C. WALDEMARSSON & W. SARASTO LÖWENBERG

No Way or the Huawei?

A Grounded Theory Approach to the 5G Debate in the EU

Master Thesis

Master in International Business and Politics

COPENHAGEN BUSINESS SCHOOL
HANDELSHØJSKOLEN

2020-05-15

Student Number: 125226; 124522
STU (Pages): 238.850 (105)
Supervisor: Eleni Tsingou

“Out of intense complexities, intense simplicities emerge.”

- Winston Churchill

Abstract

This study has analysed the debate on whether to ban Huawei in the European roll-out of 5G networks to address the current lack of nuance and oversimplification that has come to characterize the public discussion as of recent. Using a grounded theory approach, a large number of policy documents, government reports, EU publications, think tank reports, news articles and white papers have been coded and analysed in an attempt to break down the risks and underlying challenges facing the European Union in the Huawei debate. The result of the analysis was a comprehensive framework outlining the key features of the debate and how they relate to each other. Three main risks were identified in the data, each representing a specific aspect of the Huawei and 5G debate; *(I) Technical risks; (II) Industrial risks and (III) Structural risks*. The risks were further analysed and enabled the identification of three underlying challenges corresponding to the three risk categories: *trust*, *competitiveness,* and *unity*. These challenges were in turn conceptualized to increase the understanding of how they affected the European Union and its role in the Huawei and 5G debate. The research concluded that all risks and challenges were linked by their geopolitical nature and the notion of European autonomy. The Huawei debate has come to reflect a number of broader concerns, anxieties and woes about the EU project and its role in a geopolitical climate characterized by changing power structures – stretching far beyond the binary decision of allowing a Chinese vendor in EU's 5G implementation.

Keywords: Huawei; 5G; Grounded Theory; European Union; Telecommunication; Risk; Geopolitics; China

Acknowledgement

The authors would like to thank Eleni Tsingou of Copenhagen Business School for excellent supervision, insightful discussions, and unconditional support throughout the writing of this thesis.

TABLE OF CONTENTS

INDEX OF FIGURES AND TABLES

APPENDICES

1. INTRODUCTION

The global introduction of the next generation of mobile internet connectivity is upon us, with an expected first large-scale roll-out of 5G networks in 2020. The fifth-generation telecommunications networks are set to revolutionize multiple spheres of our society and lay the foundation for a range of novel technologies using artificial intelligence and machine-to-machine communication.[1] By offering faster speeds and the ability to host a significantly increased number of devices, 5G will open the door for new innovations such as smart industries, autonomous vehicles and the internet of things - bringing a range of new opportunities and serving as a catalyst in the transfer to a digital economy.[2] The new telecommunication networks are estimated to add a staggering $13.2 trillion in global economic value and 22.3 million jobs by 2035 in the global 5G value chain alone[3], making the importance of the 5G introduction for our societies and economies difficult to underestimate. As our future critical infrastructure will become increasingly dependent on telecommunications technology and the security of these networks, the governance and control of 5G operations will have implications also for the protection of national security, making it a prioritized issue for governments around the world.

The discussion of 5G implementation in the European Union has however come to focus less on the new possibilities these technologies offer and instead been dominated by the question of whether Chinese telecom vendor Huawei should be allowed to participate in the European build-out of the next generation of networks. The debate has mainly put attention on whether Huawei, one of the world's largest vendors of 5G technology with an increasing presence on the European markets, can be trusted to provide critical infrastructure in the European Union, with several countries either banning or postponing a decision on the matter with reference to national security considerations. Worries about the allegedly close governmental ties between Huawei and the Chinese government are used as the main explanation behind these concerns, and the risk that Huawei's access to European 5G networks could be used as a gateway for Chinese industrial espionage or sabotage of critical infrastructure in the West has resulted in a fierce debate. Simultaneously, Huawei and the Chinese government have denied more or less all the charges put forward and instead criticized the Western stance,[4] accusing it of being hidden protectionism and an unjustified attempt to protect the domestic industry.[5] These

[1] (Rühlig & Björk, 2020)
[2] (Triolo, Allison, & Brown, 2018)
[3] (Issa & Jha, 2019)
[4] (BBC, 2019)
[5] (Reuters, 2019)

allegations are particularly sensitive considering that Huawei's strongest competitors, Ericsson and Nokia, are European based.

