Norwegian School of Economics
Bergen, Spring 2021

U.S. Punitive Measures Against Foreign Firms

A Case Study of Huawei Technologies

Benjamin Hui

Supervisor: Professor Jan I. Haaland

Master thesis, MSc in Economics and Business Administration,
International Business

NORWEGIAN SCHOOL OF ECONOMICS

Abstract

This thesis is a study on U.S. punitive measures against foreign firms. Based on the U.S. government's campaign on Huawei Technologies, it shows how U.S. punitive measures may inflict profound financial impact on the targeted firm and some of its key stakeholders, how punitive measures may cause further implications beyond the intended purposes, and how punitive measures may be inconsistent with the rules under the WTO system.

Based on the findings, a theoretical framework for determining the optimal strategy against punitive measures imposed by a foreign government has been created. The framework provide concrete suggestions on how a firm should counter punitive measures, based on the two general dimensions of (1) how severely the punitive measures impact the firm, and (2) the ease for the firm to find alternative (input or output).

Acknowledgement

I would like to express my sincerest gratitude to my supervisor, Professor Jan I. Haaland. Firstly, for his excellent course on *Globalisation and Integration*, which helped inspire me to write this thesis. Secondly, for sharing so generously his vast knowledge and insight in the field of international trade and business. Last, but not least, for his support, guidance, and patience throughout my research process.

Clarification of Terminology

Punitive measure:

In this thesis, the term punitive measure is used as an all-inclusive term to cover “any measure that is damaging to the firm targeted”. Within the literature, the term sanction is frequently used to describe this type of measure; however, a sanction is often understood as a negative reaction for disobeying a law or a rule (Cambridge dictionary, n.d., Definition 2). However, a punitive measure might be imposed without judicial justification, and governments may intentionally be ambiguous when imposing such measure so not to be perceived as a sanction.

From a firm-level perspective, the semantics of whether a measure is a sanction or not is not essential; what is, from a managerial point of view, is the economic implications a punitive measure will inflict on the firm.

The term punitive measure is also used to avoid the mix-up between a sanction as a general penalty, and a violation of the U.S. sanctions programme. To further clarify, a sanction is indeed a punitive measure, but a punitive measure is not necessarily a sanction.

Contents

1. Introduction

On 14 December 2009, Oslo became the first city in the world where commercial 4G mobile network was made available to the public. At that time, not many outside the telecommunications industry would be familiar with the name of the firm that supplied the technology – Huawei. A decade later, many countries have been preparing to roll-out the fifth-generation mobile networks, also known as 5G. Huawei will again play a crucial role in the deployment of the technology, but as it does, it enjoys a far greater brand recognition than it did a decade ago. This greater brand recognition is partly due to the growth of its consumer electronic products, including smartphones, tablets, and laptops. It is also, and perhaps more so, due to an aggressive campaign launched by the U.S. government against the firm – where Huawei has been on the receiving end of a wide range of punitive measures.

Few firms have been imposed more punitive measures by the U.S. government than what Huawei has been facing in the past decade. Among the many U.S. punitive measures imposed on the firm are: blocking its deals with U.S. firms; forcing it to divest its U.S. assets; imposing a travel ban on its employees; adding it to its trade blacklist; arresting its CFO; banning its equipment from being used within the U.S. market; and pressuring other nations also to ban its equipment from their markets.

From an international business perspective, the U.S.'s campaign against Huawei is interesting for at least two reasons: Firstly, because it illustrates the different tactics the U.S. government is willing to employ on foreign firms to protect its interests. Secondly, because international firms can better assess the political risks they face when operating in foreign markets. Accordingly, the purpose of this thesis is to answer the following questions:

1. How can U.S. punitive measures impact the targeted firm and other stakeholders?

2. How do these punitive measures stand in the context of international trade rules?

3. How can firms prevent or cope with punitive measures imposed by foreign governments?

2. The Huawei Case

2.1 Historical background

Huawei Technologies was founded in 1987 by Ren Zhengfei, a former engineer in the People's Liberation Army, China's armed forces. Ren established Huawei in the coastal city of Shenzhen, in the southern province of Guangdong, and the closest neighbouring city of Hong Kong. In 1980, Shenzhen had been designated by the Chinese government as a special economic zone, enjoying "special financial, investment and trade privileges" (Zeng, 2010, p. 9). The government's goal was to use Shenzhen as a test lab for the country's changing policy from a planned economy to a market economy.

In the first years of business, Huawei's primary source of revenue came from reselling private branch exchange switches[1] imported from Hong Kong. At that time, China did not have its own national telecommunication equipment industry and therefore relied on imports. Huawei's vision was to become a firm that could compete with major international telecom firms, such as Ericsson, Alcatel, Motorola, and Nokia. While many Chinese firms opted to enter international joint-ventures with foreign firms, which was a common strategy for many Chinese firms that lacked technological know-how, Huawei chose to invest heavily in R&D to develop its technology in-house.

By 1993, Huawei had successfully developed its own large-scale switch. It had also strategically chosen to serve the rural areas of China, while major international firms only had a significant market presence in China's most advanced cities. With no major competitors in the rural areas, Huawei quickly captured the market shares of these areas. As its revenue continued to grow, it kept scaling up its R&D investments and expanding its product focus to routers and mobile communications equipment. Its innovation strategy focused on reverse engineering basic products and then develop more advanced products based on the original ones. It also was an eager purchaser of international consulting services, especially IBM consultants who helped organise and manage its R&D processes (Ahrens, 2013).

[1] Private Branch Exchange (PBX) is a switch system that allows for intercommunication between telephones within an organisation without using external telephone lines

In the mid-1990s, the Chinese government revised its telecommunications equipment policy to reduce its reliance on imports and promote its domestic manufacturers (DeWoskin, 2001). Fronted as a national champion, Huawei's sales in the cities and other urban areas expanded. It also received sizeable loans from state-owned banks, which with the government's new policy, is likely to have come with favourable terms and conditions.

By the late-1990s, Huawei started pushing for international expansion, primarily in other developing markets. In 1997 it entered the Russian market, followed by Thailand, Brazil, and South Africa. Suffering from negative country-of-origin effects at the time, as a Chinese manufacturer, it had to undercut international prices to win contracts abroad. Through its cost innovation strategy[2] and settling for lower profit margins, it was able to expand in several developing markets successfully. In 2001, Huawei pushed for international expansion in developed markets, including the Netherlands, Germany, France, and the United States. While it was able to win projects in the European countries, it was not able to do so within the first three years in the American market.

In 2005, Huawei's overseas markets revenue exceeded its domestic market revenue. Seven years later, in 2012, it surpassed then global telecommunications leader, Swedish Ericsson, in both sales' revenue and net profit (De Cremer & Tao, 2015).

In 2009, Swedish network operator TeliaSonera chose Huawei as a partner to build out the first 4G networks in the world, in the Nordic capitals of Stockholm and Oslo[3] (Financial Times, 18 December 2009). It represented a milestone for the Chinese telecom firm, as it illustrated how Huawei had successfully managed to develop its own cutting-edge technology that could compete with European industry leaders, such as Ericsson's and Nokia's.

Since 2009, Huawei's global market share of telecommunications equipment has continued to increase. In the 2010s, the firm also increased its focus on developing smartphones. By 2020, Huawei had become the technological leader of the 5G network deployment. In the second

[2] A strategy centred in deploying cost advantages from emerging economies to radically offer customers "dramatically more utility for less expenditure" (Williamson, 2009, p. 433)

[3] Huawei's build-out of 4G in Oslo is also mentioned in Chapter 1.

quarter of 2020, its smartphone shipments exceeded that of both Samsung and Apple, making it the world's largest smartphone manufacturer in that quarter.

2.2 U.S. government's punitive measures against Huawei

The U.S. government's campaign against Huawei follows a series of accusations against the Chinese telecommunications firm. These accusations include that it has been stealing trade secrets from the U.S. and violating its Iran sanctions; that its telecom equipment poses a national security threat; that it has been given an unfair amount of subsidies by the Chinese government, and that it is under the control or strong influence of the Chinese military. As a result, the U.S. government has imposed a series of punitive measures against the firm. This section will present these punitive measures in a chronological order.

March 2008: Blocking Huawei's deal with U.S. electronics manufacturer 3Com

On September 2007, U.S. private equity firm Bain Capital partnered with Huawei Technologies to purchase U.S. electronics manufacturer 3Com, giving Huawei a 16.5 per cent stake and board representation. The deal was called off after the U.S. Committee on Foreign Investment in the United States (CFIUS) signalled it would block the transaction. In the backdrop, U.S. lawmakers raised concerns that the deal would threaten U.S.' national security due to allegations that Huawei had close ties to the People's Liberation Army (Reuters, 23 February 2008).

December 2010: Political pressure for U.S. Sprint Nextel to rejects Huawei bid to upgrade its mobile carrier network

On December 2010, U.S. mobile network operator Sprint Nextel rejected Huawei's bid to upgrade its mobile carrier network, choosing French Alcatel, Swedish Ericsson and Korean Samsung to work with its projects. The move came after intense political pressure from U.S. lawmakers to reject Huawei's bid for their projects, citing national security concerns. The U.S. Commerce Secretary Gary Locke was reported to have made a personal telephone call to Sprint Nextel's CEO to express his deep concerns over Huawei's bid (Bloomberg, 7 December 2010), and a letter by U.S. lawmakers stated that they found it "most troubling" that Huawei's founder had been a member of the People's Liberation Army (Reuters, 24 August 2010).

February 2011: Blocking Huawei's acquisition of US-firm 3Leaf Systems technology

In May 2010, Huawei made a relatively small purchase at USD 2 million of assets from an insolvent U.S. server technology firm, 3Leaf Systems. It had sought and received approval for its acquisition of the U.S. firm's technology from the U.S. Bureau of Industry and Security (BIS). However, the U.S. Committee on Foreign Investment in the United States (CFIUS) had not given its approval and requested the deal be sent for their review. Huawei argued that approval from BIS, an agency under the U.S. Department of Commerce, was sufficient to complete the deal. CFIUS consequently blocked the transaction, based on national security concerns, ordering Huawei to divest its acquired asset, and banning Huawei from hiring any of its employees (Reuters, 19 February 2011)

October 2012: U.S. House of Representatives' Select Committee on Intelligence's report

In October 2012, the U.S. House Representatives' Select Committee on Intelligence published a report[4] after investigating both Chinese telecommunications firms, Huawei and ZTE. In the committee's report, it raised strong concerns over Huawei's ownership structure, its loan scheme to its customers, its commercial relationship with Iran, and its continued suspicion on the firm's ties to the Chinese government and military. However, the report failed to find any clear evidence of wrongdoings by Huawei. An 18-month investigation ordered by the White House also found no clear evidence of wrongdoings but highlighted the potential of a security issue (Reuters, 17 October 2012). Both reports would serve as a cautious warning to U.S. firms considering collaborating with Huawei.

January 2018: Political pressure for U.S. carrier to pull out of a partnership with Huawei

In January 2018, Huawei was expected to announce its partnership with U.S. carrier AT&T to sell its smartphones in the U.S. market. However, following a letter from U.S. Senate and House Intelligence Committee members sent in December 2017 to the U.S. Federal Communications Commissions, raising concerns over the specific deal between Huawei and AT&T, the latter party chose to pull out from the deal (Reuters, 8 January 2018).

[4] The full title of the report is *The Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*.

December 2018: Huawei CFO arrested in Canada at the request of the U.S. government

On 1 December 2018, Huawei's CFO and daughter of founder Ren Zhengfei, Meng Wanzhou, was arrested at Vancouver International Airport at the request of the U.S. Department of Justice (Reuters, 5 December 2018). The U.S. charged Meng and Huawei over bank and wire fraud in violation of U.S. sanctions on Iran and requested her to be extradited to U.S. soil. The move has caused relations between China and Canada to deteriorate. During the time of arrest, U.S. and China were engaged in a trade war and in an interview with Reuters on 12 December 2018, President Trump said he would be willing to intervene in Meng's case if it would help his administration close a trade deal with China (Reuters, 12 December 2018). President Trump's comment reinforced speculation that the arrest of Meng was politically motivated and used as a bargaining chip during the trade war between the U.S. and China.

15 May 2019: U.S. firms barred from buying Huawei equipment while adding Huawei to the U.S. trade blacklist

On 15 May 2019, President Trump issued an executive order declaring foreign adversaries' threats in the information and communications technology and services supply chain a national emergency (White House, 2019). The move was seen as directed towards Huawei, as the executive order would bar U.S. firms from using telecommunication equipment made by firms deemed by the U.S. government as posing a national security risk. In a parallel move, the U.S. Commerce Department added Huawei and 70 affiliates to its Entity List – effectively banning the firm from buying any parts and components from U.S. firms unless given special-granted license from the government (Reuters, 16 May 2019). The move was a critical blow for Huawei, which relies heavily on U.S. semiconductors to produce its telecommunications equipment and smartphones. It also prompted Google to cut off future Huawei smartphones from receiving Android operating system updates and access services like Gmail and Google Play, putting Huawei smartphones at a significant disadvantage.

May 2020: U.S. Commerce Department expands its restriction on Huawei's ability to access U.S. technology

On 15 May 2020, the U.S. Commerce Department further tightened its control on Huawei's supply chain. It required any firm, both U.S. and non-US, who has had its products been

designed or made using US-produced technology or hardware, to require special license to be able to sell to Huawei (Reuters, 15 May 2020). The difference from the 15 May 2019 restriction is that the first restriction only affected US-based firms. The 15 May 2020 restriction would also limit firms abroad who might have some U.S. technology in its product component mix to trade with Huawei.

July 2020: U.S. State Department imposes travel ban on Huawei employees

On 15 July, Secretary of State Mike Pompeo announced that the State Department would impose visa restrictions on "certain Huawei employees" under the allegations that they provide material support to the Chinese government to commit human rights abuses (Reuters, 15 july 2020). The basis of the move was likely to be related to U.S. allegations that Huawei's telecommunications equipment was being used in the Xinjiang province of China. In this province, the U.S. has accused China of abusing the human rights of one of the region's ethnic minorities, the Uighurs.

2018-2020: Exerting pressure on other nations to ban Huawei from their 5G roll-out

The U.S.' aggressive campaign against Huawei goes beyond its national borders. According to reports, U.S. officials have exerted pressure, scolded, and threatened other nations, against using Huawei in the roll-out of 5G networks in their respective nations (The New York Times, 17 March 2019).

One of the threats directed to some of the U.S.' closest allies involved withholding intelligence sharing if the countries were to choose Huawei in their 5G networks. While the U.S.' aggressive tactics initially were met by resistance from other nations, several nations have since eventually decided to formally ban the Chinese telecommunications firm, while other nations has imposed technical barriers to restrict Huawei from their markets. According to one report, the British government privately admitted to Huawei that it had switched its position from allowing Huawei to participate in building its 5G networks to banning it due to tremendous pressure from the U.S. government (Bloomberg, 18 July 2020).

As of March 2021, countries besides the U.S. that has formally banned Huawei include Sweden, Australia, the U.K., Japan, Poland, and Romania. France.

3. The financial and economic impacts of Huawei restrictions

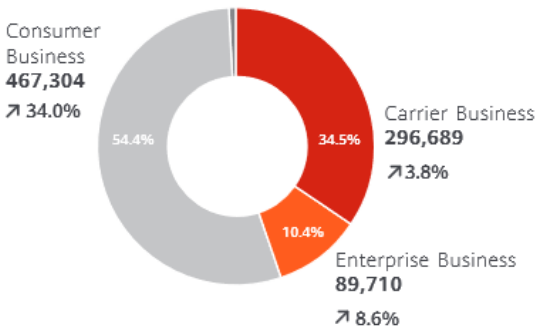
This section will attempt to identify some of the financial and economic impacts of the punitive measures against Huawei by the U.S. government. It will focus on three different perspectives: the first one is the financial impact on Huawei itself, the second one is the financial impacts on some of Huawei's top suppliers, and the third one is on the economic impact on the European market. This section aims to highlight some of the important implications of U.S.'s campaign on Huawei following the series of punitive measures launched against the firm.

