortel. Huawei allegedly hacked their way into the accounts of Nortel executives, including CEO Frank Dunn and Brain McFadden, stealing future product designs and marketing plans. Malware, most likely attributable to Huawei, was also allegedly used to record "nearly every phone call that Frank Dunn made."[32]

- A 2008 lawsuit filed by Motorola, and later amended in 2010, alleged that Huawei stole trade secrets. The case was settled out of court. Motorola claimed a string of emails marked "Motorola Confidential Proprietary" demonstrated that "Huawei and its officers knew they were receiving stolen Motorola proprietary trade secrets and confidential information without Motorola's authorization and consent."[33] There were reports that a Motorola engineer named Hanjuan Jin was stopped by customs agents at O'Hare Airport and "found with $30,000 in cash, a carry-on bag full of Motorola documents marked 'confidential and proprietary,' and a one-way ticket to Beijing."[34] A summary of the case from the Coalition for a Prosperous America observed,

  > "Subsequent investigations by the FBI revealed that Jin was simultaneously working for another company, Lemko, while she was working for Motorola. According to court documents filed in Chicago by prosecutors in 2010, Lemko was founded by Motorola engineer Shaowei Pan in 2004, shortly after Pan met with Huawei founder and CEO Ren Zhengfei and other top Huawei executives on a trip to China. According to federal prosecutors, Lemko's goal was to build wireless technology for Huawei based on Motorola technology. Pan later emailed Ren to say: 'If our plan can progress smoothly, Lemko will be the company we are planning to establish, and it will be independent of Motorola Inc.'"

  According to Motorola, Huawei allegedly paid several of its employees for the company's intellectual property. The CEO of Motorola Solutions, Greg Brown, said on television in 2018 that "Huawei definitely stole trade secrets… and we sued."[35]

- CISCO sued Huawei in 2003 over the theft of designs and software code. Huawei subsequently admitted to using a few lines of code. As summarized by Aragon Research,

---

[32] "Cyberwar Flashback: Remembering The Huawei Hacks Of Cisco And Nortel." Aragon Research. January 24, 2019.

[33] "Motorola sues Huawei for trade secret theft." Reuters. July 22, 2010.

[34] "Top Five Cases of Huawei IP Theft and Patent Infringement." Coalition for a Prosperous America. December 13, 2018.

[35] "Inside business in China: Motorola Solutions CEO details Huawei theft." Fox Business. December 11, 2018.

"CISCO claimed it copied the entire design."[36] The suit was settled out of court in 2004. CISCO sought to correct the record in 2012, after misleading statements from Huawei at the time. CISCO quoted from a neutral expert's findings involved in the settlement that,

> "The exactness of the comments and spacing not only indicate that Huawei has access to the Cisco code but that the Cisco code was electronically copied and inserted into [Huawei's]… The nearly identical STRCMP routines are beyond coincidence…It must be concluded that Huawei misappropriated this code."[37]

- As summarized by Annie Fixler, Deputy Director of the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies, an investigative report by Bloomberg dated February 4, 2019 alleged that,

> "…the U.S. startup Akhan Semiconductor Inc. provided a prototype of its diamond-coated, super-scratch resistant cell phone glass to Huawei for testing at U.S.-based facilities in March 2018. The testing, which is part of the normal sales and marketing process, was supposed to take only 60 days. The contract also prohibited testing that would damage the product.
>
> Huawei, however, did not return the prototype until August and, according to Bloomberg, broke it in efforts to reverse engineer the technology. Moreover, Huawei representatives admitted to Akhan that they shipped the sample to China for testing. Nevertheless, the representatives brushed off accusations that this action might violate U.S. export controls, which prohibit the export of goods with defense applications. 'Diamond coatings are on the list because of their potential for use in laser weapons,' Bloomberg noted."[38, 39]

- In November 2018, *The Weekend Australian* reported that it had been informed Australian officials were in receipt of secret intelligence reports outlining a case where the Chinese government pressed the staff of an unnamed "high risk vendor" to gain access codes to a foreign network. Huawei's identity as this vendor was reportedly confirmed by *The Weekend Australian*. The success of the request was reported to be unknown.[40]

---

[36] "Cyberwar Flashback: Remembering The Huawei Hacks Of Cisco And Nortel." Aragon Research. January 24, 2019.

[37] "Huawei and Cisco's Source Code: Correcting the Record." Cisco Blogs. October 11, 2012.

[38] "Huawei Breaks the Law…Again." Foundation for Defense of Democracies. February 14, 2019.

[39] "Huawei Sting Offers Rare Glimpse of the US Targeting a Chinese Giant." Bloomberg Businessweek. February 4, 2019.

[40] "China used Huawei to hack network, says secret report." The Australian. November 2, 2018.

2) CCP Control Over Huawei and Other Companies

Fundamental to the cyber-related risk calculation that comes with doing business with Huawei and other Chinese technology companies is understanding their availability to the Chinese government for hacking and/or espionage purposes.

In this connection, there have been several reports in recent months seeking to shed light on the question of Huawei's funding, owners and controlling stakeholders, some derived from unspecified U.S. government sources and others meticulously documented in the public domain.

There are also prominent examples of generic means through which the Chinese government exerts control over its "private sector" actors.

No Separation of Powers, No Checks and Balances

An assessment of state control over the private enterprise requires an understanding of the nature of the Chinese regime, the long history of the government viewing their companies as vehicles for influence and policy by state planners (rooted in the country's communist ideology), and the public touting by senior officials of a regime that is free of checks and balances.

A number of public comments attributed directly to senior officials with regard to the Chinese system are provided below, demonstrating the confidence and transparency with which Chinese officials declare their support for their authoritarian model.