Being connected to the 5G networks is described as equally important as having access to electricity,[6] and the Huawei debate has therefore become increasingly politicized. The framing of the debate in the public has also come to reflect the broader geopolitical tensions between China and the United States, which are played out on multiple arenas - not least seen in the global trade conflict and the rhetoric surrounding the recent outbreak of the covid-19 virus. The United States placed a ban on Huawei and the Chinese state-owned telecom equipment manufacturer ZTE in 2019 with reference to national security,[7] significantly affecting Huawei's operations and participation in the country's 5G roll-out and has since been pushing Western allies to follow-suit.[8] The US ban of Huawei has since then been mirrored by allies such as Australia and Japan.[9] The language used in the debate has become increasingly aggressive, and the competition or leadership in 5G technology is often framed as a *race* or a *battle*, not only between companies and states, but *between political systems.*[10] Europe finds itself in a difficult situation, being squeezed between the US and China and pressured to make decisions for the 5G roll-out.

The European Union is sometimes described as "caught in the middle of a geopolitical struggle", with a choice of either going "East or West". [11] While the EU seems reluctant to make such a binary choice, the situation is complicated by the already existing dependencies and diplomatic relations that exists between individual member states and China and the US respectively, with hard diplomatic pressures to align with either the US or China to avoid repercussions or worsened relations. This is reflected in the different approaches taken by the member states, leading to increased fragmentation on the issue. At the same time, worries about increased Chinese investments in sectors critical for security has by no means emerged first with the Huawei debate, but rather been a topic of discussion over the last decade. The rapid implementation of an investment screening mechanism for FDI into the union in 2019, by many seen as a direct response to Chinese investments, is a result of these concerns.[12] Although the EU member states initially

[6] (Kleinhans, 2019)
[7] (Bloomberg, 2018)
[8] (Wintour, 2020)
[9] (Rühlig & Björk, 2020)
[10] (Kleinhans, 2019)
[11] (Albrycht & Świątkowska, 2019)
[12] (BBC, 2019)

responded individually on their respective policy towards Huawei, initiatives are now taken for a more unified approach among the 27 member states.

The Huawei debate is truly multifaceted and interdisciplinary, and has come to represent broader, underlying challenges for the European Union going forward. Despite the inherent complexity, the public debate is often oversimplified and framing the European Union's options going forward as a binary choice between banning Huawei or not, with few attempts to go beyond the simple references to "protection of national security" as the main explanation for a potential ban on Huawei in Europe. The lack of nuance in the debate and the framing of the discussion provides an insufficient account of the actual challenges the European Union is facing following the Huawei debate and runs the risk of emphasizing an already polarized climate, contributing to an overall sense of "fear-mongering" and conflict escalation. Given the one-dimensional coverage of the debate, this thesis aims to give a more granular outline of the risks and challenges that comes with the Huawei debate in the introduction of 5G networks. This leads to the research question of this thesis.

1.1 Research question

What are the main risks identified in debate on Huawei and European 5G implementation, and what underlying challenges does the debate represent for the European Union?

1.2 Purpose and delimitation

It becomes evident from the introduction that the Huawei debate is both wicked, multifaceted and interdisciplinary in nature, requiring an understanding of fields such as technology, economics, international relations and business to fully account for the underlying challenges in the debate. This paper aims to provide a disaggregated and granular understanding of the current debate concerning Huawei and 5G deployment in the European Union. By using a grounded theory approach, this research makes use of document analysis to examine a wide range of data sources, including policy documents, expert reports, academic articles, EU publications and news articles to break down the debate into its components. The aim of the thesis is thereafter to conceptualize the risks and challenges facing the European Union to create a comprehensive framework, increasing the understanding of the complex considerations behind the decision to allow or ban Chinese investments in critical infrastructure in the European Union.

Of interest is thus to engage with the '*hows*' and the '*whys*' of the debate, transcending the spheres outlined above so as to provide a coherent and nuanced account of the central issues and risks as understood by the actors involved. What stakeholders are voicing their concerns in the debate? How can national security be understood in times when telecommunication systems are increasingly important for vital societal functions? And what role does the internal fragmentation between member states in the European Union play in the debate?