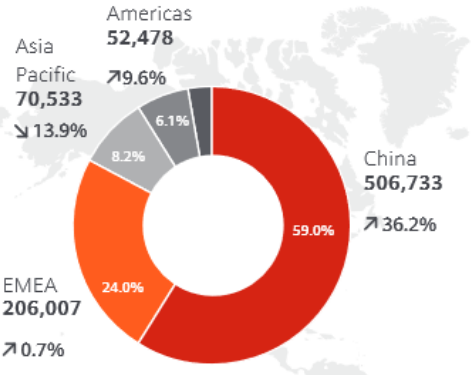
3.1 The financial impact of the punitive measures on Huawei

The punitive measures against Huawei have had both broad and severe reach on the Chinese telecom giant. The series of punitive measures have first and foremost impacted Huawei's two main business areas: its consumer electronics business and its carrier network business.

(CNY Million)	2019	2018	YoY
Carrier Business	**296,689**	285,830	3.8%
Enterprise Business	**89,710**	82,592	8.6%
Consumer Business	**467,304**	348,852	34.0%
Other	**5,130**	3,928	30.6%
Total	**858,833**	721,202	19.1%

(CNY Million)	2019	2018	YoY
China	**506,733**	372,162	36.2%
EMEA	**206,007**	204,536	0.7%
Asia Pacific	**70,533**	81,918	(13.9)%
Americas	**52,478**	47,885	9.6%
Other	**23,082**	14,701	57.0%
Total	**858,833**	721,202	19.1%





Source: (Huawei, 2020)

Together these two segments constituted the lion share of Huawei's total revenue[5] of USD 123 billion: its consumer business's revenue was at USD 66.5 billion. Its carrier network business's revenue was at USD 42.7 billion in 2019 (Huawei, 2020).

Huawei's consumer business was severely affected when the firm was added to the U.S. entity list on 15 May 2019. A few days later, a Google spokesperson revealed that the firm would suspend its business operations with Huawei to comply with the U.S. government's imposed restrictions (Reuters, 19 May 2019). Following that decision, Huawei smartphones were no longer able to access updates on its Android operating system. Huawei's next version smartphones would no longer have access to Google Play Store and Google applications such as Google Maps and Gmail. Lack of such applications put Huawei's smartphones at a considerable competitive disadvantage compared to its main competitors, and many consumers were expected to switch to other smartphone brands that did not have these restrictions. Shortly after, many phone carriers discarded their plans to sell Huawei smartphones, as estimated demand for the phones plummeted.

Huawei estimated that the trade blacklisting would reduce the firm's sales by over USD30 billion over the next two years, and a 40% decline in smartphone sales outside China in 2019 (Bloomberg, 16 June 2019). This represented a loss of sale of 40-60 million smartphone units, a substantial share of its total 206 million shipped smartphone units in 2019. In the first quarter of 2020, Huawei's smartphone shipments outside China dropped by 35%. While this was during a period of slow global demand for smartphones due to the COVID-19 pandemic, the drop in shipment was twice and four times larger than the decline of its rivals Samsung and Apple, respectively (Strumpf, 2020), and industry analysts expect Huawei's smartphone business to continue to decline by 60-70% in 2021 (Nikkei, 23 October 2020).

Huawei's carrier network business is also expected to decline overseas, as the U.S. government has successfully pressured some of its allies to exclude Huawei from its 5G networks. Huawei was the global leader of 4G networks; however, following recent geopolitical development, its market share in Europe and Australia is expected to drop significantly following potential bans from Western markets. Huawei's main competitors, Nokia and Ericsson, is expected to

[5] Converted from Chinese Yuan (CNY) to United States dollar (USD) using the closing exchange rate at the end of 2019 of USD1.00 = CNY6.9840

overtake Huawei's market share, and Nokia reported in June 2019 that it had surpassed Huawei in the number of commercial orders on 5G telecom equipment with 52 orders, compared to Huawei's 50 orders (Reuters, 3 June 2019).

While there are few estimates of these 5G commercial orders' value, it is expected to take a considerable portion off Huawei's USD 42.3 billion carrier network business and slow its future growth opportunities drastically.

The punitive measures have also impacted Huawei by severely disrupting its supply chain. The export restrictions set by the U.S. government has limited Huawei's ability to access critical components for most of its products, in particular semiconductors, which are essential for the functioning of Huawei's main products, i.e., telecommunications hardware, smartphones, tablets, and laptops.

While Huawei initially reacted to the export restrictions by stockpiling semiconductors before the restriction went into effect (Bloomberg, 22 October 2020), these stockpiles will eventually become depleted. Without the supply of semiconductors, and while not currently able to produce its own, Huawei will struggle to manufacture most of its products and cripple its ability to manufacture smartphones and telecommunications equipment – its two main business segments. This is likely to have an enormous financial impact on Huawei, as its ability to generate revenue is severely threatened.

The combined effects of Huawei's severely limited access to critical inputs for their smartphones and the lack of access of Google's Android software was likely the reason for Huawei's decision to sell its budget smartphone brand *Honor*. In the official announcement, Huawei stated that its consumer business had been “under tremendous pressure […] due to a persistent unavailability of technical elements needed for [its] mobile phone business" (Huawei, 2020). After the sale, *Honor* was expected to be released from any U.S. restrictions.

Some industry analysts also believe that the decision was motivated to raise cash that it would use to invest in its own chip-making technology, as the U.S.'s restrictions have forced the firm to become more self-reliant (BBC, 17 November 2020). In November 2020, Huawei was reported to be working on plans for a chip plant in Shanghai that would avoid any usage of U.S. technology in its component mix (Financial Times, 1 November 2020). This move will

come at an incredibly high cost for the firm, as semiconductor manufacturing requires one of the highest R&D and capital expenditures by any industry (Bown, 2020).

Additionally, Huawei has also suffered significant reputational damage following the U.S.'s campaign against the firm. Media coverage on Huawei has primarily focused on U.S.'s security and espionage allegations, which is likely to deter many consumers who otherwise would be favourable to using Huawei products from purchasing them.

3.2 The financial impact of the punitive measures on Huawei's suppliers

As one of the world's largest telecommunication equipment providers and smartphone manufacturers, Huawei has been an important customer to many of its suppliers. Recalling from Chapter 2.2, when the U.S. government added Huawei on the U.S. entity list on 19 May 2019, it prohibited U.S. firms from selling products or services to Huawei without a government-designated license. While the move targeted Huawei in an attempt to cripple its ability to produce 5G equipment, on the other side were many U.S. firms who no longer could sell their products or services to Huawei.

Following the announcement that Huawei would be placed on the U.S. entity list, many U.S. suppliers reduced their financial forecasts to adjust to the announced export restrictions. A report by investment bank Goldman Sachs identified Huawei's key U.S. suppliers and estimated the sales revenue those suppliers derived from Huawei in the third fiscal quarter of 2018 (Reuters, 16 May 2019). The report also estimated the exposure each supplier had to Huawei by calculating each suppliers' sales revenue to Huawei in relation to each suppliers' total revenue. It found more than eight U.S. firms to derive 5 per cent or more from Huawei in the third fiscal quarter of 2018, with one supplier, NeoPhotonics, deriving almost half of its total revenue from the Chinese telecom giant.

In Table 1, the estimates from the Goldman Sachs report are reproduced to illustrate how Huawei's largest U.S. suppliers might be affected by the export restrictions imposed by the U.S. government. Although their sales revenues from Huawei are considerable in dollar terms, some larger firms might have less exposure due to their sheer size. On the other hand, smaller

firms are likely more affected as their percentage of sales revenue from Huawei is significant compared to their total sales revenue.

Table 1: Top U.S. Suppliers to Huawei Q3 2018

Supplier	Industry	Revenue from Huawei (USD million)	% of Total Revenue
NeoPhotonics	Optoelectronic products	252	47
Qorvo	Radio-frequency systems	651	11
Lumentum	Optical and photonic products	223	11
II-VI	Optical devices, semiconductors	165	8
Broadcom	Semiconductors, infrastructure software	2 090	6
Skyworks	Semiconductors (radio frequency and mobile communication systems)	441	6
Qualcomm	Telecom equipment, semiconductors	1 580	5
Flex	Electronics manufacturing, original design manufacturing	2 430	5
Seagate Technology	Computer storage products	829	4
Maxim Integrated	Semiconductors (analog and mixed-signal integrated circuits)	149	4
Analog Devices	Analog, mixed-signal and DSP integrated circuits	338	3
Marvell Technology	Integrated circuits	120	3
Micron Technology	Computer memory, data storage	768	2
Corning	Glass and ceramics materials	369	2
Advanced Micro Devices	Computer processors	268	2
CommScope	Network infrastructure products	188	2
Keysight Technology	Electronic design and test solutions	128	2
Intel	Semiconductors	589	1
Western Digital	Hard disk drives, storage systems	256	1
Microsoft	Software	190	<1

Source: (Reuters, 16 May 2019) with data collected by Goldman Sachs

The figures in Table 1 do not necessarily accurately represent the financial impact on the U.S. suppliers. It is important to recall that some firms might be able to obtain a special license from the U.S. Commerce Department to still supply to Huawei. Reports reveal that some firms were successful in applying for these licenses, particularly firms that supply less-sophisticated technology products that are not related to 5G technology.

Granting some suppliers a special license would reduce the financial impact of the export restrictions on Huawei. However, later reports indicate that the U.S. Commerce Department revoked certain licenses from firms who were previously permitted to do business with Huawei, forcing them to forego sales revenue from Huawei (Reuters, 17 January 2021).

In the short run, Huawei's stockpiling efforts between the announcement of the export restrictions and the time these restrictions went into effect (90 days) would also reduce the suppliers' financial impact, as some suppliers experienced a surge in demand from Huawei.

U.S. export restrictions also impacted non-U.S. suppliers; initially, the U.S. export restrictions forced Huawei to seek suppliers outside the U.S. and did so in firms domiciled in South Korea and Taiwan. But after the Trump administration reinforced its export restriction in May 2020 to also include non-U.S. firms who used any U.S. technology in their component mix, many foreign firms were also impacted by this reinforced export restriction. As the U.S. is the world's leading semiconductor designer, the new restrictions inflicted had a significant financial impact on Huawei's non-U.S. suppliers as well. One impacted supplier is Taiwan Semiconductor Manufacturing (TSMC), the world's largest contract chip manufacturer, who stopped taking new orders from Huawei since the Trump Administration's decision in 2020 (The Wall Street Journal, 16 July 2020). In 2019, Huawei was estimated to account for 15-20% of TSMC's total revenue of approximately USD 35 billion.

The real financial impact to Huawei's suppliers is difficult to estimate and will depend on several factors such as each firm's dependency to Huawei, each firm's ability to find alternative revenue sources, and the U.S. Commerce Department's willingness to approve special licenses. However, it is clear that the imposed export restrictions have created enormous uncertainty, unpredictability and significant loss of revenue to both U.S. and non-U.S. businesses as a consequence of the U.S. government's campaign against Huawei.

3.3 The economic impact on Europe of restricting Huawei from its 5G networks

In the previous parts, the focus was on the financial impact on Huawei and its suppliers, resulting from different punitive measures, particularly the export restrictions. In this part, the focus turns towards the economic impact of restricting Huawei from certain markets, here exemplified by the European market.

In a study by Oxford Economics, the British research agency estimated the costs of restricting Huawei from the 5G networks across 31 European countries, E.U.'s 27 countries in addition to the United Kingdom, Switzerland, Norway, and Iceland (Oxford Economics, 2020). By combining a theoretical model of oligopoly, merger simulation techniques and empirical evidence, the study estimates that restricting Huawei from the European market will increase the annual cost of building 5G networks by 19%, which equates to almost EUR 3 billion per year over the next decade.

The study also estimates that restricting Huawei from the 5G networks competition will delay 56 million European users' 5G access by 2023. With a delayed rollout in 5G, the study also estimates that the reduced 5G access will cause a reduction in technological innovations and economic growth that will lead to an aggregate GDP reduction of an of EUR 40 billion (in 2020 prices) across the 31 European countries in 2035. A summary of country-by-country data is reproduced in Table 2.

While there are few similar studies, some governments have tried to make similar estimates for their respective countries. The U.K.'s National Cyber Security Centre made an analysis where it found that excluding Huawei from the sensitive part of the "core" network would cost the country roughly GBP 1.5 billion and delay the rollout of 5G networks by one year. A full ban of Huawei equipment from the U.K. market, which the U.K. has decided upon as of January 2021, will incur even higher costs and delays in the rollout and seem consistent with the estimates the study by Oxford Economics.

Table 2 The Impact of restricting Huawei from the European 5G-rollout

Country	Increased avg. annual investment cost (EUR million)	Number of people with delayed access to 5G (thousands)	Permanent loss of GDP (EUR million)
Austria	73	1 100	1,100
Belgium	65	1 700	1,100
Bulgaria	20	700	100
Croatia	23	200	80
Cyprus	7	38	40
Czech Rep.	57	1 200	400
Denmark	29	800	600
Estonia	10	130	60
Finland	79	600	400
France	447	4 000	7,300
Germany	479	11 900	6,900
Greece	37	800	600
Hungary	55	500	300
Iceland	3	20	13
Ireland	27	345	700
Italy	283	6 900	4,700
Latvia	8	180	70
Lithuania	8	200	60
Luxembourg	5	50	130
Malta	4	20	40
Netherlands	52	2 100	1,600
Norway	98	600	1,100
Poland	120	3 300	1,000
Portugal	63	1 000	500
Romania	59	2 400	80
Slovakia	31	200	200
Slovenia	15	120	150
Spain	292	5 000	3,700
Sweden	64	1 400	1,100
Switzerland	94	800	1,700
UK	374	7 300	4,400
Total	2 908	55 603	40 223

Source: Oxford Economics (2020)

The study did not consider the costs of replacing Huawei equipment in already existing mobile networks in Europe. There are limited studies on the costs associated with those actions, so-called "rip-and-replace", but the U.K.'s largest provider of broadband and mobile services estimates that it will cost them GBP 500 million to restrict Huawei from its networks. As Huawei has been one of the main equipment providers of the 4G networks in Europe, similar rip-and-replace costs are likely to incur for other countries. However, the actual costs will depend on the scale of telecommunications equipment needed to be removed and replaced is.

While Oxford Economics' study is a comprehensive one, it is still a hypothetical scenario that assumes that Huawei is entirely restricted from the European 5G market. Although some European governments have signalled a full ban on Huawei network equipment, it is doubtful that Huawei is completely restricted from the entire European market.

In January 2020, the European Union published a set of recommendations for its 27 member states with guidelines on restricting or excluding "high-risk 5G vendors" from core parts of their telecommunications networks (European Commission, 2020). Still, the final decision of whether to restrict or not and the degree of restriction is at the discretion of each member state's government. Therefore, the study's estimated costs are not necessarily a plausible representation of the actual costs that would incur. The economic impact is likely to be lower than the estimates indicate. However, the study is useful in understanding the effects that such restrictions cause.

4. Further implications of the punitive measures against Huawei

The previous chapter found high financial and economic costs associated with the punitive measures against Huawei. From the loss of sales revenue for Huawei and its suppliers on a firm-level perspective to GDP loss from reduced competition in the European market and delayed access to 5G usage. This part will discuss further implications beyond the financial and economic impacts that have arisen or might arise from the punitive measures against Huawei.

4.1 Disruptions in the global value chains

In the early months of 2021, automakers announced a sharp cut in their production output following a shortage in semiconductors. One industry analyst estimates that the shortage will reduce the global automotive industry's revenue by USD 110 billion in 2021 due to the lack of semiconductor components (CNBC, 14 May 2021). Semiconductors are crucial for advanced features in cars such as collision warning sensors or self-driving capabilities through LiDAR technology, but also basic features such as power steering and brake systems.

There were several causes of the semiconductor shortage in the automotive industry. The primary cause was the COVID-19 pandemic that shocked global markets in 2020. Firstly, many automakers temporarily shut down their factories for two months to reduce the spread of the COVID-19 virus. Many automakers also voluntarily cut back production and cancelled purchase orders of semiconductors as they expected consumer spending to drop due to the expected economic fallout from the pandemic.

Secondly, semiconductor manufacturers quickly shifted their supply to the electronics industry, which experienced a massive surge in demand. As many countries imposed lockdowns or encouraged workers to work from home, the demand for electronic equipment such as desktops, laptops, monitors and other communication gadgets grew exponentially to facilitate the shift to telecommuting and online learning. When automakers were experiencing higher demand than initially expected, the semiconductor manufacturers had already reached

their maximum production capacity. Therefore, they could not meet the automakers' demand, which led to a severe decline in automobile production (The Washington Post, 1 March 2021).