- "[China's courts] must firmly resist the western idea of 'constitutional democracy,' 'separation of powers' and 'judicial independence.' These are erroneous western notions that threaten the leadership of the ruling Communist Party and defame the Chinese socialist path on the rule of law. We have to raise our flag and show our sword to struggle against such thoughts. We must not fall into the trap of western thoughts and

"[China's courts] must firmly resist the western idea of 'constitutional democracy,' 'separation of powers' and 'judicial independence.'… We must not fall into the trap of western thoughts and judicial independence."

judicial independence. We must stay firm on the Chinese socialist path on the rule of law."[41]

Zhou Qiang, Chief Justice and President of the Supreme People's Court of China

"…[there is] no such thing as the separation of powers between the party and the government."

- "The government must be placed under the leadership of the ruling party, which is entitled to govern everything, including the government."[42]

  Zhu Lijia, Professor at the Chinese Academy of Governance

- "…[there is] no such thing as the separation of powers between the party and the government."[43]

  Wang Qishan, Vice President of the People's Republic of China

- "Historically the Chinese understanding of government is a broad one. In our eyes, all power branches belong to the government. There is no such thing as separation between the party and the government. There is only a division of functions. We must take a clear position and be straightforward on this issue."[44]

  Wang Qishan, Vice President of the People's Republic of China

- "Why can China maintain long-term stability without chaos? The fundamental reason is that we always adhere to the leadership of the Communist Party… We must further institutionalize and legalize the party's leadership."[45]

  Xi Jinping, President of China

- "We must never follow the path of Western 'constitutionalism,' 'separation of powers,' or 'judicial independence,'[46]

  Xi Jinping, President of China

---

[41] "China's top judge warns against the 'threat' of judicial independence." HKFP. January 24, 2017.

[42] "'No separation of powers': China's top graft-buster seeks tighter party grip on government." South China Morning Post. March 6, 2017.

[43] "'No separation of powers': China's top graft-buster seeks tighter party grip on government." South China Morning Post. March 6, 2017.

[44] "'No separation of powers': China's top graft-buster seeks tighter party grip on government." South China Morning Post. March 6, 2017.

[45] "Xi: China Must Never Adopt Constitutionalism, Separation of Powers, or Judicial Independence." The Diplomat. February 19, 2019.

[46] "Xi: China Must Never Adopt Constitutionalism, Separation of Powers, or Judicial Independence." The Diplomat. February 19, 2019.

- "Party, government, military, civilian, and academic, east, west, south, north, and center, the party leads everything."[47]

  Mao Zedong quote incorporated into the CCP Constitution in 2017

The National Intelligence Law

China's National Intelligence Law, enacted on June 27, 2017, further entrenched the already unwritten understanding that Chinese companies and their employees are required to comply with government orders in the area of national intelligence work.[48] Article 7 details these powers, also specifying that Chinese organizations and persons used for intelligence purposes are required to maintain the secrecy of their involvement in any such operations. It states,

- "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."

"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."

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

- "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."

---

[47] "Xi: China Must Never Adopt Constitutionalism, Separation of Powers, or Judicial Independence." The Diplomat. February 19, 2019.

[48] "China passes tough new intelligence Law." Reuters. June 27, 2017.

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." [49, 50]

As observed by *Sinopsis*, a Prague-based organization that tracks developments involving China,

> "This law in effect only codifies common practice in an increasingly totalitarian regime. Even before current CCP Secretary General Xi Jinping came to power, it would have been difficult for a Chinese citizen to turn down a request for cooperation from the PRC intelligence apparatus. With Xi's centralisation of CCP power, and in an atmosphere of constant struggle against "hostile foreign forces" (**境外**敌对势**力**), refusing cooperation becomes all but impossible, regardless of the actual letter of applicable laws."[51]

As the Law became so widely used as validating concerns that had previously been based only on an implicit understanding of the way things work in China, the CCP and Huawei ultimately saw it necessary to refute its applicability to the company. It has done so via a recycled May 2018 legal opinion, signed by a CCP member and issued by Zhong Lun Law Firm, that disputes what is stated explicitly in the law. As also noted by *Sinopsis*,

> "The opinion, from May 2018, was prepared by Zhong Lun Law Firm (**中**伦**律**师**事**务**所**), a well-known legal practice whose founding and managing partner and deputy Party secretary Zhang Xuebing 张**学兵**, has also brought his qualities as an 'outstanding Party member' to his positions at the All-China Youth Federation (ACYF, **中**华**全国青年联合会**), a United Front organisation led by the CCP Youth League. The opinion for Huawei was coauthored by a CCP member, Chen Jihong 陈际红. It is worth remembering that Chinese lawyers who openly challenge the CCP's views face disbarment, imprisonment and torture."[52]

Another analysis from *Sinopsis* delved into the questions raised regarding the special status that Huawei must have to get away with promulgating a legal opinion that directly challenges such an important law.

---

[49] "National Intelligence Law of the People's Republic of China." China Copyright and Media. May 16, 2017.

[50] National Intelligence Law. People's Republic of China.

[51] "Lawfare by proxy: Huawei touts "independent" legal advice by a CPP member." Sinopsis. February 8, 2019.

[52] "Lawfare by proxy: Huawei touts "independent" legal advice by a CPP member." Sinopsis. February 8, 2019.