As suggested by the above research question and purpose, the thesis delimits itself to challenges of the debate of Huawei as faced by the European Union *as a whole*, and not the individual member states. While there is merit to examining the responses and challenges of individual countries and member states, this research is particularly interested in understanding the complexity of the issue stemming from the internal tensions arising from coordinating 27 member states within the European Union. While the United States indeed holds a prominent role in the debate as the *de facto* leader of the current crusade on Huawei, this thesis wants to highlight that the multifaceted nature of the debate is most evident in the case of the European Union. In addition, this thesis will not extend its scope beyond the debate on Huawei to for example include Chinese telecom vendor ZTE. There are indeed similarities in the respective discussions on allowing Huawei and ZTE access to European telecom markets, but also clear differences – primarily in the fact that ZTE is state-owned, making the discussion on governmental ties of less importance. In addition, the market share for ZTE is not close to that of Huawei. In short, there is a reason why the heated public debate has come to focus on Huawei, and these factors are also important in the choice of Huawei as the main focus of this thesis. Although the framework and reasoning of this paper could be applied to understand similar debates on decisions to allow foreign investments in critical infrastructure – and such applications are indeed encouraged - the 5G and Huawei debate will be the exclusive focus of this thesis, as the debate is both topical and speculated to likely be reflective of future discussion similar in nature.

The grounded theory approach allows the researchers to go back and forth between analysis and data collection to continuously increase both the understanding and level of abstraction, while not being bound by previous theoretical accounts of the debate. This approach is aiming to create a bottom-up outline of the most important aspects of the Huawei debate in the European Union. A more in-depth explanation of the framework of this thesis, including the distinction between the unit of analysis and level of abstraction,

can be found in chapter 5.5. Lastly, the aim of the thesis is *not to provide a prediction* of the outcome of the debate. Neither is it intended as a set of recommendations for the European Union. Instead, the goal is to provide the first academic account of the Huawei debate from a European Union perspective. By categorizing the identified risks in the debate, the research allows for the formation of underlying concepts that serves as deeper, more fundamental concerns for the future strategy of the European Union.

1.3 Structure of the thesis

The rest of the thesis is structured as follows; Chapter 2 provides the reader with a broad background on the topics important for the rest of the thesis, including an outline of the history of telecommunications and its technical aspects, the rising Chinese economy and the history of Huawei, and the European investment climate and telecom market. The background chapter is followed by a description of the methodology and research design of this paper, found in chapter 3. Thereafter, chapter 4 will give the reader an initial understanding of the preliminary findings in the purposive sample of this paper. The chapter on preliminary findings is included to provide the reader with the necessary knowledge and scene setter to better grasp the context of the subsequent analysis, but also a chapter reflective of the methodology of this paper, where the researcher continuously further their knowledge of the research topic.

After presenting the main identified risk categories of the Huawei debate towards the end of chapter 4, the following chapter will provide the majority of the analysis in this paper. The analysis in chapter 5 is initially structure around the three main risk categories presented in the preliminary findings to thereafter "climb the analytical ladder" and increase the level of abstraction to identify a number of underlying challenges that these risks come with. The analysis chapter will then continue by introducing the theoretical framework developed in this paper and discuss its characteristics, to thereafter discuss the geopolitical considerations of the Huawei debate. Chapter 6 provides the reader with the main conclusions of the analysis and a summary of the findings, and the paper is thereafter rounded off with a discussion chapter.

2. BACKGROUND

2.1 Reader's guide

The following chapter introduces the themes which represent the foreground of the current debate regarding Huawei and 5G in the European Union, including both technical and historical aspects. The chapter begins with a brief historical look at mobile telecommunications and a conceptual outline of how 5G technology differs from previous generations of telecommunication networks. This is followed by an overview of the telecommunication sector in Europe, a sector first characterized by industrial policies and national champions to later see increased liberalization and free competition. These subchapters are followed by a brief historical account of the rapidly growing Chinese economy and the history of a highly successful product of China's expanding economy - telecom firm Huawei. The background chapter is thereafter rounded off by a section on the investment climate in the European Union and its view on the increased Chinese presence on the EU markets.