Another cause comes from several ripple effects of several of the US punitive measures discussed earlier. One of them was the punitive measure against Semiconductor Manufacturing International Corporation (SMIC).

In September 2020, the US Commerce Department notified U.S. firms that they would no longer be allowed to sell their equipment, designs, and software to SMIC before adding the Chinese semiconductor manufacturer to the US entity list on 18 December 2020. The move attempted to cripple SMIC's ability to manufacture its semiconductors, especially its most advanced ones. In 2020, SMIC had an estimated 5% market share in the semiconductor manufacturing market (TrendForce, 2020) and about 10% market share in older-generation semiconductors (Financial Times, 27 September 2020).

When the US government targeted SMIC, it prohibited US semiconductor firms from trading with SMIC and caused clients of SMIC, including some automakers, to re-evaluate their exposure to SMIC as concerns about its ability to manufacture its semiconductors grew. Following such re-evaluations, several firms diversified their supply chains away from SMIC and into Taiwan Semiconductor Manufacturing Company (TSMC). However, as TSMC already operated at maximum production capacity due to the surge in consumer electronics, it could not meet the extra demand (Reuters, 15 January 2021). The additional pressure towards TSMC's production capabilities, which is estimated to manufacture 54% of the global supply of semiconductors (TrendForce, 2020), further intensified the global semiconductor shortage that was already evident.

A second ripple effect comes from the punitive measures against Huawei. Recalling from Chapter 3.1, when the US Commerce Department added Huawei to the US entity list in May 2019, one of Huawei's responses was to stockpile semiconductors, including from one of Huawei's main suppliers, TSMC. Huawei has not been the only Chinese firm stockpiling; several Chinese tech firms have also been stockpiling semiconductors either due to being designated by a US export restriction or in anticipation of such measure. According to official trade data gathered by Bloomberg (2 February 2021), China's imports of semiconductors reached USD380 billion in 2020 and accounted for 18% of China's total imports that year,

compared to USD300 billion the previous year (Reuters, 26 August 2020). The stockpiling efforts have increased the pressure on the global semiconductor manufacturers, further intensifying the semiconductor shortage.

A third ripple effect also comes from the punitive measures against Huawei but from another perspective. Recalling from Chapter 2.2, when Huawei was no longer able to access its key suppliers, it severely reduced its ability to produce its consumer electronics and reduced the consumer demand for especially its series of smartphones (following the loss of the Android operating system). Following the punitive measures against Huawei, many of Huawei's competitors sought to capture parts of the global market share that Huawei was expected to lose. Therefore, several smartphone makers increased their production capabilities, which also meant increasing their purchase of semiconductors. One of them was the Chinese smartphone maker Xiaomi, which increased its spending on semiconductors by 26% compared to the previous year (Gartner, 2021), which again added pressure on semiconductor manufacturers and further tightened the global semiconductor shortage.

The COVID-19 pandemic was the main immediate cause of the global shortage of semiconductors; however, the ripple effects of the US punitive measures against firms like Huawei and SMIC further exacerbated the pressure on the global semiconductor supply. This highlights how punitive measures do not unfold themselves in a vacuum between the designating government and the targeted firm, as participants in the global value chains reassess their positions while facing an unpredictable business environment.

4.2 Design-out of U.S. technology

The U.S. government has continuously argued that its punitive measures against Huawei have been necessary to protect its national security. Critics argue that these unilateral measures have weakened the U.S. credibility as a reliable trading partner. Consequently, foreign firms might perceive a heightened risk of relying on U.S. technology, especially those that involve advanced technology such as semiconductors. That has been the concern of the U.S.'s Semiconductor Manufacturing Industry Association (SEMI), who represents more than 2,400 member companies. In a statement, SEMI expressed that the "restriction [would] fuel a

perception that the supply of U.S. technology is unreliable and would lead non-U.S. customers to call for the design-out of U.S. technology" (SEMI, 2020).

The design-out of U.S. technology, which can be understood as the process of phasing out U.S. technology from one's supply chain, might indeed be an implication of the punitive measures against Huawei. Not only for Huawei, whose supply was forcibly cut off, and has already developed its own operating system and plans to build its own semiconductor plant, but other Chinese firms are likely to be deterred from relying on U.S. technology and thus might start phasing out U.S. technology and components from their supply chains.

Additionally, other foreign firms, such as European ones, which are not likely targets of U.S. punitive measures, might want to replace U.S. technology and components with non-U.S. alternatives to avoid being forced to stop supplying to Chinese firms. According to one report (Financial Times, 23 December 2020), European technology executives and diplomats have grown increasingly frustrated over U.S.'s unilateral measures against certain Chinese firms, such as Huawei, because it unwillingly could no longer supply to those firms. According to one source, this has accelerated European efforts to be less dependent on U.S. technology and might be one of the motivations for the European Commission's December 2020 announcement of a "European initiative on processors and semiconductor technology", with plans on using EUR 145 billion on digital transition projects, including semiconductor research.

The U.S.'s tight export controls on semiconductors have led RISC-V, a non-profit organisation that promotes open and free semiconductor chip instruction sets to relocate its headquarters and intellectual properties from the U.S. to Switzerland. The organisation, which is composed of more than 325 firms and entities, including U.S., European and Chinese chip suppliers and universities, made the decision after growing concerns among its non-U.S. members over possible geopolitical disruption, a reference to the U.S.'s export controls (Reuters, 25 November 2019).

4.3 Strive for self-reliance

From a short-run perspective, the U.S.' efforts towards restricting Chinese firms from accessing advanced semiconductor technology have been partially successful in its objective. Huawei has been struggling to source advanced semiconductors needed in its production, which has damaged its position as a leading telecommunication equipment provider. However, as Huawei has attempted to resolve some of the challenges through investing heavily in its R&D and trying to develop its own advanced semiconductors, other Chinese technology firms who have been affected by similar punitive measures have also shifted their expenditure to heavily focus on R&D towards the development of advanced semiconductors and other high-tech components. It has also accelerated China's national effort towards becoming more self-reliant in critical technologies, with a particular focus on boosting the nation's semiconductor abilities (The New York Times, 24 December 2020).

The implication of severely restricting Chinese firms access to advanced semiconductor technology has therefore pushed China and other countries' drive for greater technological self-reliance. This may eventually hurt U.S. long-term national security interests, as it increases the risk of U.S. semiconductor capabilities being surpassed by other countries and risk losing control and lead of this strategically important technology.

To illustrate the possible implications of restricting one country's access to a strategically important technology, one can look at the case of the cooperative project between EU and China on satellite technology. In September 2003, the EU invited China to jointly fund and develop a common satellite system, called the Galileo Global Navigation Satellite System (European Commission, 2003). China invested EUR 200 million in the joint initiative, which was set out to reduce both region's reliance on the widely used U.S. government-owned satellite system, the Global Positioning System (GPS). From the Chinese side, the motivation to join this collaboration was further motivated by the U.S. blocking of China's access to its satellite technology. As with semiconductor technology, satellite technology would also have civilian and military applications, which made the technology strategically even more important for both the EU and China.

The EU-China collaboration on the satellite system broke down in 2007. According to released U.S. diplomatic cables[6], U.S. diplomats and officials had been urging European governments and aerospace firms to withhold sensitive technology from China due to security concerns (Reuters, 22 December 2013). There was also disagreement on the initial funding plan between China and the EU, and internally between different EU member states.

Undeterred by the setback, China made it a strategic priority to continue to develop its own satellite system, which was named Beidou Global Navigation Satellite System, and invested heavily into the project. While the European satellite system's funding and progress faltered, the Chinese counterpart managed to develop its own satellite components and completed the system in three phases: an experimental phase in 2000-2003, a national and regional coverage phase in 2012, and finally, a global coverage phase in 2020.

The Beidou satellite system enjoyed first-mover advantages as it was able to secure more favourable signal frequencies at the Galileo system's expense. As of 2020, the Beidou system has an estimated accuracy of 1 meter for public use, while the older GPS system has an estimated 4.9-meter accuracy (Peng, 2020).

The example of China's development of the Beidou Satellite System, though not as wide-ranging as the current semiconductor conflict, demonstrates that short-term coercive measures may lead to technological independence for the receiver of punitive measure. It might end up losing more control of the technology than before the restrictions and increase the risk of eventually being technologically surpassed by other countries, which would not serve the U.S.'s long-term national security and economic interests. Therefore, the U.S. government's punitive measures against Chinese firms may therefore yield tactical success in the short-run but end up as strategic setback in the long-run.

[6] These diplomatic cables, of highly confidential nature, were released by Wikileaks, an international non-profit organisation publishing classified information, news leaks and classified media provided by anonymous sources.

5. Common U.S. punitive measures

In the previous chapters, the focus has been on the implications of the U.S. punitive measures specifically targeting Huawei. In this chapter, the scope broadens beyond Huawei, and seeks to identify and understand on a more general basis, the U.S. government's arsenal of punitive measures against foreign firms.

5.1 CFIUS Reviews

The Committee on Foreign Investment in the United States (CFIUS) is an interagency committee composed of nine powerful agencies of the U.S. government. Headed by the U.S. Secretary of the Treasury, its members also include representative from the Departments of State, Defence, Homeland Security, and Energy, the Attorney General, the U.S. Trade Representative, and the Director of the Office of Science and Technology Policy (U.S. Department of the Treasury, n.d.) Its purpose is to serve the U.S. president in "overseeing the national security implications of foreign investment in the economy" (Jackson, 2020, p. 1)

CFIUS was originally established in 1975 as a reporting and monitoring committee by President Gerald Ford as a response to growing concerns over increasing OPEC investments. Members of the U.S. congress feared that foreign firms that were controlled or influenced by the Organization for Petroleum Exporting Countries (OPEC) could gain leverage over U.S. oil supplies through their investments in the United States.

Initially, both its jurisdiction and activity were limited, but it has since developed into a "formidable force with the power to review and investigate foreign investments" (Westbrook, 2019, p. 634). Now, with the president's authority, the committee can "block or suspend proposed or pending foreign mergers, acquisitions, or takeovers of U.S. entities, including through joint ventures, that threaten to impair the national security [of the United States]" (Congressional Research Service, 2020, p. 1). The committee has also retroactively prohibited already completed acquisition and forced foreign firms to divest its U.S. assets.

On 13 August 2018, President Trump signed into law the Foreign Investment Risk Review Modernization Act (FIRRMA) of 2018 (Caine, Franceski, & Rosenberg, 2018). The law came as a response to concerns that the existing U.S. technological leadership's ability to support

U.S.' "national defence and economic security" was at risk due to increasing foreign direct investments, particularly by Chinese firms, into U.S. high tech firms.

The new law has updated CFIUS procedures to formally and specifically also include reviews on any "non-controlling investment in certain U.S. business involved in critical technology, infrastructure, or personal data" (Congressional Research Service, 2020, p. 1).

FIRRMA also allows for CFIUS to "potentially discriminate among foreign investors by country of origin and transactions tied to certain countries in reviewing certain investment transactions" (Congressional Research Service, 2020, p. 1). Although it does not disclose which specific countries that face discriminatory reviews, it is reasonable to assume that close allies of the United States are not included. At the same time, geopolitical rivals such as China and Russia are likely to be prone to such reviews.

Some legal professionals and scholars have criticised CFIUS for the committee's secretive nature and its lack of transparency regarding how it operates and how it justifies its decisions (Broadman, 2019). There are minimal ways to challenge a CFIUS decision – once CFIUS decides to block a transaction, "[it] has so far proven impossible to overcome" (Westbrook, 2019, p. 649).

How exactly can a CFIUS review be used to target a foreign firm? A recent high-profile case involving one of the world's most popular social apps, TikTok, can serve to illustrate. On 14 August 2020, President Trump issued an executive order for ByteDance Ltd., a Chinese multinational tech firm headquartered in Beijing and developer of the video-sharing service TikTok, to divest its U.S. assets and property (The White House, 2020). ByteDance Ltd. had in 2017 acquired another Chinese-based firm, Musical.ly, which had a well-established footing in the U.S. market, and rebranded it into TikTok. Failure to comply with the order would lead to a ban of the app, prohibiting any U.S. transactions and removing the app from the U.S. market.

Divestiture orders are traditionally mostly used in antitrust cases to deter a dominant firm from exploiting its position for market competition purposes. However, in CFIUS reviews, national security concerns is used to serve as a basis for divestiture orders. The app had about 100 million monthly active U.S. users in August 2020 (CNBC, 24 August 2020), and according to

the Executive Order, the user data on those American users posed a national security threat to the United States because it could end up at the Chinese government's. The tech firm rebutted that the allegations that the user data poses a national security threat, arguing that its servers and data maintained in the United States.

In September 2020, following President Trump's divestiture order, ByteDance had reached an agreement with the American technology firm Oracle Corporation and American retail corporation, Walmart for a significant stake in its U.S. operations (The Wall Street Journal, 19 September 2020). As of February 2021, the agreement had not yet formally been approved by the White House.

The TikTok case is noteworthy because it illustrates how foreign firms that operate in the U.S. and collect data on its users can be deemed a national security threat, and subsequently targeted of punitive measures by the U.S. government. Huang and Madnick (2020) point out that the data that TikTok collects is significantly less than what most U.S. tech firms, banks, credit agencies, and hotels collect. Therefore, it is not only tech firms such as Huawei and TikTok, that are susceptible to be targeted by this kind of measure. Seemingly, any firm that possesses any kind of user data may be subject to this punitive measure.

As Huang and Madnick (2020) has found in their research, restrictions have been imposed on "medical devices, videoconference services, software products, security software, social media, security cameras, banking I.T. systems, drones, smartphones, smart toys, online content services, satellite communications, A.I. software, and financial services (…)". With the growing usage of Big Data and the Internet of Things, an increasing number of firms in a wide variety of industries are likely to collect user data that could eventually deem them a national security threat. Thus, also increasing the risk of being susceptible to this punitive measure.

5.2 U.S. Sanctions enforcement actions

The United States is renowned for its extensive use of sanctions and imposes sanctions more than any other country (Masters, 2019). As of August 2020, it has over 8,000 sanctions in place (Zakaria, 2020) through over 30 active sanctions programmes (U.S. Department of the

Treasury, u.d.). Examples of active sanction programmes are ‘Cuba Sanctions’, ‘Foreign Interference in a United States Election Sanctions’, ‘Hong Kong-Related Sanctions’, ‘Global Magnitsky Sanctions’, ‘Iran Sanctions’ and ‘North Korea Sanctions’.

U.S. sanctions generally apply to U.S. parties, but the U.S. government has in recent years practised aggressive extraterritorial enforcement of their sanctions (Townsend, 2020). Therefore, the U.S. sanctions also pose a significant risk to foreign firms without US-presence who otherwise operates internationally.

U.S. sanctions are administered by the Office of Foreign Assets Control (“OFAC”) within the U.S. Department of the Treasury and in conjunction with U.S. State Department and other relevant agencies (McVey, 2019). U.S. sanctions are regulated through an increasingly complex and changing legal landscape. The main statutory authority for U.S. sanctions includes the International Emergency Economic Powers Act and the National Emergencies Act and are typically imposed through the issue of an Executive Order by the U.S. President.

Primary sanctions

U.S. sanctions are either primary or secondary sanctions. Primary sanctions generally apply to (1) all entities organised in the U.S.; (2) U.S. citizens and permanent residents; and (3) all persons physically located in the U.S., regardless of nationality (collectively called ‘U.S. persons’). Legal professionals often refer to this as having a U.S. nexus, and any firm having a U.S. nexus can be held liable if they violate U.S. sanctions laws, e.g., most dealings involving sanctioned countries such as Iran, Cuba, Syria, North Korea, and sanctioned persons, i.e., organisations or individuals on the Specially Designated Nationals and Blocked Persons List (SDN List), or sanctioned activities, e.g., activities involving certain parts of Russia’s energy sector.

Primary sanctions are meant to directly deter U.S. entities from dealings with countries, persons or activities that are not aligned with U.S. interests. What is notable is that the definition of U.S. entities is relatively broad, and thus can be applied to foreign parties who have a physical presence within the U.S., and foreign firms without a physical presence within the U.S., but who have “board members, directors, or employees who hold U.S. citizenship or U.S. green cards” (Townsend, 2020).