> "Again the proper context for such a document risks being lost in translation: contradicting the official Party line on matters of national security would be suicidal for a normal lawyer in a legal system where such behaviour routinely leads to disbarment, imprisonment and torture; an analysis at odds with the official line would be even more unlikely to come from the authors of the pro-Huawei document, one of whom has received a distinction as an 'outstanding lawyer Party member' (优秀律师党员). Huawei had the CCP-linked legal opinion reviewed by Clifford Chance, an international law firm with extensive operations in China, whose endorsement of it came with a disclaimer explicitly rejecting its construal as a "legal opinion on the application of PRC law.' While keeping the document confidential, Huawei officers including its top executives in Poland and the Czech Republic took to citing the document as an 'independent legal opinion' by a British firm."[53]

Research Alleges Huawei May Actually be State-Owned

Below are summary findings presented by a detailed and compelling research document written by Donald Clark (a Professor of Law at George Washington University Law School) and Christopher Balding (Associate Professor of Economics, Fulbright University Vietnam) into the narrative presented by Huawei that the company is 99% "employee-owned."

- The Huawei operating company is 100% owned by a holding company, which is in turn approximately 1% owned by Huawei founder Ren Zhengfei and 99% owned by an entity called a "trade union committee" for the holding company.
- We know nothing about the internal governance procedures of the trade union committee. We do not know who the committee members or other trade union leaders are, or how they are selected.
- Trade union members have no right to assets held by a trade union.
- What have been called "employee shares" in "Huawei" are in fact at most contractual interests in a profit-sharing scheme.
- Given the public nature of trade unions in China, if the ownership stake of the trade union committee is genuine, and if the trade union and its committee function as trade unions generally function in China, then Huawei may be deemed effectively state-owned.
- Regardless of who, in a practical sense, owns and controls Huawei, it is clear that the employees do not.[54]

[53] "Lost in Translation: 'Economic Diplomacy' with Chinese characteristics." Sinopsis. March 11, 2019.

[54] "Who Owns Huawei." SSRN. April 17, 2019.

This analysis notwithstanding, Guo Ping, one of Huawei's rotating Co-Chairmen, told the *Los Angeles Times* that, "No Chinese government agency or legal entity from China or abroad holds any share of Huawei."[55] Regardless, the analysis contained in a recent analysis from MERICS, entitled "Chinese Telecommunication Companies: Political and Legal Vulnerabilities and How Europe Should Deal with Them," that dissects the present realities in China with regard to Party control over private enterprise is instructive.

> "Additional risks of state inference lie in the institutionalized channels for political influence on businesses and the justice system in China. While private Chinese enterprises are not merely agents of the CCP and generally function largely independently both within China and in international markets, the Chinese party-state has implemented and recently expanded mechanisms (party committees, party cells and secretaries) to exert influence where it deems necessary. New party regulations clearly state the aim of expanding party committees (branches) and their role in the private sector. There have been numerous complaints from Western private enterprises to their governments about being 'guided' by party committees. Therefore, it is reasonable for Western governments to assume that the CCP has the intention to influence and to use party committees or cells in at least some instances.
>
> Within the judicial and law enforcement systems, the political-legal committees, party committees and secretaries fulfill a similar steering function that allows targeted

"The CCP's hold over state institutions is likely to increase under the ongoing initiative to strengthen party leadership over the legal system. Independent oversight bodies over state security organs that citizens and enterprises might turn to if they receive undue requests for cooperation are de facto non-existent."

"While private Chinese enterprises are not merely agents of the CCP and generally function largely independently both within China and in international markets, the Chinese party-state has implemented and recently expanded mechanisms (party committees, party cells and secretaries) to exert influence where it deems necessary."

[55] "The man behind Huawei." Los Angeles Times. April 10, 2019.

> political interference. The CCP's hold over state institutions is likely to increase under the ongoing initiative to strengthen party leadership over the legal system. Independent oversight bodies over state security organs that citizens and enterprises might turn to if they receive undue requests for cooperation are de facto non-existent. This has facilitated the Chinese state's and the CCP's selective violation of domestic and international law as well as the sovereignty of other states to safeguard and assert their interests (a well-documented pattern that ranges from hostage diplomacy to detentions of dissidents and ethnic minority members)."[56]

Huawei Has Received Significant Funds from State-Owned Policy Banks

Although a secondary sign of state control, there is significant evidence of Huawei receiving state support for its business operations and overseas growth. The China Development Bank (CDB) – a self-described "financial institution under the direct leadership of the State Council[57] – has served as a major financier supporting the growth of Huawei's international presence and corporate business development.

On numerous occasions, Huawei has received massive CDB offers of financial support (and actual export financing loans) to promote strategic expansion in global markets. In 2005, it was reported that Huawei received a $10 billion credit line from CDB.[58] The loan "letter of support" documenting this agreement was posted to Wikileaks.[59] The letter said the funding was being provided,

> "…in order to assist Huawei in its overseas development, including the export of products and equipment, overseas investments, overseas contracting and so on."

In 2009, Huawei received another CDB credit line of $30 billion to "implement [China's] globalization strategy," according to China's state-run news outlet, *Xinhua*.[60] CDB reportedly offered an additional $30 billion credit line to Huawei again in 2011 – this time, with low interest rates and a two year grace period on repayments.[61] According to RWR transactional data, which has catalogued Huawei's

[56] "Chinese telecommunication companies: Political and legal vulnerabilities and how Europe should deal with them." Mercator Institute for China Studies. March 13, 2019.

[57] "About CDB." China Development Bank.

[58] "Huawei Funded for Overseas Expansion." Shenzhen Daily. January 5, 2005.

[59] https://file.wikileaks.org/file/support-letter-to-huawei-from-cdb-2004.png

[60] "Huawei gets $30b credit line from CDB." Telecomasia. September 24, 2009.