2.2 Telecommunications

This chapter introduces mobile telecommunications, defined as the *"aggregate local-area wireless transmission technologies and infrastructures which connect individual customers to the network through the use of mobile devices"*.[13] As such, the chapter first provides a brief outline of the developments which has led to the fifth generation of telecommunications technology, to thereafter provide a conceptual overview of telecom network infrastructure, both generally and in the case of 5G. This is done to introduce the more technical considerations which underpin the subsequent chapters and discussions of this thesis.

Mobile telecommunication has undergone significant changes over the last forty years. These have happened in a series of successions, commonly referred to as *mobile generations*.[14] Each of these generations have led up to the functionalities and speeds which are associated with telecommunication today, like mobile internet and text messaging. Since the first generation, 1G, introduced wireless cellular technology and voice calls in the 1980s, subsequent generations have been introduced in decade-long

[13] (Claici *et al.,* 2017)

[14] (Clark, 2020)

intervals. The second generation, 2G, enabled data services, including text and picture messages, while 3G introduced faster data-transmission speed which enabled the *"mobile broadband"* and effectively brought mobile users online.[15] This was followed by 4G, providing increased the data speeds and introduced functions which users are familiar with today, such as live streaming and video conferencing. Fast forward to present day and the commercial introduction of 5G is upon us.

2.2.1 Mobile network infrastructure and how 5G differs

To appreciate the implications of 5G one must first understand how it differs from prior generations, both in terms of infrastructure and capabilities. This subchapter will therefore provide a conceptual overview of how telecom network infrastructure functions to showcase why and how 5G differs. In a simplified version of a telecom network, there are essentially three components: (1) a network of antennas and masts referred to as the *Radio Access Network* (RAN); (2) the central, integral network known as the *core network*; and (3) *the mobile devices* which connect to the network in order to communicate.[16] The RAN are made up of the various masts and phone towers which allow data signals to be transferred between cellular devices. These signals are routed through the core network, which carries out the authorization and invoicing of phone calls and services and thus represents a crossroad for enormous amounts of personal data. As such, it is the core network that routes calls and data transfers between different mobile devices. Each mobile network operator – the companies which carries out cellular services, such as *TDC* or *Telia*, have their own core network verifying user data.[17] These core networks are in turn interlinked with one another.

The above stylized overview of the architecture and function of networks has held for all of the previous generations of telecom. This is however expected to fundamentally change with 5G. To fully appreciate these infrastructural changes however, one must consider *what 5G is* and how it differs from prior generations of telecommunication technologies. In much of the current media coverage, 5G is described in broad strokes, in terms of the expected benefits or simply as a *"faster 4G"*.[18] Although 5G indeed is both expected to be much faster than 4G and to come with a range of various benefits - and conversely stakes, neither of these provide the full picture. Accordingly, given that 5G – or any prior generation of mobile networks for that matter – is not one singular

[15] (Clark, 2020)
[16] (Gupta & Kumar Jha, 2015)
[17] (Husar, Komada, & Habanova, 2019)
[18] (Rockman, 2019)

technological advancement but a combination of legacy and novel technologies, attention must be put to its components. In essence, there are three technologies which underpin 5G, all separating it from previous generations of telecom: (1) *millimetres waves*; (2) *small cells networks*; and (3) *massive MIMO*.[19] These three are conceptualized and contrasted to prior generations below.

All mobile communication consists of data being transferred between *nodes* in a network – all done via radio signals residing in a specific *frequency spectrum*. However, as an increasing number of mobile devices connect to the network, this slot of the spectrum becomes 'overcrowded' which leads to lost signals or slower data speeds. To put this in perspective, data traffic from mobile devices increases by an estimated 53% annually.[20]The first technology which is expected to be introduced with 5G is thus a way to open more *'digital real estate'* by sending signals at a different, higher frequency than previously, called *millimetres waves*. By using a higher frequency, the overall spectrum used for telecommunication broadens, allowing for more devices to connect without lost signals or slowed-down speeds. Until very recently, millimetres waves have only been used for satellites and radar systems. To utilize millimetres waves to communicate between base stations and mobile devices is however a novel use of this technology.