Secondary sanctions

Secondary sanctions are sanctions that do not require a U.S. nexus. Through these sanctions, the OFAC can impose sanctions on foreign persons that do not have a direct connection to the United States but is involved with U.S. sanction targets (Townsend, 2020).

Foreign firms can become subject to U.S. sanction laws if there is "sufficient level of contacts with the United States" (McVey, 2019, p. 4). If a foreign firm engages in transactions involving a U.S. person or a U.S. product, technology, or service, or has a U.S. presence, the firm can be subjected to the U.S. sanctions programme. While this suggests a close link to the U.S., OFAC has opted for a broad interpretation of what this entails.

Through its enforcement, OFAC has established that if a foreign firm engages in business transactions outside U.S. jurisdiction but with the use of U.S. dollars, it is deemed as using the U.S. financial system and therefore is subject to U.S. sanction laws.

It has also established that if a foreign firm has previously filed for bankruptcy in a U.S. bankruptcy court, it is also subject to U.S. sanction laws even though it is not engaged in transactions involving U.S. parties or products.

OFAC has also enforced U.S. sanctions on a foreign firm by alleging that the firm has purchased American components and incorporated into its product, before selling to a country sanctioned by the U.S.

Additionally, OFAC has targeted foreign parties who have no contact or link to the U.S., but whom it finds to engage in activity that is not aligned to U.S. policy goals (McVey, 2019). An example of this was when OFAC on 6 April 2018, added 38 Russian parties on its SDN List under its sanctions on Russia and Crimea (U.S. Department of the Treasury, 2018). Among the 38 parties were business executives, firms that were owned or controlled by those executives, government officials and a bank.

It is also noteworthy that OFAC operates under a so-called "50% rule", whereas if a firm is owned 50% or more by an entity on the SDN List, they are also considered to be on the list. The designation of parties on the SDN List is a non-public process and is not required to follow any criminal or civil legal procedure. Severe restrictions were imposed on the parties on the

list, including assets freeze and travel bans. Severe restrictions were imposed on the parties on the list, including assets freeze and travel bans.

While the SDN List is a relatively extreme measure, foreign firms who are not on the SDN List, but conducts business with an SDN List party, would also become at risk of being targeted by OFAC for violating U.S. sanctions. OFAC has established that providing "material assistance" to others in violating its sanctions laws makes the assisting party also subject to its sanctions. It has also perhaps deliberately not clarified on what "material assistance" entails, thus giving OFAC wide access to decide whether another party is violating its jurisdiction.

5.3 FCPA enforcement actions

The Foreign Corrupt Practices Act ("FCPA") is a U.S. statue that criminalises the bribery of foreign officials anywhere in the world by firms subject to its provisions. FCPA was signed into law by President Jimmy Carter in 1977 and was initially intended to target U.S. firms operating abroad, following numerous reports finding U.S. firms to "[making] millions of dollars of questionable payments to foreign government officials to secure business […]" (Diamant, Sullivan, & Smith, 2019, p. 356). Although FCPA enforcement levels were low the first decades after it was introduced, U.S. firms heavily criticised the statue for putting U.S. firms at a competitive disadvantage, arguing that U.S. firms effectively had to comply with higher anti-corruption standards than many of their foreign competitors, who did not face similar provisions or enforcement regimes in their home countries

In 1998, the FCPA was amended to address the concerns that U.S. firms had raised regarding the competitive disparity to foreign competitors, and FCPA's jurisdictional reach thus was extended to include foreign firms and persons acting within U.S. territory (Brown, 2001). FCPA provisions are enforced by the U.S. Department of Justice ("DOJ") and the Securities and Exchange Commission ("SEC"). Like OFAC, the DOJ and SEC have opted for a wide interpretation of its provisions to give them an extraterritorial reach.

For example, in 2006 and 2008 respectively, German conglomerate Siemens AG and the Norwegian state-owned petroleum giant Statoil ASA[7] were found to be held under FCPA jurisdiction because both firms were listed on the NYSE through American Depositary Receipt (ADR). Both firms were charged under FCPA provisions for paying bribes in other countries, though it was not directly an American branch or subsidiary of the firms involved (U.S. Securities and Exchange Commission, 2008; Department of Justice, 2009).

FCPA provisions also have jurisdiction when foreign firms use U.S. banks or the U.S. banking system. In one case, a Japanese firm was found to violate FCPA provisions when it bribed a Nigerian government official by wiring from a Dutch bank account to a Swiss bank account through a New York correspondent account (Diamant et al., 2019). Therefore, although transactions were made through two non-U.S. banks, because there was a U.S. element through the U.S. correspondent bank, the U.S. authorities found it could enforce FCPA provisions.

The DOJ has also established that a foreign firm can be held liable to FCPA provisions if an email used to conspire to foreign corruption passes through U.S. email servers. This was the case when a Hungarian telecommunications firm had sent an email to a foreign official, allegedly as part of the bribery scheme, and the email had passed through U.S. email servers (Mirenda & Smith, 2013). In another case, the DOJ held a Chinese firm liable to FCPA provisions because the Chinese firm had approved a budget with improper payment amounts via emails sent to an employee working in the U.S.

While the FCPA Act was originally intended to deter U.S. firms from paying bribes to foreign officials, in recent years, it has aggressively been used on foreign firms. Diamant et al. (2019) find that foreign firms fare far worse under FCPA provisions than U.S. firms. While the DOJ and the SEC in absolute terms have brought more enforcement actions against U.S.-firms, when looking at average costs to resolve FCPA enforcement actions, foreign firms had four times higher average costs than U.S. firms. In 2017, foreign firms paid on average USD 150 million in settlements, while US-firms on average was significantly less, at USD 16.1 million.

[7] In 2018, Statoil ASA changed its name and now goes under the name Equinor ASA.

This suggests that the U.S. government imposes discriminatory enforcement of FCPA violations to foreign firms' disadvantage.

5.4 Trade blacklisting: the U.S. entity list

The U.S. Entity List, which was briefly mentioned in the introduction, is a supplement to the U.S.' Export Administration Regulations (EAR). EAR governs the export, re-export and transfer of items from the U.S. to a foreign country, and such items include both tangible and intangible items, such as technology and software. When first published in February 1997, the list was created to inform the public of entities that the U.S. government red-flagged for engaging in activities that "could result in an increased risk of the diversion of exported, re-exported and transferred (in-country) items to weapons of mass destruction (WMD) program[mes]." (U.S. Department of Commerce, u.d.).

Today, the U.S. Entity List has expanded significantly, to include any activity that is deemed a threat to U.S. national security or foreign policy interests by the U.S. government. The list is published by the U.S. Department of Commerce's Bureau of Industry and Security. It can target "businesses, research institutions, governments and individuals" deemed a national threat to the United States (U.S. Department of Commerce, 2020).

Firms on the list are severely restricted from accessing U.S. supply chains and must apply for an export license to the Bureau of Industry and Security ("BIS") to be exempted from the ban to export to entities on the list; however, the BIS will often have a license review policy of "presumption of denial", meaning that they are unlikely to grant such license.

5.5 Investment bans and delisting from U.S. stock exchanges

On 12 November 2020, President Trump issued the *Executive Order on Addressing the Threat from Securities Investments that Finance Communist Chinese Military Companies* (The White House, 2020). The order's main statutory authority is derived from the International Emergency Economic Powers Act, the National Emergencies Act, and section 301 of title 3, United States code.

This punitive measure banned U.S, investment in firms that the U.S. Department of Defense claim to be linked with the Chinese military. The above provisions were used to force the delisting of several of China's largest public firms from the New York Stock Exchange (NYSE) and removed them from several global benchmark indices (Reuters, 1 January 2021). The measure also prohibited US investors, both retail and institutional, from engaging in securities transactions with more than 40 Chinese firms that are mainly large, well-established leaders in their industries and forcing US investors with existing ownership in these firms to completely divest themselves by November 2021 (Reuters, 14 January 2021) .

5.6 Travel bans on employees

The United States has also imposed punitive measures against a foreign firm by restricting its employees from obtaining visas to enter the United States. The statutory authority to impose such visa restrictions comes from the Immigration and Nationality Act. It allows for U.S. officials to deem aliens inadmissible to the United States on several grounds, e.g., public health-, crime- and security-related reasons.

On 16 July 2020, the Trump Administration announced that it would impose visa restrictions on unnamed Huawei Technologies employees, effectively banning them from entering the U.S. Secretary of State Mike Pompeo used the Section 212(a)(3)(C) of the Immigration and Nationality Act, which allows him to deem aliens inadmissible if he has reason to believe that admitting the unnamed employees to the United States "would have serious adverse foreign policy consequences for the United States" (U.S. Department of State, 2020).

While this form of punitive measure is rarely used on specific foreign firms, it illustrates the U.S. government's willingness to use national security reasons to impose punitive measures to target a foreign firm they deem a threat to U.S. interests.

6. Punitive measures under the global trade regime

For decades, global trade rules have been developed to provide predictable and stable trading terms that facilitate more trade between countries. Under the World Trade Organization (WTO) system, which is responsible for operating a global system of trade rules and settle trade disputes between its 164 member states (as of February 2021), there are provisions and dispute settlement mechanisms in place to address disputes over any trade restricting measures, including several of the punitive measures discussed in previous chapters. This section will address the punitive measures in the context of the rules set by the WTO system.

The WTO works towards ensuring that trade flows as smoothly, predictably, and as freely as possible through its guiding principles (World Trade Organization, u.d.) of:

1. Trade without discrimination;
2. Freer trade with less barriers to trade;
3. Predictability through commitment and transparency;
4. Promotion of fair competition; and
5. Encouraging development and economic reform.

These principles are reflected in all WTO agreements, and therefore, given the trade-disrupting nature of many of the U.S. punitive measures against Huawei, an important question is how the WTO system addresses these types of punitive measures, which represents deviations from WTO's goal and guiding principles.

6.1 Non-compliance with WTO rules

In general, following the most-favoured-nation (MFN) principle of GATT Article I, a WTO member cannot discriminate between trading partners. Legal scholar Peng (2015) argues that the U.S.'s punitive measure that bans Huawei's access to the U.S. market would be non-compliant with WTO agreements, as it would give Huawei's foreign (i.e., non-Chinese) competitors, such as Sweden's Ericsson, Finland's Nokia, and South Korea's Samsung favourable trade access to the U.S. market.

Similarly, this would be applicable to any member state that has imposed a ban on Huawei to their markets, such as the UK, Australia, France, and Sweden. By excluding Huawei from participating in its 5G networks, they are effectively favouring Huawei's foreign competitors, and thus, violating GATT Article I.

Additionally, this would also apply to the U.S. punitive measures related to restricting Huawei from U.S. and U.S.-originated inputs, as GATT Article I stipulates that:

[…] any advantage, favour, privilege or immunity granted by any contracting party to any product originating in or destined for any other country shall be accorded immediately and unconditionally to the like product originating in or destined for the territories of all other contracting parties.

If other non-Chinese firms can access U.S. and U.S.-originated inputs, while Huawei cannot, this too would be inconsistent with the MFN principle, as it would favour non-Chinese trading partners.

Secondly, under GATT Article III, *National Treatment on Internal Taxation and Regulation*, a member state is prohibited from using "internal tax and regulatory measures" to discriminate foreign producers over domestic producers. Article III's provision is relevant if it gives a domestic producer favourable treatment over a foreign one. Therefore, in the Huawei case, Article III would only be applicable if the member state imposing the trade-restricting measure had a domestic firm producing equivalent or "like products" as Huawei. Peng (2015) argues that U.S.'s telecom equipment provider Cisco and Huawei produce "like products" (routers and network switches), and by excluding Huawei from its market, it is effectively discriminating a Chinese firm over a domestic firm. However, the recent restrictions have focused on Huawei's 5G equipment, and competing firms for these types of products are fewer, but includes Sweden's Ericsson, Finland's Nokia, and South Korea's Samsung. Therefore, in the case of Sweden's ban of Huawei to its 5G networks, Article III would be relevant and applicable.

Thirdly, under GATT Article XI, *General Elimination of Quantitative Restrictions*, a member state is prohibited from imposing or maintaining a quantitative restriction on imports and exports from another member state. The U.S.'s export restriction of U.S.-based inputs to

Huawei would account as a quantitative restriction. Additionally, member states that has imposed bans on Huawei products, such as 5G-related equipment, are effectively imposing a quantitative restriction on telecom equipment imports from China. Therefore, both bans, on export of U.S.-based inputs to Huawei, and imports from Huawei appear inconsistent with Article XI.

Above, it has been established that many of the punitive measures against Huawei seem to be inconsistent with WTO rules. In such case, it begs the questions of why some member states still have chosen to impose these punitive measures, and how the WTO can address any potential violations of WTO rules. To answer these questions, one must refer to GATT's national security exception and the WTO dispute settlement process.

6.2 The national security exception

In the Huawei case, national security has been the primary reason used to justify most of the punitive measures imposed on the firm. This is not a coincidence, as the WTO system have four provisions that allow a government to exempt from the general trade rules on the basis of national security: Article XXI of the GATT, Article XIV of the General Agreement on Trade in Services (GATS), Article 73 of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), and Article XXIII of the Agreement on Government Procurement (GPA).

The Security Exceptions provision of Article XXI of the GATT states that:

Nothing in this Agreement shall be construed

- *(a) to require any contracting party to furnish any information the disclosure of which it considers contrary to its essential security interests; or*
- *(b) to prevent any contracting party from taking any action which it considers necessary for the protection of its essential security interests*
  - *(i) relating to fissionable materials or the materials from which they are derived;*
  - *(ii) relating to the traffic in arms, ammunition and implements of war and to such traffic in other goods and materials as is carried on directly or indirectly for the purpose of supplying a military establishment;*

(iii) taken in time of war or other emergency in international relations;

(c) to prevent any contracting party from taking any action in pursuance of its obligations under the United Nations Charter for the maintenance of international peace and security.

Relating to the imposing of trade restricting punitive measures, the most relevant sections of Article XXI are Section (b) and Section (b)(iii). These sections consist of the key points that address a country's ability to use the national security exception to impose trade restricting measures. The article stipulates that for a WTO member to be able to deviate from its WTO obligations, it can "[take] any action which it considers necessary" to protect its "essential security interests" during an "emergency in international relations".

National security is a dynamic term. Pre-20th century thinking equated national security with military security; however, today, it has also evolved to include political security, economic security, energy and natural resources security, cybersecurity, human security, and environmental security (Holmes, 2015). Because national security has such a vague and broad definition, it not only allows countries to have dissimilar interpretation of what "essential security interests" entails, but it can also give countries the flexibility and credible deniability to determine when the national security exception can be applied, as it fits their policy agenda.

This has caused disagreement among WTO members. Some WTO members argue, based on sovereignty, that only the country itself can truly determine what their "essential security interests" are. On other side, some members believe this should be open to review by a WTO panel (Reinsch, 2019), as the former would allow countries to easily misuse the provision to pursue other policy goals that is not rooted in national security concerns.

The issue of the possibility to misuse the national security exception was already a concern as early as during the preparatory sessions that would lead to the General Agreement on Tariffs and Trade (GATT) of 1947. During those session, the U.S. delegation stated that the security exception provision in the Charter's Article XXI, could not be too broadly interpreted so that "under the guise of security, countries will put on measures which really have a commercial purpose" (World Trade Organization, u.d.)

For decades, GATT/WTO has avoided any ruling on the interpretation of the national security exception, as it could provoke member states to withdraw their obligations to the WTO. However, in a recent dispute settlement case (DS512) filed by Ukraine against Russia, titled "Russia – Traffic in Transit", the WTO Dispute Settlement Body offered for the first time a clarification on how Article XXI's national security exception should be interpreted. Specifically, in this landmark case, the WTO panel established that the invocation of the national security exception is not completely self-judging by the member state, but may be subject to the scrutiny of the WTO Dispute Settlement Body (World Trade Organization, 2019).

Relating back to the Huawei case, a WTO member state could impose punitive measures against Huawei that would be inconsistent with GATT Articles 1, III and XI and argue that the national security exception of Article XXI is applicable. However, after the landmark case "Russia – Traffic in Transit", invoking the national security exception can now be subject to the scrutiny of the WTO Dispute Settlement Body, and could rule that the member state's invocation of the exception is invalid.