[61] "Huawei's $30 Billion China Credit Opens Doors in Brazil, Mexico." Bloomberg. April 24, 2011.

transactions outside of China, the company has carried out at least 45 identifiable deals since 2010 with export and project financing provided by China's state-owned banks. The funds provided across these deals totaled $10.54 billion.

As recently as April 2019, the *Wall Street Journal* summarized the relationship between Huawei and CDB.

> "As with subway cars, the support of Beijing is a huge part of sustaining China's rising dominance in wireless. Financial aid from China's state-owned development bank [CDB] allows Huawei to provide below-market financing for its products, an offer that has proven irresistible to wireless carriers in Saudi Arabia, Turkey, and many other countries."[62]

"Financial aid from China's state-owned development bank [CDB] allows Huawei to provide below-market financing for its products, an offer that has proven irresistible to wireless carriers in Saudi Arabia, Turkey, and many other countries."

In addition to some implied control or, at minimum, state involvement that is derived from receiving state-backed financing of this kind, the advantage that it has provided Huawei in terms of pricing is also centrally important, as explained by James Lewis of the Center for Strategic and International Studies (CSIS),

> "Huawei's primary advantage is its government-subsidized price, and the Chinese government is not paying hundreds of millions of dollars to build another country's telecom infrastructure because they admire its cuisine."[63]

Huawei's primary advantage is its government-subsidized price, and the Chinese government is not paying hundreds of millions of dollars to build another country's telecom infrastructure because they admire its cuisine."

This point was also made by Philippe Le Corre, Senior Fellow at the Harvard Kennedy School, who said in a *CNN Business* article,

---

[62] "China's Subsidized Conquest of Trade." WSJ Opinion. April 23, 2019.

[63] "Issue the Executive Order." Center for Strategic & International Studies. March 29, 2019.

> "There's only one reason Huawei is so powerful, it's because they received loans without interest from [Chinese state banks]. And that helped them to penetrate European markets."[64]

The article also cites a CSIS study by Nathaniel Ahrens from February 2013 that observed,

> "While export credit programs are available in many countries, the United States, Sweden, and Japan included, the sheer size of the Chinese loans dwarf comparable programs in other countries."[65]

Indeed, the spokesperson for Huawei, Glenn Schloss, told *CNN Business* that "Between 2005 and 2011, China Development Bank agreed to provide as much as $40 billion to potential Huawei customers." He asserted, however, that, Huawei only accessed some $3 billion of that amount. Although the amount, compared to total sales, was characterized as insignificant, the *CNN* article also cited a former project director at Huawei, saying that Beijing's support was key to the company's success.[66]

Huawei's High-Risk Activity

Huawei's willingness to take on controversial clients, including Saddam Hussein's Iraq and Iran during a period of tight, international sanctions, is persuasive to some that government influence could have been behind seemingly high risk, low-reward business decisions.

U.S. claims that Huawei shipped products with U.S. components to Iran and other sanctioned countries, in part, by fraudulent claims to U.S. banks is the reason behind the arrest and pending extradition request for Meng Wanzhou, the Chief Financial Officer of Huawei and daughter of the company's founder, Ren Zhengfei. Notably, Chinese officials have said they do not consider their companies to be bound by U.S. trade restrictions and sanctions policy.[67]

Beyond compliance with sanctions, Huawei's credibility with regard to complying with the guidelines it sells publicly has been undercut

"Beyond compliance with U.S. sanctions, Huawei's credibility with regard to complying with the guidelines it sells publicly has been undercut by allegations of bribery and corruption."

[64] "Wolf culture, state finance and bribery: Huawei's rise to the top wasn't pretty." CNN Business. April 17, 2019.
[65] "China's Competitiveness: Huawei." Center for Strategic & International Studies. February 15, 2013.
[66] "Wolf culture, state finance and bribery: Huawei's rise to the top wasn't pretty." CNN Business. April 17, 2019.
[67] "The 6 reasons why Huawei gives the US and its allies security nightmares." MIT Technology Review. December 7, 2018.

by allegations of bribery and corruption. A recent *Voice of America* article noted,

> "In Algeria, it was banned from bidding for public contracts after one of its executives was convicted of bribery.
>
> In Zambia, it was probed over allegations of bribery involving a multi-million-dollar contract to build cell towers in rural areas.
>
> In the Solomon Islands, it was accused of offering millions of dollars to the ruling party in exchange for an undersea fiber optic cable contract.
>
> In all three cases – and half a dozen others in recent years – the alleged perpetrator was Huawei Technologies, the Chinese telecom behemoth facing scrutiny from Western nations over allegations of intellectual property theft and espionage."[68]

[68] "Bribery, Corruption Charges Follow Huawei Around the World." VOA News. February 11, 2019.

3) China's Stated Strategic Objectives

This section describes the strategic agenda the Chinese government is seeking to advance at home and abroad through its growth, including via its companies.

President Xi: Opening Remarks before the 19th National Congress of the CCP

According to coverage of President Xi's remarks before the 19th National Congress of the CCP, he remarked of China's global ambitions,

> "…the path, the theory, the system, and the culture of socialism with Chinese characteristics have kept developing, blazing a new trail for other developing countries to achieve modernization. It offers a new option for other countries and nations who want to speed up their development while preserving their independence; and it offers Chinese wisdom and a Chinese approach to solving the problems facing mankind."[69]

"[The culture of socialism with Chinese characteristics] offers a new option for other countries and nations who want to speed up their development while preserving their independence…"

President Xi: Remarks Published in Political Journal, *Qiushi*, April 2019

Perhaps most compelling in summarizing CCCP objectives are the words of President Xi, published by *Qiushi*, a top political journal, on April 1, 2019. The publication was of a speech President Xi gave after being elected General Secretary in 2013. In re-printing these words, Xi makes clear their ongoing pertinence and importance.