By transmitting signals via millimetres waves, more devices can come online.[21] On the other hand, the drawback of millimetres waves is that these frequencies do not travel as well through objects, forestry or buildings as those currently used, and they cannot travel as far either. In short, if there is an obstacle in the way the signal will be lost. To cater the introduction of millimetres waves, a second novel technology will be used, called *small cells*. In simple terms, small cells are low-powered network nodes similar to the masts and antennas we are already familiar with, yet with smaller area coverage. Whereas the masts used in today's networks can reach a coverage of up to 40 kilometres, small cells' coverage ranges between ten meters up to a few kilometres.[22] Accordingly, to cater the use of millimetres waves a vast network of small scale, low-powered transmitters will be installed on buildings, rooftops and the like to assure that there is a constant signal.

Current base stations in 4G networks have a dozen ports on average for antennas which handle all the cellular traffic for that base station. These ports are together called Multiple Input Multiple Output (MIMO) as they route the various inputs and outputs traveling through the base stations. As a result of technological advancements and cost

[19] (Gupta & Kumar Jha, 2015)
[20] (Nordrum & Clark, 2017)
[21] (Nordrum & Clark, 2017)
[22] (Nordrum & Clark, 2017)

reductions[23], it is now possible to equip base stations with about one hundred ports - referred to as *massive MIMO.*[24] Massive MIMO for more data to travel through the base station and increases in network capacity by a factor of twenty-three or more.

What is suggested to be transformative about 5G however transcends just higher data speeds and a denser telecom network. What makes 5G different is that it, compared to previous generations, has developed and fine-tuned user-to-user communication (e.g. voice calls, text messages), making 5G enable machine-to-machine communication at large scale.[25] As such, 5G is seen as the catalyst for the digital economy, by enabling autonomous vehicles, smart industries or any other application of artificial intelligence (AI) and machine learning. As these technologies themselves are commonly argued to be key driver in revolutionizing our societies across levels, it is easier to understand the overall implications of 5G. Indeed, according to some estimates, 5G expected to enable more than $13 trillion of global economic output in the next 15 years.[26] Economically then, much is deemed to be at stake.

In summary, while there are various other features and functionalities that define telecom networks generally, and 5G technology specifically, the above conceptual overview is aiming to makes the main implications clearer. It should be beyond doubt that the topic of this thesis thereby concerns something more fundamental than a *"faster 4G"*.[27] Accordingly, when 5G is discussed throughout this thesis, it is in reference to the characteristics and implications outlined above. Given how this paper emphasizes 5G deployment in the European context, the official EU definition of 5G networks is adopted. As such, 5G networks are defined as '*all relevant network infrastructure elements for mobile and wireless communications technology used for connectivity and value-added services with advanced performance characteristics...These may include legacy networks elements based on previous generations of mobile and wireless communications technology such as 4G or 3G*'.[28]

2.3 The European Union and telecommunication

To appreciate the challenges of 5G deployment in the context of the European Union, it is useful with a basic understanding of the European telecom market and sector. This subchapter therefore provides a brief historical account of telecommunication in the EU,

[23] (Gupta & Kumar Jha, 2015)
[24] (Nordrum & Clark, 2017)
[25] (Triolo, Allison, & Brown, 2018)
[26] (Campbell, o.a., 2019)
[27] (Rockman, 2019)
[28] (European Commission, 2019)

both in terms of politics and industry. The *European telecom sector* as defined in this section consists of the aggregate 27 European Union member states' individual markets. Accordingly, there is no common EU telecoms market to mention, although it has been on the agenda of policy makers[29] and businesses.[30] As will be discussed in later sections of this thesis, the challenges the European Union is facing today stand in reflection of the policies of yesterday.

To understand the developments that lead to the present situation, one must first familiarize oneself with the EU telecom sector in terms of its structure, governance and actors. While the individual markets are bound by European legislation, it is still interpreted and enacted by *National Regulatory Authorities* (NRAs) in the individual member states.[31] While the regulation on telecom is rather all-encompassing, there are certain regulatory aspects which remains within the jurisdiction of the member states, such as licensing and procurement of mobile infrastructure. Within and across these individually regulated telecom market there are two sub-sectors, each of which corresponding to one market actor: (1) *mobile telecom services*; and (2) *telecom equipment and infrastructure*. Mobile telecom services are provided by mobile network operators (MNO) such as *Telia*, *TDC* or *Deutsche Telekom*. MNOs own or control the access to a radio spectrum licenses, which are issued by the NRA. Telecom equipment vendors (TEV) such as *Ericsson*, *Nokia* and *Huawei* supply and maintain the mobile infrastructure through which MNOs provide their services.[32]