6.3 Dispute Settlement Process

It has now been established that the U.S. punitive measures against Huawei can be challenged in the WTO system; however, in practice, how would the WTO's dispute settlement mechanism handle such an issue?

The WTO dispute settlement process is divided into three stages: (1) consultations between disputing parties; (2) adjudication by panels and (if applicable) by the Appellate Body; and (3) the implementation of the ruling. It is important to note that only member states can file a complaint under the WTO Dispute Settlement Mechanism, and not individual firms. Therefore, in the Huawei case, the Chinese government would have to file a dispute on Huawei's behalf.

The WTO estimates that a case normally takes between one year to 15 months to be fully processed (World Trade Organization, u.d.); however, recent development has severely challenged that time frame. Under the current dispute settlement process, during stage (2), a

panel will hear the dispute case and conclude with a report to both parties, as well as to all WTO member states. Both parties can then choose to appeal the report, which would send the case for review by the Appellate Body. The Appellate Body then has the authority to reach a final ruling on the case, which would be legally binding for the member states. But since December 2019, the Appellate Body has not been able to function due to the U.S. government's refusal to appoint new members to the minimum three-person panel. Without a functioning Appellate Body, any appealed case cannot continue to the last stage of the dispute settlement process, effectively paralysing the entire WTO dispute settlement mechanism. Thus, until[8] the Appellate Body are appointed new members, the WTO dispute settlement mechanism is unable to decide on any cases.

6.4 National security: a pretext for economic protectionism?

In the Huawei case, national security has been the primary reason used to justify most of the punitive measures imposed on the firm. Huawei has continually denied wrongdoing and rebutted the allegations the U.S. government's claims against the firm. The U.S. has generally not provided evidence to support the accusations it has made against the firm and repeatedly argues that it does not need to provide this evidence. It believes that Huawei's close ties to the Chinese government and its role as a leading telecommunications supplier constitutes a security threat in itself.

Given the nature of the telecommunications industry, Huawei's main business area, it is understandable that a government would seek to ensure that its commercial actors operate legitimately. Telecommunications is deeply penetrated in today's economy and society, as the technology facilitates countless daily activities of individuals, businesses, and governments. Not only is it a critical infrastructure, but it also supports the "foundation upon which all other critical infrastructure operates" (Lobel, 2014, p. 1).

[8] As of May 2021, U.S. President Joe Biden has continued his predecessor's refusal to appoint new members to the Appellate Body.

In some sense, even if the United States were to categorically use national security solely as a pretext for economic protectionism, it is conceptually easy to understand the concern for

national security given the nature of telecommunications technology, and the critical role it has for a country's infrastructure. On the opposite side, it would, for example, be more difficult for a government to justify introducing trade-restrictive measures on products that conceptually had little relevance to a country's national security[9]. Therefore, the level of importance an industry has to national security issues is likely, to some extent, to determine how easily these trade-restrictive measures can be justified using national security provisions.

When President Trump imposed tariffs on steel and aluminium imports, it followed a U.S. Department of Commerce's report on aluminium that found that these imports threatened to impair U.S. national security. One of the arguments it presented was that aluminium was needed to upgrade its military aircraft (Chinn, 2018). However, in a memo in response to this report, the U.S. Secretary of Defence noted that "U.S. military requirements for steel and aluminium each only represent about three [per cent] of U.S. production" (Secretary of Defense, n.d.). Thus, he concluded that the military requirement for both steel and aluminium supply was not at risk.

When the United States invoked Article XXI of the GATT to justify these tariffs, Canada, Mexico, the E.U., Switzerland, Norway, Russia, Turkey, China and India filed complaints to the WTO, arguing that there was "no legitimate or plausible national security rationale for the tariffs" (Reinsch, 2019). Some critics of the tariffs note that the U.S.'s supply of steel stem primarily from Canada and the E.U., close military allies of the U.S. (BBC, 31 May 2018).

Similarly, critics did not find President Trump's declaration that some imported automobiles and auto parts impaired U.S. national security credible, suggesting that the threat of imposing tariffs on these imports were mainly for the purpose of economic protectionism and as leverage in his trade negotiations with the E.U. and Japan.

[9] This was the case in 1975, when the Swedish government notified the GATT Secretariat its intentions to introduce import restricting measures on leather shoes, plastic shoes and rubber boots. (legg til WTO-kilde, 1975) After other GATT signatories expressed doubts over the justification, the import restrictions were later discarded (legg til WTO-kilde, 1977).

The examples of steel, aluminium and automobiles are notable because all three lacked a substantial degree of credibility within the international community that national security was the real motivation behind the trade-restrictive measures. This has reinforced the notion that the United States would use national security concerns as a pretext to economic protectionism, and would further undermine U.S. credibility, even in more security-relevant cases such as the Huawei case. It could also encourage other countries to misuse the national security exception in pursue of economic goals.

7. Punitive measures: key factors to increased risk

Previous chapters have described how Huawei has been aggressively targeted by a wide range of U.S. punitive measures. While the Huawei case is unique, this part will draw upon the findings from the case to generalise how certain key factors in a firm may lead to increased risk of being targeted by punitive measures from a foreign government. This part will present four key factors that are considered important in determining whether a firm is at a heightened risk of being the target of punitive measures. These factors are: (1) Firms originating from a rival country to the issuer of the punitive measure; (2) Firms that have access to private data; (3) Firms engaged in trade of potential dual use items; and (4) Firms operating in an industry of strategic or technological important industry.

The list is not an exhaustive list of risk factors but attempts to draw upon the most relevant risk factors concerning punitive measure. The factors must also be understood as interrelated to one another, in the sense that one factor may affect the risk assessment of other factors. This is especially the case of the first factor, in such that if the firm originates from a rival country, the associated risk will trickle down onto the other factors. E.g., a firm that has access to private data (factor 2), will by itself have an increased risk of being the target of punitive measures, but combined with of originating from a rival country to the issuer of the punitive measure (factor 1), the risk is significantly heightened.

If all factors are applicable to a firm, the associated risk will be at the highest level. Such seems to be evident in the Huawei case, which could help explain why it has been so aggressively targeted by U.S. punitive measures.

7.1 Firms originating from a rival country to the issuer of the punitive measure

The first factor looks at whether the firm is originating from a country that is a rival country to the sender of the punitive measure. The assumption is that the greater the rivalry between two countries, both economic and militarily, the lower the threshold is for a country to impose punitive measures on a rival country's firm. On the other hand, if two countries are close allies,

it is assumed that the barriers for one country's government to impose punitive measures against a firm originating from the other country are higher.

As seen repeatedly, many of the punitive measures are justified through national security concerns, and whether legitimate or pretextual, it is easier for a government to justify punitive measures to a firm that do not originate from a country that is considered a close security allied. For example, Chinese and Russian firms are more likely to be the target of U.S. punitive measures than firms originating from Canada or United Kingdom. It was therefore a more predicted outcome that the U.S. government declared the Chinese telecom firms Huawei and ZTE as threats to its national security, while their main competitors, Sweden's Ericsson and Finland's Nokia have not received similar punitive measures.

When assessing the rivalry between two countries, one can do so by identifying whether the two countries have aligned economic and security interest. Thus, for especially the latter part, whether the two countries are engaged in security alliances such as NATO, may provide strong indication of whether this element creates increased risk or not.

7.2 Firms that have access to private data

The second factor is whether the firm collects, processes, analyses or in any way has access to private data. In this paper, private data is defined broadly as any data that should not be publicly available. It may include sensitive data containing classified information and/or personal data that may be used to identify individuals and that is susceptible to being exploited in some capacity.

In recent years, firms have increasingly perceived data as an important asset in creating value. Emerging technologies, such as artificial intelligence and predictive analysis has also increased firm's ability to leverage on data it can gather from its customers. As the world has moved towards greater connectivity, there has also been a growing concern towards the vast amount of data is being handled in terms of privacy issues, and the possibility for the data to be used for malicious purposes. This has for example led the European Union to strengthen the protection of its member states' citizens data, through the General Data Protection

Regulation (GDPR). Other governments are also addressing the perceived threats to its citizens privacy, but also from a greater national security perspective.

The risk associated with this factor is mostly focused on the firm's output side. In the Huawei case, concerns over the existence of a "backdoor" in Huawei's telecommunications equipment was used to justify the punitive measures against Huawei. If that were to be the case, proponents of the punitive measures argued, not only could it be used to access personal data from private citizens, but also sensitive communication of governmental and military nature.

In today's digital age, data is ubiquitous, and most firms have access to user data in some capacity. Access to user data itself is not necessarily a factor to increased risk of being targeted by punitive measures; however, because of the possibility that data can be maliciously exploited, it is easier for governments to rationalise punitive measure against a firm who in some capacity has access to private data. The more sensitive the data is, the more reason does a government have for imposing punitive measures against the firm, either for legitimate concerns for its citizens privacy or national security, but also using those concerns as a pretext in pursuit of other policy goals.

On this basis, firms that in some capacity has access to private data are at increased risk of being the target of punitive measures by a government, and the more sensitive the nature of the data, the higher the risk becomes. Additionally, when considering the continuous technological developments and digitalisation efforts, as more firms are delivering products and services that are connected to the internet and can collect large quantities of private data, from automobiles, smart home systems, watches, TVs etc., the more relevant this factor has become in recent years and will continue to be.

7.3 Firms engaged in trade of potential dual use items

The third factor is whether the firm is engaged in trade of potential dual-use items. Dual-use items refer to goods, software and technology that can be used for both civilian and military applications (European Commission, 2018). Due to national and international security considerations, foreign trade of dual-use items is normally highly regulated and subject to

strict export controls by most major economies, through national regulations and multilateral export control regimes such as the Wassenaar Arrangement[10].

By using the Wassenaar Arrangement list as a guide, one can identify ten different categories of dual-use goods and technologies: 1. special materials and related equipment, 2. materials processing, 3. electronics, 4. computers, 5. telecommunications, 6. information security, 7. sensors and lasers, 8. navigation and avionics, 9. marine, 10. aerospace and propulsion (Wassebaar Arragement Secretariat, 2020).

Navigation systems such as the U.S. Global Positioning System (GPS) is a classic example of a dual-use item, a technology that has a widespread commercial-use (e.g., automotive navigation system, ship tracking, cartography, and clock synchronisation) and military-use (e.g., missile and projectile guidance, reconnaissance and target tracking). However, there are also many items that are not obvious dual-use items, and which under normal circumstances are not considered as such, either by the producer, consumer, or both. For example, in 2000, Sony's highly popular game console, the PlayStation 2, was imposed export controls because its memory card could process high quality images, which could potentially also be used in missile guidance systems (BBC, 17 April 2000). Therefore, dual-use items need not have an actual, existing military application, the theoretical potential itself is enough to define it as a dual-use item.

In the Huawei case, the U.S. government has repeatedly alleged a close link between the telecommunications firm with the Chinese military and has even designated Huawei as "owned or controlled by the Chinese military" (Reuters, 24 June 2020), suggesting that Huawei's products and services can be used for military applications.

Consequently, firms which are producing goods and services for commercial use only, but has a potential military application, has an increased risk of being targeted by punitive measures, and the closer the link exists for a potential military application-usage, the higher the risk becomes.

[10] Short for *The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, an intergovernmental forum which facilitates information sharing and standard settings for export controls of conventional arms and dual-use goods and technologies. As of 2021, it has 42 participating states, including the United States, most EU member states, Australia, Argentina, India, and Japan* (Wassenaaar, 2020).

7.4 Firms operating in an industry of strategic or technological importance

The fourth factor relates to whether the firm is operating in an industry that is of strategic or technological importance. Firms who are involved in such industries may be considered more critical for the society's security and welfare, and governments might impose punitive measures against foreign firms to limit its reliance on such firms. It may also be a pretext for purely economic protectionism or as part of greater geopolitical considerations.

The ICT industry is often considered a sensitive industry due to the amount of and quality of data transmitted. Natural examples would be Huawei and ZTE as already mentioned in this paper. The energy sector could be considered critical, particularly if the supplier is a foreign player who is domiciled in a country that has no security cooperation with the country. High-end equipment industry, particularly those, but not limited to, equipment that may be used for military application, e.g., aircraft, ship, satellite components, are also at increased risk of being targeted.

Not all countries are in the position to impose punitive measures on a given firm in a given industry. Smaller countries with less developed industries may not develop its own capacity due to lack of capital, skilled labour, or market. As certain industries require enormous capital expenditures, not all countries have the necessary large market to enjoy the economies of scale. These countries would embrace foreign companies in order to develop its own economies, especially if the country is neutral or friendly towards the country of origin of the foreign firm. For smaller countries that have a security cooperation with other countries, they may not be allowed to cooperate with a given foreign country.

8. Factors determining a firm's ability to respond effectively to punitive measures

Punitive measures can affect the target firms in many ways, but primarily either from an input side or output side, i.e., the firm's ability to produce its goods and/or services through access to technology, commodities, components etc., or the firm's ability to sell its goods and services through access to different markets. In the Huawei case, the wide range of punitive measures has affected both input side and output side of the firm, through a ban on U.S.-based inputs on the firm and a ban on Huawei's participation in roll-out of 5G networks in certain geographical markets. This part will present factors that are important in determining a firm's capability to respond effectively to punitive measures.

A firm's capability to respond effectively is determined by the alternatives a firm has to the restriction or barrier that a punitive measure represent. This part will divide factors into two perspectives: market-level conditions, and firm-level conditions. The former conditions relate to how important or impactful the punitive measures are for the firm, while the latter conditions relate to the firm's ability to adapt to the measures.

8.1 Market-level perspective

Firms that rely heavily on the issuer of punitive measures' market are assumed to be less likely to produce any meaningful countermeasure to the punitive measures imposed on the firm. If a firm is reliant on the issuer's market, can be determined by several factors.

Share of total sales revenue

The first factor is whether the firm derives a significant share of its total sales revenue from said market. If the firm depends on selling to said market, and is suddenly restricted from accessing the market, it will severely impact the firm's ability to generate revenue, and therefore also reduce the firm's ability to produce any meaningful countermeasures to the punitive measures.

In Huawei's case, the majority of its total sales revenue is derived from the Chinese market. Thus, the restriction from several Western market has not been affected its main source of revenue, which is likely to have allowed Huawei to produce meaningful countermeasures.

Reliance on inputs

The second factor is whether the firm relies heavily on sourcing inputs from said markets, this will also negatively affect the firm's ability to respond to punitive measures. The more technologically sophisticated inputs a firm needs from said market to produce its goods or services, the more difficult it is assumed for the firm to be able to find alternatives. An example of this is found in the Huawei case: when the U.S. government first tightened the export restriction to prohibit U.S. firms from supplying Huawei, Huawei was able to respond effectively by sourcing from other markets such as South Korea and Taiwan. However, when the U.S. government further tightened the export restrictions to include non-U.S. semiconductors firms, Huawei struggled to produce its latest smartphone series because they required highly advanced semiconductors. Since there were only two manufacturers, TSMC and Samsung (both affected by the U.S. rule), able to produce the highly sophisticated semiconductors needed, Huawei had no alternative supplier to procure from. If Huawei only needed less-sophisticated input, it would have been far more likely to be able to find alternative suppliers from other markets.

Firm's domestic market

The third factor is whether the firm originates from a country with a large domestic market that it can re-shift its supply to. If the firm can do so, it will positively affect the firm's ability to produce meaningful countermeasure, by giving the firm alternative revenue sources. As seen in the Huawei case, when foreign governments imposed punitive measures that restricted Huawei from their markets, one of Huawei's responses were to shift its supply to the Chinese market, whose sheer size provides an alternative to the restricted markets of many Western countries.

Access to well-functioning financial markets

A fourth factor is whether the firm has access to well-functioning financial markets that can be critical in the firm's ability to raise capital needed to finance countermeasures such as R&D

investment, building in-house production capabilities, diversifying supply chains and investing in strategic partnership.