[69] "Socialism with Chinese Characteristics Enters New Era: Xi." Xinhua. October 18, 2017.

"…our party has always adhered to the lofty ideals of communism. Communists, especially leading cadres, should be staunch believers and faithful practitioners of the lofty ideals of communism and the common ideals of socialism with Chinese characteristics. The belief in Marxism, socialism and communism is the political soul of the communists and the spiritual prop of the communists to withstand any test. The party constitution clearly stipulates that the highest ideal and ultimate goal of the party is to realize communism.

"The party constitution clearly stipulates that the highest ideal and ultimate goal of the party is to realize communism."

"…capitalism must die out and socialism must win."

At the same time, the party constitution clearly stipulates that the communist ideal pursued by the Chinese communists can only be realized on the basis of the full development and highly developed socialist society. It is unrealistic to expect to enter communism in one or two strokes. Comrade Deng Xiaoping said that the consolidation and development of the socialist system still needs a very long historical period and requires our generations, more than a dozen generations and even dozens of generations to make unremitting efforts…

Facts have repeatedly told us that Marx and Engels' analysis of the basic contradictions in capitalist society is not out of date, nor is their historical materialism view that capitalism must die out and socialism must win. This is an irreversible general trend in social and historical development, but the road is tortuous. The final demise of capitalism and the final victory of socialism must be a long historical process. We should have a deep understanding of the self-regulation ability of capitalist society, fully estimate the objective reality of the

"We should have a deep understanding of the self-regulation ability of capitalist society, fully estimate the objective reality of the long-term dominance of western developed countries in economic, scientific, technological and military aspects, and earnestly prepare for the long-term cooperation and struggle between the two social systems…"

long-term dominance of western developed countries in economic, scientific, technological and military aspects, and earnestly prepare for the long-term cooperation and struggle between the two social systems…"[70]

Other Observations of China's Foreign Policy Objectives

Other, external observations of Chinese principles and overseas objectives appear below.

- "Russia and China view efforts to support democracy—especially U.S. efforts—as thinly veiled attempts to expand U.S. influence and undermine their regimes and have consistently sought to counter Western democracy promotion. These efforts are not new, but they are changing in scope and intensity…Chinese leaders have sought to gradually weaken democratic norms as a way to enhance the international legitimacy of China's Leninist-capitalist brand of governance."[71]

  Andrea Kendall-Taylor and David Shullman, *Foreign Affairs,* October 2018

- "China, in part to defend its economic interests, also interferes in the political systems of developing countries around the world, tipping the scales towards China-friendly politicians and policies…Beijing wants to protect its growing investments, ensure Party control over ideology and information that might enter China, and legitimize China's authoritarian development model abroad. Presenting a positive 'China story,' as Xi has put it, helps to smooth the path for investments that benefit China's economy."

  "China achieves significant political influence through its economic leverage, prompting some beneficiaries to tamp down criticism about human rights in China or support China on the South China Sea in multilateral forums. Countries that support China's interests, or at a minimum do not challenge it on sensitive issues, receive benefits; conversely, countries that oppose China are denied access to these rewards and might even be punished."[72]

  David Shullman, *Brookings Institution,* January 2019

[70] "Liu He to DC; Decent economic data; Xi and the final victory of socialism; Taiwan." Sinocism. April 1, 2019.

[71] "How Russia and China Undermine Democracy." Andrea Kendall-Taylor, David Shullman. Foreign Affairs. October 2, 2018.

[72] "Protect the Party: China's Growing Influence in the Developing World." David Shullman. Brookings. January 22, 2019.

- "The CCP commands an extensive state and party apparatus to wield an authoritarian form of soft power. This goes beyond routine public diplomacy, to include 'unorthodox' means to co-opt political elites, academia, think-tanks and media to support CCP policy goals, and to silence criticism on sensitive topics."[73]

  European Parliamentary Research Service (EPRS), May 2018

- "China's rapidly increasing political influencing efforts in Europe and the self-confident promotion of its authoritarian ideals pose a significant challenge to liberal democracy as well as Europe's values and interests. While Beijing's efforts have received much less scrutiny than the efforts of Putin's Russia, Europe neglects China's increasing influence at its own peril."

  "The effects of this asymmetric political relationship are beginning to show within Europe. European states increasingly tend to adjust their policies in fits of 'preemptive obedience' to curry favor with the Chinese side. Political elites within the European Union (EU) and in the European neighborhood have started to embrace Chinese rhetoric and interests, including where they contradict national and/or European interests."

  "The Chinese leadership's political influence-seeking in Europe is driven by two interlocking motivations. First and foremost, it seeks to secure regime stability at home. Second, Beijing aims to present its political concepts as a competitive, and ultimately superior, political and economic model. Driven by these motivations, Beijing pursues three related goals."

  "…China's political model is based on an authoritarian regime intent on strengthening a deeply illiberal surveillance state at home while also exporting – or at least trying to popularize – its political and economic development model abroad. Thus, today, all areas of Europe's interaction with China have strong political undertones."[74]

  Mercator Institute for China Studies (MERICS), February 2018

- "The deeper challenge is that China has begun to engage at a global level, building an expansive international network for influence, increasingly backed by technologies for digital censorship and monitoring. China has substantial appeal, both for its enormous success in fostering economic development, but also for its ability to retain political control while doing so. China is moving assertively to position itself for influence—economic, diplomatic, and in some areas coercive—in Europe, in Latin America, and in Africa."[75]

  Bruce Jones, Torrey Taussig, *Foreign Policy at Brookings*, February 2019

---

[73] "China's foreign influence operations in Western liberal democracies: An emerging debate." European parliament. May 2018.

[74] "Authoritarian Advance: Responding to China's Growing Political Influence in Europe." Mercator Institute for China Studies. February 2018.

[75] "Democracy and Disorder: The Struggle for Influence in the New Geopolitics." Bruce Jones, Torrey Taussig. Foreign Policy at Brookings. Brookings Institution. February 2019.

Huawei and Civil/Military Fusion in China

Under the Chinese concept of civil-military integration, Huawei's development, as a prominent company within a government-designated strategic industry, appears to have relevance for the Peoples Liberation Army (PLA), both as a force multiplier, as well as a vehicle for strategic research and development and capability modernization. From a Chinese leadership perspective, Huawei's international growth serves a strategic purpose.

> *"We need to build an innovative system of defense science and technology […] that integrates military and civilian scientific-technological resources, and that organically integrates basic research, applied R&D, product designing and manufacturing, and procurement to technologies and products so as to create a good structure under which military and civilian high technologies are shared and mutually transferable."*[76]
>
> Hu Jintao, Former President, People's Republic of China

Dating back to the 1970s, China has implemented a policy of civil-military integration in an effort to reduce research and development burdens and expedite capability modernization.[77] According to the U.S.-China Economic and Security Review Commission (USCC), the concept was originally implemented to spur commercial development.[78] However, the concept eventually shifted when commercial technologies grew significantly in the 1990s, leading the Chinese government to drive its military development off commercial successes.[79]

As stated in the USCC's 2010 Annual Report to Congress,

> "From the late 1970s into the 1990s, China promoted policies that required China's defense industry to support the development of China's civilian economy. However, in the late 1990s, Beijing reversed the direction of civil-military integration to capitalize on China's growing civilian economy as a means to develop its moribund defense economy. As the [USCC] heard during a meeting in Beijing with the Ministry of Science and Technology, collaboration on research between the commercial and defense sectors occurs when 'goals are consistent,' minimizing the use of resources on similar projects."[80]

---

[76] "Annual Report to Congress: Military Power of the People's Republic of China. The United States Department of Defense. 2008. Page 31.

[77] "2010 Report to Congress of the U.S.-China Economic and Security Review Commission. U.S.-China Economic and Security Review Commission. November 2010. Page 100.

[78] "2010 Report to Congress of the U.S.-China Economic and Security Review Commission. U.S.-China Economic and Security Review Commission. November 2010. Page 100.

[79] "2010 Report to Congress of the U.S.-China Economic and Security Review Commission. U.S.-China Economic and Security Review Commission. November 2010. Page 100.

[80] "2010 Report to Congress of the U.S.-China Economic and Security Review Commission. U.S.-China Economic and Security Review Commission. November 2010. Page 100.

In 2003, China implemented a series of official slogans to articulate the goals of civil-military fusion, which the USCC summarized as[81]

- *Combine civil and military needs* – focus on increasing the amount and pace of both military-to-civilian and civilian-to-military technology transfers;
- *Locate military potential in civilian capabilities* – establish civilian enterprises that are able to satisfy the requirements of the military and defense economy;
- *Promote coordination and cooperation* – promote close cooperation among various commercial and military entities involved in research and development; and
- *Conduct independent innovation* – ensure that China is self-reliant when it comes to developing its military equipment.[82]

In March 2018, the U.S. Trade Representative (USTR) published a report describing civil-military fusion as follows,

> "The Chinese government's interest in securing advanced technology through outbound investment reflects both economic and national security objectives. The close relationship between these objectives is reflected in the strategy of 'military-civil fusion' (MCF), which is an important driver of government policy and outbound investment patterns. In 2016, China established the country's first MCF fund which allocated CNY 2 billion ($302 million) to fund domestic projects and overseas acquisitions. Elevated as a national security strategy by General Secretary Xi in 2014, MCF embodies China's national strategic philosophy of coordinating the planning of economic development and national security to fully realize the rejuvenation of the Chinese nation. MCF emphasizes indigenous development, restriction of inbound FDI, and the absorption of foreign technologies and know-how in key sectors. The PLA has drawn a direct link between MCF policy and overseas investment.
>
> As a national security strategy, MCF cuts across economic and industrial development, talent, and military modernization plans. It calls for the development of integrated MCF information-sharing platforms and MCF industry demonstration bases to facilitate S&T

[81] "2010 Report to Congress of the U.S.-China Economic and Security Review Commission. U.S.-China Economic and Security Review Commission. November 2010. Page 100.

[82] "2010 Report to Congress of the U.S.-China Economic and Security Review Commission. U.S.-China Economic and Security Review Commission. November 2010. Page 100.

> resource sharing and collaboration between state laboratories, the PLA, and enterprises, including foreign companies and Sino-foreign joint ventures."[83]

This analysis underscores the likelihood of stolen intellectual property being assigned to (and even motivated by) military applications. Huawei's technological growth, and that of other leading Chinese technology companies, has the potential to enhance such activities. This underscores the difficulty – and lack of practical means – of distinguishing between the commercial activities of a Chinese company and the government, Communist Party, or PLA.

[83] "Findings of the Investigation into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation Under Section 302 of the Trade Act of 1974." Office of the United States Trade Representative Executive Office.