Access to domestic and foreign talents

A fifth factor is whether the firm is based in a country that has readily access to both domestic and foreign talents, skilled labour and management. A firm that is based in such a country, will be more efficient in attracting qualified personnel in sufficient numbers. In order to attract such a work force, the country should have either relaxed immigration laws overall or have a fast track for talents and desired workers. For example, the U.S. is known for being able to attract talents and skilled engineers from all over the world. China, on the other hand, have access to an enormous domestic labour pool of skilled labours and engineers, but may attract less foreign talents and workers compared to the U.S.

8.2 Firm-level perspective

Strong balance sheets

Firstly, if the firm has strong balance sheets, i.e., solid cash reserves, low levels of debt and adequate credit lines, it is more resilient to shocks (Lund, et al., 2020) and is therefore also better equipped to manoeuvre through the challenges of being targeted by punitive measures. Punitive measures can often represent high financial liabilities for the targeted firms and create high unexpected costs or high negative impact on revenue that can disrupt the firm's ability to resume normal operations. If the firm has weak balance sheets, it may not have the financial capabilities to produce meaningful countermeasure to its received punitive measures, and larger concessions and bankruptcy might be likely outcomes.

Capital expenditure requirements

The second factor is related to the fourth factor in the previous section regarding a firm's access to well-functioning financial markets. Depending on the industry that the firm operates in, the capital expenditures needed to increase capacity may vary greatly. If the industry has relatively low capital expenditures requirements, the firm may choose to insource or to promote alternative suppliers to increase capacity in the near run. Hence, low capital

expenditures requirements will facilitate for stronger countermeasures by the firm, and vice versa.

Organisational culture

The third factor is whether the firm possesses an organisational culture that allows the firm to effectively cope and adapt to new market conditions. Because punitive measures may represent vast changes to a firm's market conditions, such as being restricted from an entire market or losing access to key inputs, in order for the firm to be able to respond effectively with countermeasures, it must possess the characteristics of an agile business. The management should be able to take effective decisions quickly when the punitive measures are imposed. Optimally, they should also already have drawn action plans or contingency plans for various scenarios.

Ownership structure

The fourth factor concerns the firm's ownership structure. As the management often could be beholden to its owners, in many cases it is the owners that may manage changes and crisis better. A privately held firm, like Huawei, for example, could be better positioned in managing changes than compared to a publicly held firm that has various stakeholders to address. On the other hand, state-owned enterprises might also be better positioned to respond effectively to punitive measures, as they might be more inclined to receive financial support from the state during a crisis, giving them more financial capabilities to counter the negative effects of punitive measures.

9. A framework for defining optimal strategy towards punitive measures

This part will present a model for defining an optimal strategy towards punitive measures. Any punitive measure will challenge a firm's status quo and cause some degree of disruption to its business operations, and firms should systematically evaluate its vulnerability against punitive measures. This framework can be used pre-emptively to evaluate a firm's current vulnerability towards punitive measures, or reactively to evaluate what countermeasures the firm should impose to mitigate the negative effects of imposed punitive measures.

This chapter is divided into three sections: firstly, an input side model related to punitive measures that targets the firms' inputs, i.e., access to commodities, components, technology etc.; secondly, an output side, which relates to punitive measures that target the firms access to certain markets; lastly, an application of the framework on the Huawei case.

The purpose of this chapter is to offer a framework for firms to systematically evaluate the impact of punitive measures based on two general dimensions related to 1. *How severely the punitive measures impact the firm* and 2. *The ease for the firm to find alternative (input or output)*. Based on how the firm evaluates its vulnerability towards punitive measures, the framework suggests countermeasures (pre-emptive or reactive) to cope with the punitive measures. However, note that the suggested countermeasures are not dogmatic – the optimal countermeasures may be subject to interpretation of the situation and there could be a gradual transition between each scenario.

The sections regarding the optimal strategy towards punitive measures in terms of input and output level could be regarded as having a somewhat narrow scope. It is on component level or geographic market level. The firm's overall long-term strategy or *grand* strategy should also be considered. Even though many geographic markets may individually be considered small, it could in total account for a significant share of its total sales. Losing one small geographic market or a supplier could lead to a negative spill over effect. Conversely, winning a market may further penetrate the global market and let the firm further entrench its foothold.

A grand strategy could very well be different from the more short-term strategies. For example, to gradually invest more in those seemingly unimportant small markets, or undertake

a strategic retreat in certain markets, either permanently or temporarily – depending on what would be most beneficial for the firm in the long run. Naturally, not all firms have the financial resources to have the freedom of choosing strategies. Some firms may only have the resources to undertake ad hoc strategies. Each firm must weigh its abilities and act accordingly.

9.1 Input side

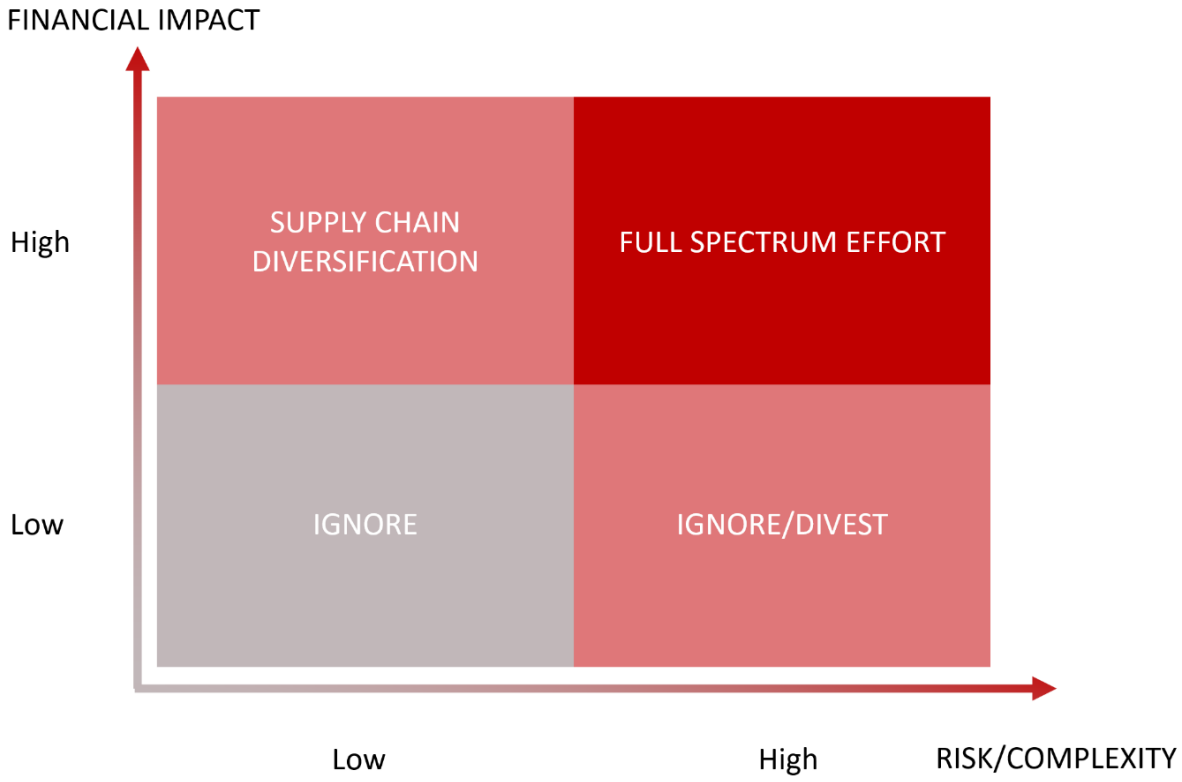
This section introduces a framework for defining the optimal strategy towards punitive measures for a targeted firm on the input side. In this framework, a firm should identify its potential weaknesses in terms of possible or actual punitive measures imposed by a foreign government. After identifying these weaknesses, the next step would be to suggest concrete short-term countermeasures towards the punitive measures and lastly, develop and implement a coherent long-term strategy to manage the potential risk from punitive measures.

The firm should analyse a strategy against punitive measures along two dimensions, namely *financial impact* and *risk/complexity*. In *financial impact*, one shall determine the degree or share of total revenue the punitive measure inflicts upon the firm. A high financial impact would be inflicted upon a firm typically if the punitive measure hits the firm's core activities or subcomponents of the core product. Financial impact may also be measured by proxies such as impact on product performance or growth opportunities.

Risk/complexity dimension is a catchall for the difficulties the firm would face in diversifying its suppliers, finding alternative replacement components/technology, or insourcing a certain component. The dimension is related to risk factors such as market structure (monopoly or free competition), barriers to entry and technological substitution, innovation, and disruptions. To determine whether this dimension is high or low, one may refer to the previous chapter which presents key factors to increased risk.

By evaluating the firm's situation along these two dimensions, it may fully exploit its bargaining power, while reducing its risk to an acceptable level. The firm classifies its products or components into four categories of optimal strategies towards punitive measures. Each of these four categories implies a given, optimal strategy towards the punitive measures imposed on the firm or the product/component. The optimal strategy ranges from simply ignoring the punitive measures, to counter it at all costs, sparing no effort. Note that a product's category may adjust according to changes in supply or demand patterns as well as technological development.

Figure 1: Model on optimal strategy against punitive measures: input side



Source: Author's own creation

Low financial impact, low risk/complexity: IGNORE

In the case of low financial impact and low risk/complexity, the subcomponent or technology the firm is purchasing has a low impact on its sales or profits. In this scenario, the risk associated with finding an alternative supplier is low or the firm can with ease insource the said component. The kind of products or raw materials could be goods that are traded freely

in the market with many suppliers. The nature of this good is typically low tech or belonging to the primary industry. The firm should keep an eye on the market, so it knows all its alternative suppliers in the market. In this case, the firm could choose to simply ***ignore*** the punitive measures.

High financial impact, low risk/complexity: SUPPLY CHAIN DIVERSIFICATION

In the case of high financial impact and low risk/complexity, the targeted activity is typically part of the core activity or product and may account for a substantial part of its sales. Typically, punitive measures that restrict commodities would be classified as low risk/complexity, especially if they are traded in the free/open market. Note that risk/complexity dimension is dynamic and subject to world trends and technological development.

Risk/complexity is not only confined to the production phase, but also to the rest of supply chain. Commodities, e.g., might be easy to extrude, but hard or complex to receive (reliable) supplies of. Historic examples would be sanctions on oil or steel upon oil refineries and steel plants. For example, Japan was the subject of heavy sanctions on U.S steel prior to the World War II, and it hampered its economy heavily. Even though the nature of the product might be relatively simple, such as a primary industrial product, the risk/complexity may be high due to supply difficulties. Nowadays, most commodities are low complexity except notable exceptions such as rare earth minerals.

In the typical case of high impact, low risk/complexity, the firm should strive to ***diversify its supply chain.*** A firm might diversity its supply chain both as a pre-emptive risk mitigating strategy, and retroactively as a response to punitive measures targeting its access to inputs.

Low financial impact, high complexity: IGNORE/DIVEST

When the punitive measures have a low financial impact, but high complexity, the firm is not able to produce certain products or services; however, these products or services do not account for a large share of the total revenue of the firm. In the case of the low financial impact with high complexity, the firm can therefore choose to either ***ignore*** or **divest** its activity out of the firm.

For example, when the U.S. restrictions on semiconductors hit Huawei's low-budget smartphones, these offered low-margin profits and accounted for low shares of the total revenue of the firm. As such, Huawei chose to divest this line of products from the firm, while focusing on other countermeasures to respond to activities that had a higher financial impact

High financial impact, high complexity: FULL SPECTRUM EFFORT

When a firm is targeted by both high financial impact and high risk/complexity, it represents the most critical financial impact on the firm, where typically its core activities are involved. The high risk/complexity dimension also indicates that the firm will have difficulties finding alternative supply chain solutions, which limits its ability to respond to the punitive measure.

In such case, a firm should opt for a **full spectrum effort** where it engages in multiple series of risk-mitigating measures available to do its utmost to countermeasure the punitive measure.

Suggested actions for the firm to consider include but is not limited to:

1. Diversify supply chains away from the country imposing punitive measures

2. Co-operate and coordinate with similar firms, suppliers, and/or customers to counter the imposed punitive measures

3. Circumvent the punitive measures by using a third-party agent to import restricted inputs on behalf of the targeted firm

4. Relocate the ownership of the firm's patents to a country deemed less vulnerable to the punitive measures

5. Promoting open, international standards that is not vulnerable to a specific government's control, but freely accessible to any firm

6. Reverse engineer a critical product or components of critical importance that is blocked through a government's punitive measure

7. Stockpile inputs before the punitive measure go into effect

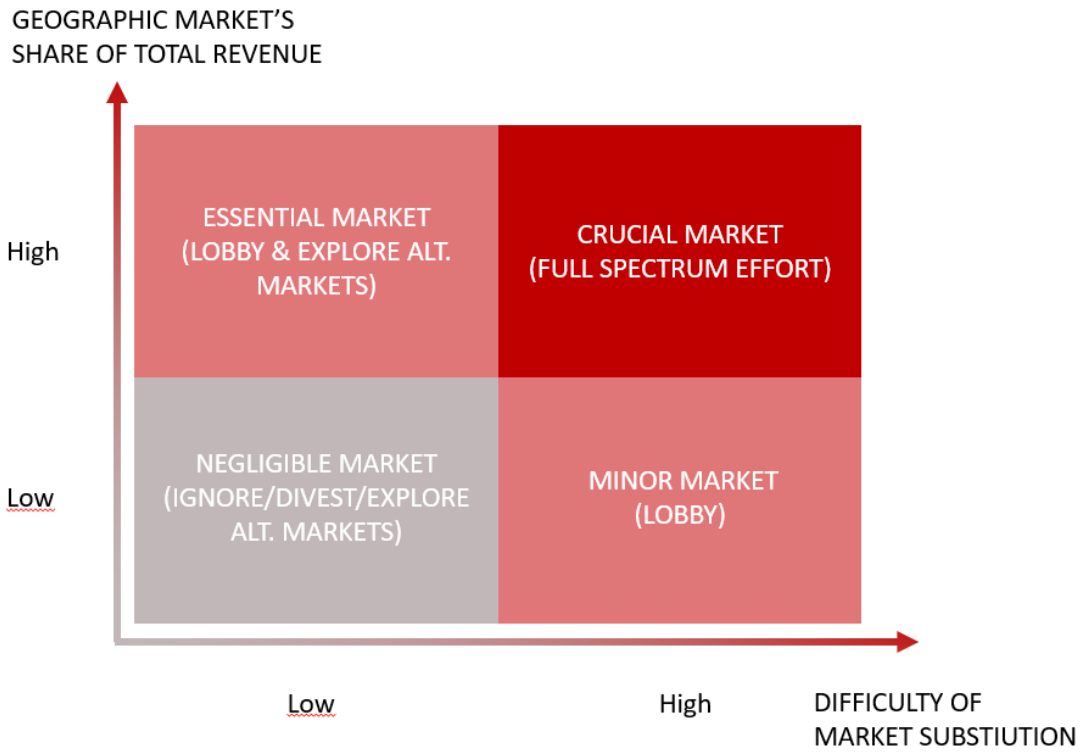
8. Lobby own government to file dispute in the WTO system/exert diplomatic pressure on the imposing country to revoke the punitive measures

9.2 Output side

While the model above describes the optimal strategy towards punitive measures on supplier level, it does not suggest how a firm should act if a country impedes or blocks the sales to its market, i.e., output side.

This model shall describe what kind of countermeasures, pre-emptive or reactive, a firm may implement when the punitive measure restricts a certain market. There are two dimensions: first is the market's share of the firm's total revenue (y-axis). This dimension is similar to the previous model's dimension of financial impact but emphasises the importance and reliance of a firm to a certain market, rather than generalising it to only consider financial impact.

Figure 2: Model on optimal strategy against punitive measures: output side



Source: Author's own creation

The second dimension is the difficulty of substituting the geographic market of interest (x-axis), which refers to the difficulty for the firm to shift its output to alternative markets. In the latter dimension, it is assumed that the firm ideally would wish to keep supplying the original market as it is a profitable or strategically important market for the firm and shifting its supply to an alternative market would yield lower profit margins or be less strategically important than the original market[11].

1. Low share of total revenue, low difficulty of substitution: NEGLIGIBLE MARKET

In this scenario, the punitive measure restricts the targeted firm from selling in a market that accounts for a low share of the firm's total revenue, and the firm can easily substitute the market with an alternative market. In this scenario, it is assumed that the firm ideally would like to keep the original market; however, due to restrictions, it now must re-evaluate its position in said market.