4) Examples of China Using Its Economic Weight for Coercion, Influence

Would China use a position of leverage for political, economic or geostrategic gain? The examples listed below demonstrate that have done so repeatedly. The first several below were catalogued by the Center for New American Security.[84]

Greece Blocks EU Consensus on Criticizing Human Rights Violations in China

In June 2017, Greece reportedly blocked an EU consensus statement at the UN criticizing China's record on human rights. It was the first instance of the EU failing to make this joint statement before the UN Human Rights Council. A Greek representative from its Ministry of Foreign Affairs called it "unconstructive criticism of China." As noted by *Reuters*,

> "…as business ties grow, the bloc is struggling to speak out against a Chinese government crackdown on human rights lawyers and other activists since 2015. China's COSCO Shipping, owner of the world's fourth-largest container fleet, took a 51 percent stake in Greece's largest port last year."[85]

In the lead-up to this event, Greece had been in the process of courting significantly higher levels of Chinese trade and investment and, it hoped, a prominent place for its ports along China's Belt and Road Initiative. As noted by the *New York Times*,

> "Greece is increasingly courting Chinese trade and investment as it faces pressure from international creditors and a cold shoulder from its traditional rich allies in Europe. China's largest shipping company, known as China COSCO Shipping, bought a majority stake last year in the Greek port of Piraeus. The Greek prime minister, Alexis Tsipras, has visited China twice in two years. And China will be the 'country of honor' at Greece's annual international business fair in September in the port of Thessaloniki."[86]

---

[84] "China's Use of Coercive Economic Measures." Peter Harrell, Elizabeth Rosenberg, Edoardo Saravalle. Center for a New American Security. June 2018.

[85] "Greece Blocks EU Statement on China Human Rights at UN." Robin Emmott, Angeliki Koutantou. Reuters. June 18, 2017.

[86] "In Greece, China Finds an Ally Against Human Rights Criticism." Nick Cumming-Bruce, Somini Sengupta. New York Times. June 19, 2017.

Hungary, Greece Reportedly Among Countries Blocking EU Declaration Calling on China to Uphold Hague Ruling on South China Sea

On July 14, 2017, EU diplomats declared that an effort to issue a joint statement that would urge China to abide by an arbitrator's ruling on its disputed claims in the South China Sea had failed. Three countries (reportedly Hungary, Greece and Croatia) withheld their support. The pursuit of Chinese infrastructure investment by Hungary and Greece were flagged by diplomats and expert observers as likely influential in their decision (i.e., to avoid upsetting Beijing and deterring economic and financial engagement).[87]

Rare Earths Exports to Japan Halted to Secure Return of of Detained Trawler Captain After Collision, 2010

A Chinese trawler captain was detained by the Japanese government after he collided with a Japanese patrol boat in September 2010 while operating in the vicinity of the Senkaku Islands. When the captain was not immediately returned, China halted the export of rare earths to Japan, which was significantly dependent on these materials for its high-tech manufacturing industry. At the time, China had a monopoly position, mining some 99% of the world's supply. This leverage was used against Tokyo to influence Japan's judicial treatment of the Chinese national in this incident. Later, in 2014, when tensions rose again over the islands, Beijing reportedly encouraged boycotts of Japanese goods and permitted protests that damaged the property of Japanese companies operating in China.[88]

Nobel Peace Prize Decision Prompts Economic Penalty in Search of Formal, Government Apology

After the Chinese dissident, Liu Xaobo, was awarded the Nobel Peace Prize in 2010, China reportedly demanded a public and private apology. When that was not forthcoming, punitive economic measures were taken, cutting off trade talks and implementing regulatory obstacles that curtailed significantly the import of Norwegian salmon. In 2016, Norway eventually made some public acknowledgements of China's sovereignty and that it had harmed the "mutual trust." As noted by CNAS, "Salmon exports to China quickly resumed as did trade talks between the two countries. During the economic coercion campaign, Norway declined to meet the Dalai Lama in 2014, and upon Liu's death in 2017 it issued a muted statement noting the passing."[89]

---

[87] "China's Use of Coercive Economic Measures." Peter Harrell, Elizabeth Rosenberg, Edoardo Saravalle. Center for a New American Security. June 2018.

[88] "China's Use of Coercive Economic Measures." Peter Harrell, Elizabeth Rosenberg, Edoardo Saravalle. Center for a New American Security. June 2018.

[89] "China's Use of Coercive Economic Measures." Peter Harrell, Elizabeth Rosenberg, Edoardo Saravalle. Center for a New American Security. June 2018.

Dispute with Philippines over Scarborough Shoal Leads to Punitive Measures, 2010

After clashes with China over disputed Scarborough Shoal in the South China Sea in 2012, China took several steps designed to use economic coercion to influence the willingness of the Philippines to persist. These included adding extra controls on agricultural imports and restricting Chinese tourist travel to the country. These measures got worse when the Philippines put the dispute to an international tribunal. Under the leadership of President Duterte, after winning the arbitration decision, the Philippines took very little – if any – action to assert and defend its legitimized claims.[90]

Mongolia Economically/Financially Penalized for Hosting Dalai Lama, 2016

After Mongolia hosted the Dalai Lama in November 2016, China reportedly expressed its displeasure by raising fees on Mongolian mining exports, limiting cross-border traffic and ceasing discussion of a major loan. According to CNAS, "The Chinese cutoff of assistance loan talks, in particular, exacerbated the coercive effect on Ulaanbaatar and accelerated the country's deteriorating fiscal situation, to which the International Monetary Fund (IMF) eventually responded with a bailout. Although it initially stood up to Chinese coercion, the Mongolian government eventually offered a public apology to Beijing, including a promise not to host the Dalai Lama in the future."[91]

Influence Over News Media Censorship Questioned in Australia

In April 2014, the international arm of the Australian Broadcasting Corporation (ABC) signed a large deal with the state-backed Shanghai Media Group that promised unprecedented access to Chinese audiences. The agreement was later discovered to include a provision whereby ABC had agreed to censor its news coverage of content that was objectionable to Beijing from its Mandarin-language services – not just in China, but also in Australia and overseas. As described in an article, entitled "What is Sharp Power," by Christopher Walker of the National Endowment for Democracy, this was,

> "…a grave compromise of the journalistic integrity of the taxpayer-funded Australian broadcaster." China, he wrote, had "induced the Australians to muzzle an important independent voice."[92]

---

[90] "China's Use of Coercive Economic Measures." Peter Harrell, Elizabeth Rosenberg, Edoardo Saravalle. Center for a New American Security. June 2018.

[91] "China's Use of Coercive Economic Measures." Peter Harrell, Elizabeth Rosenberg, Edoardo Saravalle. Center for a New American Security. June 2018.

[92] "What is "Sharp Power"?" Journal of Democracy. July 2018.

Australia 5G Decision Followed by Punitive Import Bans

After Australia excluded Huawei and ZTE from its 5G network in August 2018, some important agricultural exports, such as canola, were banned from China. Coal imports from Australia were also held up at China's Dalian Port. Both sides denied there was a connection, but there was significant speculation that these moves were punitive.[93]

Suppressed Opposition to Uighur Persecution

It is also noteworthy that despite China's imprisonment of hundreds of thousands – if not millions – of Muslim Uighurs in Xinjiang Province to suppress the Muslim community and elevate the preeminence of the ethnical Han population, most Muslim countries, including those that objected to Myanmar's treatment of the minority, Muslim Rohingya population, have been silent on this issue. It likely stems from a fear of retribution. As reported by Brahma Chellaney in the Australian Strategic Policy Institute,

> "Pakistan's military-backed prime minister, Imran Khan, has feigned ignorance about the Xinjiang crackdown, and Saudi Arabia's powerful crown prince, Mohammed bin Salman, has gone so far as to defend China's right to police 'terrorism'."[94]

[93] "Australia's Huawei 5G ban if a 'hedge' against future Chinese aggression, says former prime minister Malcolm Turnbull." South China Morning Post. March 29, 2019.

[94] "Global silence on China's gulag." Australian Strategic Policy Institute. April 9, 2019.

Conclusion

The Chinese government's notorious reputation as a state-sponsor of economic espionage and intellectual property theft in the cyber domain, combined with the nature of the authoritarian regime, undermines the ability of Huawei – and other technology companies – to distinguish itself as an independent private sector actor. The rules of the regime with regard to state control have been openly documented by them and touted via public comments from senior officials that reject any separation of powers that limit the reach of the Chinese Communist Party and its leadership.

Like any other company in China, Huawei will have difficulty plausibly characterizing itself as being free from the CCP's dominance over industry. In fact, the telecommunications industry, specifically, has long been a direct target of Chinese government influence and support. For over a decade, the Chinese government has singled out telecommunications as a so-called "chosen industry." According to the USCC's 2007 Annual Report to the U.S. Congress, when the Chinese government identifies a strategic industry, the State must then maintain "absolute control through state-owned enterprises."[95]

"Like any other company in China, Huawei will have difficulty plausibly characterizing itself as being free from the Party's – and the government's – dominance over industry."

"An airtight engineering solution does not resolve the problem of the Chinese government's track record of cyber abuses, its ability to use its companies as vehicles for such abuses, and its continuing strategic agenda as being defined by economic and political ascendancy – and eventual superiority – of the country's communist ideology over liberal democracy and capitalism."

The contents of this report, for the most part, highlight non-technical risk factors that are present in doing business with Chinese entities, like Huawei, in the cyber domain. These risk factors persist, however, even when a more technical scrub of a company's hardware and software might deliver a clean bill of

[95] "2007 Report to Congress of the U.S.-China Economic and Security Review Commission." U.S.-China Economic and Security Review Commission. November 2007. Page 4.

health. An airtight engineering solution does not resolve the problem of the Chinese government's track record of cyber abuses, its ability to use its companies as vehicles for such abuses, and its continuing strategic agenda as being defined by the need for economic and political ascendancy – and eventual superiority – of the country's communist ideology over liberal democracy and capitalism.

The GCHQ signals intelligence agency of the UK government declared – after 8 years of running a special center specifically designed for the purpose of monitoring Huawei's involvement in the country's telecommunications infrastructure – that the company's "approach to software development [brings] significantly increased risk to UK operators" and that "it will be difficult to appropriately risk-manage future products in the context of UK deployments, until the underlying defects in Huawei's software engineering and cyber security processes are remediated."[96] In addition to the problems implied by this conclusion, it is worth noting that, even if such technical issues were fully addressed, significant issues of trust would remain.

At this point, given what is available in the public domain, those governments and companies that choose to accept these risks will be left to hope that their vulnerabilities are not exploited by Chinese government-backed actors that have a clearly demonstrated and publicly available track record of doing so in the past.

Ultimately, this problem is about risk – the risk of having one's economic assets stolen, the risk of having personal and government data hacked, and the risk of being vulnerable to coercion, influence and control by a government with vastly different political values and principles.

At this point, given what is available in the public domain, those governments and companies that choose to accept these risks will be left merely to hope that their vulnerabilities are not exploited by Chinese government-backed actors that have a clearly demonstrated and publicly available track record of doing so in the past.

[96] "British spy agency delivers scathing assessment of security risks posed by Huawei to U.K. telecom networks." The Washington Post. March 28, 2019.

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.

RWR Advisory Group LLC