The low share of total revenue implies that the financial impact of losing the market is not high enough to justify the implementation of mitigating strategies focused on retaining the market. The low difficulty of substituting this market with alternative market(s), which might not be as profitable or strategic important as the original market, implies that the firm's cost of shifting its efforts towards this/these market(s) are feasible. Thus, the combination of low share of total revenue and low difficulty of substituting this market deems the market as a **negligible market**, where the optimal strategy would be to *ignore/explore alternative markets.* The strategy suggests that the firm should consider *ignoring* the original market and seek possibilities in alternative geographic or product markets (if applicable[12]). The firm could also consider divesting the business unit or retreat from the market altogether.

Low share of total revenue, high difficulty of substitution: MINOR MARKET

This scenario is similar to the previous scenario, but with some notable differences and areas of focus. In this scenario, it is assumed that the firm is facing a market restriction from a market

[11] If both the original and alternative market yielded the exact same profit margins or had the same strategic importance, it is assumed that the firm would already supply to both markets.

[12] This is only applicable if only certain products/services have been restricted in the original market. E.g., in several European markets, Huawei's 5G telecommunications equipment was banned, while Huawei's mobile phones were not.

that accounts for a low share of the firm's total revenue, but high difficulty of market substitution implies that the costs associated with finding alternative markets are high and not economically feasible.

The combination of low share of total revenue and high difficulty of market substitution suggest that the market is a **minor market,** and the firm should consider to *ignore* or *lobby against* the restriction to this market. The firm should conduct a cost-benefit analysis where it considers the costs of the lobbying efforts and the probability of successfully persuading a government to revoke the punitive measures, with the benefits of staying in the market. If the costs exceed the benefits, the firm should opt to *ignore* the punitive measures, and retreat from the market.

High share of total revenue, low difficulty of substitution: ESSENTIAL MARKET

In this scenario, the targeted geographic market accounts for a considerably share of the firm's total revenue, while the firm can fairly easily find alternative markets. Given the low difficulty of finding an alternative market to supply to, the firm should explore this opportunity. However, given the high share of total revenue derived from this market, it cannot be deemed a negligible market.

The combination of a high share of total revenue derived from this market with the low difficulty of finding a substitute market suggests that that it is an **essential market**. Further, it implies that the opportunity costs of losing this market are higher than the costs associated with implementing efforts against the market restricting punitive measure. Therefore, the firm should utilise a hybrid approach, where it focuses its efforts and resources on *exploring alternative markets* and focuses its efforts and resources on *lobbying* for the market restricting punitive measures to be revoked.

High share of total revenue, high difficulty of substitution: **CRUCIAL MARKET**

In this scenario, the firm derives a high share of total revenue from the market, and there is a high difficulty of substituting this market with an alternative market. The combination of these two factors implies that the market is both highly profitable and of high strategic importance to the firm, whilst few options exist for the firm to replace this market. Therefore, this market is deemed a **crucial market** for the firm.

Given these conditions, the firm should spare no effort in attempting to countermeasure the market restricting punitive measure, as the alternative would be for the firm to surrender its position or divest its assets. A *full spectrum effort* should be considered, where the firm engages in multiple series of countermeasures available to do its utmost to reverse the negative effects of the punitive measure.

1. Modify the product to satisfy new requirement; if not sufficient, reconsider the feasibility of the entire product market or geographic market and consider retreating from the market

2. Shift the firm's business operations to a product that does not fall under the imposed punitive measures

3. Dispute the legality, the scope, and the level of punitive measures through judicial means

4. Lobby own government to file a dispute in the WTO system/exert diplomatic pressure on the imposing country to revoke the punitive measures

5. Co-ordinate with important stakeholders, such as collaborating firms, suppliers, and customers to launch a campaign that counters the imposed punitive measures

9.3 Applying the framework on the Huawei case

This section will apply the above framework on the Huawei case. With the many punitive measures against Huawei, the case is both complex and extensive; however, for the sake of conciseness, the framework is applied in simplified version of the Huawei case.

The punitive measures that have targeted Huawei's input side are primarily related to the designation of Huawei on the U.S. entity list. Initially, the trade blacklist restricted Huawei from accessing key inputs from its U.S. suppliers. Restricting of this input was of high financial impact to Huawei, as it jeopardised its ability to produce some of its most core business products, including 5G equipment and smartphones. However, the risk/complexity was somewhat manageable for Huawei because it was still able to source similar inputs from non-U.S. manufacturers. Therefore, at this point of time, the U.S. entity list represented a punitive measure with **high financial impact** and relative **low risk/complexity.** The

framework suggested action for Huawei would therefore be to undergo *supply chain diversification*.

Indeed, following the initial trade blacklisting of Huawei, it did take steps to reduce its reliance on U.S. chip manufacturers, by shifting its input source from U.S. semiconductor designer to an in-house semiconductor designer that used a non-U.S. semiconductor manufacturer, i.e., Taiwan Semiconductor Manufacturing Company (TSMC).

When the U.S. government tightened its export control on Huawei to also include non-U.S. firms that used U.S.-based technology, the risk/complexity dimension changes from low to **high risk/complexity**, as almost all semiconductor production is based on some U.S. technology, and thus, severely limiting Huawei's ability to find alternative sources of inputs. Therefore, as the framework suggests, Huawei's optimal countermeasure would be to apply *full spectrum efforts*, which it seemingly has done. Some of the many countermeasures it has deployed include stockpiling semiconductors, promoting open semiconductor design standards (RISC-V), heavily investing in R&D, and partnering with domestic firms to build semiconductor plant.

The punitive measures that have targeted Huawei's output side are primarily related to the bans several countries have imposed against its participation in their 5G networks roll-out. While the U.S. market may only represent a smaller share of Huawei's total revenue, if one treats the combined geographic markets of countries that the U.S. has successfully pressured to impose a full or partial ban, this punitive measure represents a **high share of total revenue**. On the other hand, Huawei's difficulty in substituting these markets with other markets is still manageable, as there are other markets in Asia, Africa, and Latin America still accessible to Huawei, Thus, the punitive measure represents a **low difficulty of market substitution**, and further, would indicate that the combined geographic markets that has imposed a ban on Huawei represents an *essential market.*

Under the framework, an *essential market* suggests that the firm should opt for the hybrid approach of *lobbying* the government(s) to revoke the ban, while also exploring alternative markets. Although little information has been made publicly available regarding Huawei's internal strategy, it is reasonable to assume that Huawei has put considerable efforts into lobbying against the ban against them. It has also seemed to re-focus its efforts onto

alternative markets, including its large domestic market. For example, in March 2021, Huawei was reported to seek to deliver ICT solutions to a completely new market, namely Chinese fish farms. It was also reported to exploring the possibility of delivering products and services to the Chinese mining industry, citing specifically the U.S. punitive measures as the motivation for exploring these new markets (Bloomberg, 14 March 2021)

In terms of its grand strategy, Huawei may have retreated parts of its business units from some geographic markets. While it has divested its *Honor* smartphone brand and its submarine cable subsidiary, it has kept its premium Huawei smartphone brand and developed its own smartphone and Internet of Things operating system (*Harmony OS*), as an alternative to Google's Android OS. It has also focused on selling to the Chinese market and other geographic markets not as vulnerable to punitive measures. Additionally, it has invested large amounts of capital in semiconductor expertise and other business areas that are related to its core business. Huawei's grand strategy is to provide its customers telecommunications equipment and devices and related products and services. When faced with punitive measures, some short-term retreats have been made in certain areas to maintain its long-term goal.

10. Conclusion

This thesis has examined the U.S. punitive measures against Huawei. The first notable measures undertaken by the U.S. against Huawei occurred in 2008. Since then, the U.S. punitive measures have inflicted large financial losses for Huawei, as well as for Huawei's suppliers. It seemingly will also cause economic disadvantages for would-be customers in markets where Huawei has been restricted access to participate in the roll-out of 5G networks. The punitive measures have also severely complicated Huawei's operations, particularly in Western markets, forcing it to retreat from certain markets. As not uncommon with economic policies, the campaign against Huawei has also led to some unintended consequences, notably partially causing the chip shortage in the automotive industry, likely design-out of U.S. technology in some parts of the global supply chain and increased Chinese technological self-reliance.

The thesis outlined various common punitive measures the U.S. government possesses in its legal arsenal, as well as the legal foundation of punitive measures and dispute settlements in the WTO framework. The WTO provides a legal and institutional framework that seeks to ensure smooth, predictable, and free trade flow. The campaign against Huawei may be considered as running against the guiding principles of the WTO, and inconsistent with GATT provisions. However, the WTO specifically has national security as a reason for exemption from these guiding principles. There is, however, a precedence that the national security exception should not be unilaterally settled by a country but may be subject to the scrutiny of the WTO Dispute Settlement Body. The big elephant in the room, however, is that the punitive measures imposed by the U.S. out of national security concerns are regarded by many to be a pretext for economic protectionism.

Moreover, the thesis identified key factors that increase the risk for a firm to be targeted by punitive measures by a foreign government. The key factors are (1) Firms originating from a rival country to the issuer of the punitive measure; (2) Firms that have access to private data; (3) Firms engaged in trade of potential dual use items; and (4) Firms operating in an industry of strategic or technological important industry.

Later, key factors that may determine a firm's ability to effectively cope with punitive measures were outlined. The factors are divided into two, the first is market-level conditions,

the second is firm-level conditions. At the market-level, we have factors such as: *share of total sales revenue, reliance on inputs, firm's domestic market, access to well-functioning financial markets, access to domestic* and *foreign talents.* At the firm-level, we have *strong balance sheets, capital expenditure requirements, organisational culture,* and *ownership structure.*

Finally, this thesis sought to create a theoretical framework to define a firm's optimal strategy towards punitive measures – what the firm ought to do to counter the punitive measures. The framework consists of an input side model and an output side model, where the former considers the input, component, or supplier side, while the latter considers the output or market side. It analyses and categorises a firm among four scenarios along two dimensions, 1) how severely the punitive measures impact the firm, and 2) the ease for the firm to find alternative (input or output) and suggests a broader long-term strategy for the firm to consider.

References

Ahrens, N. (2013). *China's Competitiveness: Myth, Reality, and Lessons for the United States and Japan - Case Study: Huawei.* Washington, D.C.: Center for Strategic and International Studies (CSIS).

BBC. (17 April 2000). *Military fears over PlayStation2*. Retrieved April 16, 2021, from BBC News: http://news.bbc.co.uk/2/hi/asia-pacific/716237.stm

BBC. (17 November 2020). *Huawei sells youth brand over tech restrictions*. Retrieved from BBC: https://www.bbc.com/news/world-asia-54970003

BBC. (31 May 2018). *US tariffs: Steel and aluminium levies slapped on key allies*. Retrieved February 16, 2021, from BBC: https://www.bbc.com/news/world-us-canada-44320221

Bloomberg. (14 March 2021). *Huawei Pivots to Fish Farms, Mining After U.S. Blocks Its Phones*. Retrieved from Bloomberg: https://www.bloomberg.com/news/articles/2021-03-14/huawei-pivots-to-fish-farms-mining-after-u-s-blocks-its-phones

Bloomberg. (16 June 2019). *Huawei Braces for Phone Sales Drop of Up to 60 Million Overseas*. Retrieved from Bloomberg: https://www.bloomberg.com/news/articles/2019-06-16/huawei-braces-for-a-steep-drop-in-overseas-smartphone-sales

Bloomberg. (18 July 2020). *U.K. Told Huawei That U.S. Pressure Contributed to Ban: Observer*. Retrieved from Bloomberg: https://www.bloomberg.com/news/articles/2020-07-18/u-k-told-huawei-that-u-s-pressure-contributed-to-ban-observer

Bloomberg. (2 February 2021). *China Stockpiles Chips, Chip-Making Machines to Resist U.S.* Retrieved from Bloomberg: https://www.bloomberg.com/news/articles/2021-02-02/china-stockpiles-chips-and-chip-making-machines-to-resist-u-s

Bloomberg. (22 October 2020). *Huawei Outhustles Trump by Hoarding Chips Vital for China 5G*. Retrieved from Bloomberg: https://www.bloomberg.com/news/articles/2020-10-22/huawei-outhustles-trump-by-stockpiling-chips-needed-for-china-5g

Bloomberg. (7 December 2010). *Locke Says Sprint's Chief Was Called About Huawei Bid Concerns*. Retrieved from Bloomberg: https://www.bloomberg.com/news/articles/2010-12-07/commerce-s-locke-says-sprint-s-chief-was-called-about-huawei-bid-concerns

Bown, C. B. (2020, December 18). How the United States marched the semiconductor industry into its trade war with China. *Peterson Institute for International Economics Working Paper No. 20-16*. Retrieved from https://www.piie.com/publications/working-papers/how-united-states-marched-semiconductor-industry-its-trade-war-china

Broadman, H. G. (2019, January 4). *U.S. Foreign Investment Policy Gets A Tougher But More Transparent CFIUS*. Retrieved from Forbes: https://www.forbes.com/sites/harrybroadman/2019/01/04/u-s-foreign-investment-policy-gets-a-tougher-but-more-transparent-cfius/?sh=76c9d58c1fe6

Brown, H. L. (2001). Extraterritorial Jurisdiction under the 1998 Amendments to the Extraterritorial Jurisdiction under the 1998 Amendments to the Foreign Corrupt Practices Act: Does the Government's Reach Now Foreign Corrupt Practices Act: Does the Government's Reach Now Exc. *North Carolina Journal of International Law, 26*(2), 239-360. Retrieved from https://scholarship.law.unc.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1696&context=ncilj

Caine, K., Franceski, L. G., & Rosenberg, A. L. (2018, August 16). *President Trump signs into law CFIUS reform bill*. Retrieved from Norton Rose Fulbright: https://www.nortonrosefulbright.com/en/knowledge/publications/2405ee63/president-trump-signs-into-law-cfius-reform-bill

Chinn, M. (2018, June 6). *What is the National Security Rationale for Steel, Aluminum and Automobile Protection?* Retrieved February 10 2021, from Econofact:

https://econofact.org/what-is-the-national-security-rationale-for-steel-aluminum-and-automobile-protection

CNBC. (14 May 2021). *Chip shortage expected to cost auto industry $110 billion in revenue in 2021*. Retrieved from https://www.cnbc.com/2021/05/14/chip-shortage-expected-to-cost-auto-industry-110-billion-in-2021.html

CNBC. (24 August 2020). *TikTok reveals detailed user numbers for the first time*. Retrieved from CNBC: https://www.cnbc.com/2020/08/24/tiktok-reveals-us-global-user-growth-numbers-for-first-time.html

Congressional Research Service. (2020). *CFIUS Reform Under FIRRMA.* Congressional Research Service. Retrieved from https://crsreports.congress.gov/product/pdf/IF/IF10952

De Cremer, D., & Tao, T. (2015, June 11). *Huawei's Culture Is the Key to Its Success.* Retrieved from Harvard Business Review: https://hbr.org/2015/06/huaweis-culture-is-the-key-to-its-success

Department of Justice. (2009, 19 November). *tatoil ASA Satisfies Obligations Under Deferred Prosecution Agreement and Foreign Bribery Charges Are Dismissed*. Retrieved from Department of Justice: https://www.justice.gov/opa/pr/statoil-asa-satisfies-obligations-under-deferred-prosecution-agreement-and-foreign-bribery

DeWoskin, K. J. (2001, September). The WTO and the Telecommunications Sector in China. *The China Quarterly*, 630-654.

Diamant, M. S., Sullivan, C. W., & Smith, J. H. (2019). FCPA Enforcement Against U.S. and Non-U.S.Companie. *Michigan Business & Entrepreneurial Law Review, 8*(2), 353-378. Retrieved from https://www.gibsondunn.com/wp-content/uploads/2019/09/Diamant-Sullivan-Smith-FCPA-Enforcement-Against-U.S.-and-Non-U.S.-Companies-Michigan-Business-Entrepreneurial-Law-Review-Spring-2019.pdf

European Commission. (2003, September 23). *China to participate in GALILEO*. Retrieved from European Commission: Internal Market, Industry, Entrepreneurship and SMEs: https://ec.europa.eu/growth/content/china-participate-galileo-0_en

European Commission. (2020, January 29). *Secure 5G networks: Questions and Answers on the EU toolbox*. Retrieved from European Commission: https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_127

Financial Times. (1 November 2020). *Huawei develops plan for chip plant to help beat US sanctions*. Retrieved from Financial Times: https://www.ft.com/content/84eb666e-0af3-48eb-8b60-3f53b19435cb

Financial Times. (18 December 2009). *Huawei beats Ericsson for network contract*. Retrieved from Financial Times: https://www.ft.com/content/dfb2b7f6-ebca-11de-930c-00144feab49a

Financial Times. (23 December 2020). *European tech accuses US of using sanctions to shut it out of China* . Retrieved from Financial Times: https://www.ft.com/content/7baa8caf-ca3f-4d95-967c-e315a3ee348f

Financial Times. (27 September 2020). *China's biggest chipmaker SMIC hit by US sanctions*. Retrieved from Financial Times: https://www.ft.com/content/7325dcea-e327-4054-9b24-7a12a6a2cac6

Gartner. (2021, February 9). *Gartner Says Apple and Samsung Extended Their Lead as Top Semiconductor Customers in 2020* . Retrieved from Gartner: https://www.gartner.com/en/newsroom/press-releases/2021-02-09-gartner-says-apple-and-samsung-extended-their-lead-as

Holmes, K. R. (2015). *What Is National Security?* The Heritage Foundation. Retrieved from https://www.heritage.org/sites/default/files/2019-10/2015_IndexOfUSMilitaryStrength_What%20Is%20National%20Security.pdf

Huang, K., & Madnick, S. (2020, August 28). *The TikTok Ban Should Worry Every Company*. Retrieved November 17, 2020, from Harvard Business Review: https://hbr.org/2020/08/the-tiktok-ban-should-worry-every-company

Huawei. (2020). *2019 Annual Report.* Shenzhen: Huawei Investment & Holding Co., Ltd. Retrieved from https://www-file.huawei.com/-/media/corporate/pdf/annual-report/annual_report_2019_en.pdf?la=en

Huawei. (2020, November 17). *Statement, 17 November 2020*. Retrieved from Huawei: https://www.huawei.com/en/news/2020/11/huawei-honor-statement

Jackson, J. K. (2020, February 14). *The Committee on Foreign Investment in the United States (CFIUS).* Retrieved from Congressional Research Service: https://fas.org/sgp/crs/natsec/RL33388.pdf

Lobel, M. (2014). *Security risks and responses in an evolving telecommunications industry.* Pwc. Retrieved from https://www.pwc.com/gx/en/communications/publications/communications-review/assets/cyber-telecom-security.pdf

Lund, S., Manyika, J., Woetzel, J., Barriball, E., Krishnan, M., Alicke, K., . . . Hutzler, K. (2020). *Risk, resilience, and rebalancing in global value chains.* McKinsey Global Institue (MGI). Retrieved from https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Operations/Our%20Insights/Risk%20resilience%20and%20rebalancing%20in%20global%20value%20chains/Risk-resilience-and-rebalancing-in-global-value-chains-full-report-vH.pdf

Masters, J. (2019, August 12). *What Are Economic Sanctions?* Retrieved September 5, 2020, from Council on Foreign Relations (CFR): https://www.cfr.org/backgrounder/what-are-economic-sanctions

McVey, T. B. (2019). *U.S. Sanctions Laws: Dangers Ahead For Foreign Companies.* Williams Mullen. Retrieved from https://www.williamsmullen.com/sites/default/files/files/U_S_%20Sanctions%20Laws%20Dangers%20Ahead%20For%20Foreign%20Companies%20(Part%20I)%20McVey.pdf

Mirenda, A. D., & Smith, G. A. (2013, February 19). *Business Crimes Alert*. Retrieved from Foley Hoag LLP: https://foleyhoag.com/publications/alerts-and-updates/2013/february/increased-risk-of-fcpa-prosecution-of-foreign-national-executives-021913

Nikkei. (23 October 2020). *Huawei's Q3 growth slows as 'intense' US pressure hits supplies*. Retrieved from Nikkei Asia: https://asia.nikkei.com/Spotlight/Huawei-crackdown/Huawei-s-Q3-growth-slows-as-intense-US-pressure-hits-supplies

Oxford Economics. (2020). *Restricting Competition in 5G Network Equipment Throughout Europe: An Economic Impact Study.* London: Oxford Economics.

Peng, Z. (2020, August 14). *Is China's BeiDou a Better Version of GPS and GLONASS?* Retrieved from Equal Ocean: https://equalocean.com/analysis/2020082614631

Reinsch, W. A. (2019, April 5). *The WTO's First Ruling on National Security: What Does It Mean for the United States?* Retrieved January 14, 2021, from Center for Strategic and International Studies (CSIS): https://www.csis.org/analysis/wtos-first-ruling-national-security-what-does-it-mean-united-states

Reuters. (1 January 2021). *NYSE starts process of delisting three Chinese telco companies*. Retrieved from Reuters: https://www.reuters.com/article/us-usa-china-nyse-delisting-idUSKBN29621Q

Reuters. (12 December 2018). *Exclusive: Trump says he could intervene in U.S. case against Huawei CFO*. Retrieved from Reuters: https://www.reuters.com/article/us-usa-trump-huawei-tech-exclusive-idUSKBN1OA2PQ

Reuters. (14 January 2021). *Trump bolsters ban on U.S. investments in China*. Retrieved from Reuters: https://www.reuters.com/world/china/trump-signs-amended-china-investment-ban-requiring-complete-divestment-by-nov-2021-01-14/

Reuters. (15 January 2021). *Trump's China tech war backfires on automakers as chips run short*. Retrieved from Reuters: https://www.reuters.com/business/autos-transportation/trumps-china-tech-war-backfires-automakers-chips-run-short-2021-01-15/

Reuters. (15 july 2020). *Pompeo says U.S. to impose visa curbs on Huawei over rights*. Retrieved from Reuters: https://www.reuters.com/article/us-usa-china-huawei-idUSKCN24G268

Reuters. (15 May 2020). *U.S. moves to cut Huawei off from global chip suppliers as China eyes retaliation*. Retrieved from Reuters: https://www.reuters.com/article/us-usa-huawei-tech-exclusive-idUSKBN22R1KC

Reuters. (16 May 2019). *China's Huawei restricted from using U.S. suppliers*. Retrieved from Reuters: https://www.reuters.com/article/us-usa-huawei-tech-commerce-idUSKCN1SM2MG

Reuters. (16 May 2019). *Huawei's $105 billion business at stake after U.S. broadside*. Retrieved from Reuters: https://www.reuters.com/article/us-usa-trade-china-huawei-analysis-idUSKCN1SM123

Reuters. (17 January 2021). *Exclusive: Trump admin slams China's Huawei, halting shipments from Intel, others - sources*. Retrieved from Reuters: https://www.reuters.com/article/us-usa-huawei-tech-exclusive-idUSKBN29M0KD

Reuters. (17 October 2012). *Exclusive: White House review finds no evidence of spying by Huawei - sources*. Retrieved from Reuters: https://www.reuters.com/article/us-huawei-spying-idUSBRE89G1Q920121017

Reuters. (19 February 2011). *Huawei backs away from 3Leaf acquisition*. Retrieved from Reuters: https://www.reuters.com/article/us-huawei-3leaf-idUSTRE71I38920110219

Reuters. (19 May 2019). *Exclusive: Google suspends some business with Huawei after Trump blacklist - source*. Retrieved from Reuters: https://www.reuters.com/article/us-huawei-tech-alphabet-exclusive-idUSKCN1SP0NB

Reuters. (22 December 2013). *SPECIAL REPORT-In satellite tech race, China hitched a ride from Europe*. Retrieved from Reuters: https://www.reuters.com/article/breakout-beidou-idUSL4N0JJ0J320131222

Reuters. (23 February 2008). *3Com rebuff due to 'complexities' and costs -Huawei*. Retrieved from Reuters: https://www.reuters.com/article/us-huawei-3com-idUSHKG5460020080223

Reuters. (24 August 2010). *US senators raise concern about Huawei-Sprint deal.* Retrieved from Reuters: https://www.reuters.com/article/usa-china-telecoms/us-senators-raise-concern-about-huawei-sprint-deal-idUSN2425764520100824

Reuters. (24 June 2020). *Exclusive: Trump administration says Huawei, Hikvision backed by Chinese military*. Retrieved March 26, 2021, from Reuters: https://www.reuters.com/article/us-usa-china-military-exclusive-idUSKBN23V309

Reuters. (25 November 2019). *U.S.-based chip-tech group moving to Switzerland over trade curb fears*. Retrieved from Reuters: https://www.reuters.com/article/us-usa-china-semiconductors-insight-idUSKBN1XZ16L

Reuters. (26 August 2020). *China to import $300 billion of chips for third straight year: industry group*. Retrieved from Reuters: https://www.reuters.com/article/us-china-semiconductors-idUSKBN25M1CX

Reuters. (3 June 2019). *Nokia says it has moved ahead of Huawei in 5G orders*. Retrieved from Reuters: https://www.reuters.com/article/us-nokia-5g-idUSKCN1T428W

Reuters. (5 December 2018). *Top Huawei executive arrested on U.S. request, clouding China trade truce*. Retrieved from Reuters: https://www.reuters.com/article/us-usa-china-huawei-idUSKBN1O42S1

Reuters. (8 January 2018). *Huawei's AT&T U.S. smartphone deal collapses*. Retrieved from Reuters: https://www.reuters.com/article/us-at-t-huawei-tech-idUSKBN1EX29E

Secretary of Defense. (n.d.). *Department of Defense Memo: Response to Steel and Aluminum Policy Recommendations*. Retrieved from U.S. Department of Commerce: https://www.commerce.gov/sites/default/files/department_of_defense_memo_response_to_steel_and_aluminum_policy_recommendations.pdf

SEMI. (2020, August 24). *SEMI Statement on New U.S. Export Control Regulations*. Retrieved from SEMI: https://www.semi.org/en/news-media-press/semi-press-releases/semi-export-control

The New York Times. (17 March 2019). *U.S. Campaign to Ban Huawei Overseas Stumbles as Allies Resist*. Retrieved from The New York Times: https://www.nytimes.com/2019/03/17/us/politics/huawei-ban.html

The New York Times. (24 December 2020). *With Money, and Waste, China Fights for Chip Independence*. Retrieved from The New York Times: https://www.nytimes.com/2020/12/24/technology/china-semiconductors.html

The Wall Street Journal. (16 July 2020). *A Pandemic and Huawei Woes? No Problem, Says Taiwan's Chip Champion.* . Retrieved from The Wall Street Journal: https://www.wsj.com/articles/a-pandemic-and-huawei-woes-no-problem-says-taiwans-chip-champion-11594899491

The Wall Street Journal. (19 September 2020). *Trump Signs Off on TikTok Deal With Oracle, Walmart*. Retrieved November 19, 2020, from The Wall Street Journal: https://www.wsj.com/articles/trump-signs-off-on-deal-allowing-tiktok-to-continue-u-s-operations-11600551352?mod=article_inline

The Washington Post. (1 March 2021). *Biden can't fix the chip shortage any time soon. Here's why.* Retrieved from The Washington Post: https://www.washingtonpost.com/technology/2021/03/01/semiconductor-shortage-halts-auto-factories/

The White House. (2020, November 12). *Executive Order on Addressing the Threat from Securities Investments that Finance Communist Chinese Military Companies*. Retrieved January 5, 2021, from The White House: https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-addressing-threat-securities-investments-finance-communist-chinese-military-companies/

The White House. (2020, August 14). *Order Regarding the Acquisition of Musical.ly by ByteDance Ltd*. Retrieved from The White House: https://trumpwhitehouse.archives.gov/presidential-actions/order-regarding-acquisition-musical-ly-bytedance-ltd/

Townsend, T. (2020, April 15). *The Aggressive Extraterritorial Reach of U.S. Economic Sanctions: Foreign Company Exposure to OFAC Enforcement*. Retrieved August 25, 2020, from The National Law Review: https://www.natlawreview.com/article/aggressive-extraterritorial-reach-us-economic-sanctions-foreign-company-exposure-to

TrendForce. (2020, October 5). *China's Semiconductor Industry to Brace for Impact as SMIC Assesses Export Restrictions Placed by U.S., Says TrendForc*. Retrieved from TrendForce: https://www.trendforce.com/presscenter/news/20201005-10499.html

U.S. Department of Commerce. (2020). *CBC FAQs - 1. What is the Entity List?* Retrieved August 26, 2020, from Bureau of Industry and Security: https://www.bis.doc.gov/index.php/cbc-faqs/faq/281-1-what-is-the-entity-list

U.S. Department of Commerce. (n.d.). *Entity List*. Retrieved August 26, 202, from Bureau of Industry and Security: https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list

U.S. Department of State. (2020, July 15). *U.Michael R. Pomepo, Press Statement: Visa Restrictions on Certain Employees of Chinese Technology Companies that Abuse Human Rights*. Retrieved October 15, 2020, from https://2017-2021.state.gov/u-s-imposes-visa-restrictions-on-certain-employees-of-chinese-technology-companies-that-abuse-human-rights/index.html

U.S. Department of the Treasury. (2018, April 6). *Treasury Designates Russian Oligarchs, Officials, and Entities in Response to Worldwide Malign Activity*. Retrieved August 25, 2020, from U.S. Department of the Treasury: https://home.treasury.gov/news/press-releases/sm0338

U.S. Department of the Treasury. (n.d.). *Sanctions Programs and Country Information*. Retrieved August 25, 2020, from U.S. Department of the Treasury: https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information

U.S. Securities and Exchange Commission. (2008, December 15). *SEC Charges Siemens AG for Engaging in Worldwide Bribery*. Retrieved from U.S. Securities and Exchange Commission: https://www.sec.gov/news/press/2008/2008-294.htm

Wassebaar Arragement Secretariat. (2020). *Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies: List of Dual-Use Goods and Technologies and Munitions List.* Retrieved April 15, 2021, from https://www.wassenaar.org/app/uploads/2020/12/Public-Docs-Vol-II-2020-List-of-DU-Goods-and-Technologies-and-Munitions-List-Dec-20-3.pdf

Wassenaaar. (2020, December 17). *About us*. Retrieved April 16, 2021, from Wassenaar: https://www.wassenaar.org/about-us/

Westbrook, A. D. (2019, December 6). Securing the Nation or Entrenching the Board? The Evolution of CFIUS Review of Corporate Acquisitions. *Marquette Law Review, 102*, 643-699. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3490830

White House. (2019, May 15). *Executive Order on Securing the Information and Communications Technology and Services Supply Chain*. Retrieved from The White House: https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/

World Trade Organization. (2019). *Russia — Measures Concerning Traffic in Transit*. Retrieved March 25, 2021, from World Trade Organization: https://www.wto.org/english/tratop_e/dispu_e/cases_e/ds512_e.htm

World Trade Organization. (n.d.). *Article XXI: Security Exceptions*. Retrieved from WTO: https://www.wto.org/english/res_e/publications_e/ai17_e/gatt1994_art21_gatt47.pdf

World Trade Organization. (n.d.). *The WTO*. Retrieved March 3, 2021, from World Trade Organization: https://www.wto.org/english/thewto_e/thewto_e.htm

World Trade Organization. (n.d.). *UNDERSTANDING THE WTO: SETTLING DISPUTES: A unique contribution*. Retrieved March 25, 2021, from World Trade Organization: https://www.wto.org/english/thewto_e/whatis_e/tif_e/disp1_e.htm

WTO. (n.d.). Article III: National Treatment on Internal Taxation and Regulation. Retrieved from https://www.wto.org/ENGLISH/res_e/booksp_e/gatt_ai_e/art3_e.pdf

Zakaria, F. (2020, August 28). *America's excessive reliance on sanctions will come back to haunt it*. Retrieved September 2 2020, from The Washington Post: https://www.washingtonpost.com/opinions/global-opinions/americas-excessive-reliance-on-sanctions-will-come-back-to-haunt-it/2020/08/27/e73a9004-e89c-11ea-970a-64c73a1c2392_story.html

Zeng, D. Z. (2010). *Building Engines for Growthand Competitiveness in China: Experience with Special Economic Zonesand Industrial Clusters.* Washington, D.C.: The World Bank.