2.3.1 From national champions to liberalization

Few sectors in the EU have undergone changes as substantial as telecommunication.[33] For much of the 20th century, European telecommunication was characterized by public ownership. In most countries, telecommunications networks were operated by post, telegraph, and telephone administrations and thus a part of the government.[34] These administrations thus acted as both the supplier and regulator of telecom services and held *de facto* monopolies. Telecommunication equipment contracts were similarly awarded in a political manner and in the interest of safeguarding the interest of the 'national champions' in each member state; companies such as *Siemens*, *Nokia* and

[29] (European Commission, 2019)
[30] (van Tetering, 2019)
[31] (Claici, o.a., 2017)
[32] (Eliassen, Mason, & Sjøvaag, 1999)
[33] (Cave, Genakos, & Valletti, 2019)
[34] (Eliassen, Mason, & Sjøvaag, 1999)

Ericsson.[35] At the time, telecom was deemed as being at the core of national autonomy and had thus been excluded from the competition rules under the *Treaty of Rome*.[36]

Starting in 1988, markets were gradually liberalized through a series of legislative packages proposed by the European Commission.[37] This shift in opinion reflected several macro level trends. First, rapid technological advancement in the sector underscored the need for new modes of governance. Countries such as the United States and Japan were becoming increasingly competitive and the European 'national champions' system was hindering European companies from competing on design and innovation. In order to remain competitive, coordination in terms of regulation, research and development was necessary to ensure that Europe would not fall behind. Second, the US themselves had recently liberalized and opened their markets to European firms, which showcased the benefits of liberalization and led to calls of reciprocity.[38] The former national-level regulatory system was thus gradually replaced by a system in which the Commission held a central role, and by 1998 the sector was fully liberalized and much of its regulation harmonized.[39]

European telecom equipment vendors experienced a surge in competition as a result of the new regime. Yet, harmonization of regulation and standards would also result in certain competitive advantages. In 1991, the European Telecommunications Standards Institute (ETSI), a standard-setting body, introduced the Global Standard for Mobile communications (GSM) for 2G to replace the five different standards which had existed prior[40,41]. European firms such Ericsson, Nokia and Alcatel had all participated in defining the standard, and as a result they had been able to secure needed technical capabilities to adhere to it. The GSM would later become the global standard for mobile communications and be used in over 190 countries. Taking part in defining the GSM standard as part of ETSI would thus translate into a significant first-mover advantage for European suppliers. Table 1 illustrates the dominance of European suppliers in GSM markets in 1996. The initial advantage would later put European firms on a positive trajectory in the following years, and European firms would have advantages under the subsequent 3G and 4G standard-setting processes. [42]

[35] (Eliassen, Mason, & Sjøvaag, 1999)
[36] (Eliassen, Mason, & Sjøvaag, 1999)
[37] (Eliassen, Mason, & Sjøvaag, 1999)
[38] (Liikanen, 2001)
[39] (Liikanen, 2001)
[40] (Pawlicki, 2017)
[41] (Drahokoupil, McCaleb, & Szunomár, 2017)
[42] (Pawlicki, 2017)

Table 1. Market share in 33 largest GSM networks in Europe in 1996. [43]

Supplier	Market share base stations (%)	Market share mobile Terminals (global; %)	Rank on total GSM market
Ericsson	37	25	1
Nokia	22	24	2
Siemens	2	9	3
Motorola	13	20	4
Alcatel	10	6	5

The global market for mobile telecom equipment has however undergone considerable changes since then, both in terms of competition and consolidation, and the screws have been tightened on the European giants. The Long-Term Evolution (LTE) – the current standard for 4G networks launched in 2008 – showcases these changed dynamics. By the time that the LTE standard for 4G networks was introduced, new market players had entered the European marketplace[44] – most notably the Chinese firms *Huawei and ZTE* (see subchapter 2.5). These late comers would in the coming years put significant pressure on Ericsson and Nokia. Table 2 illustrates the significant changes in the global market for advanced telecom equipment. Out of all the LTE contracts worldwide, Huawei would close 39 percent of them, more than twice that of Nokia and significantly higher than that of Ericsson. Chinese firms had officially caught up with its European rivals. Having reviewed the European telecom market, attention will now be turned towards the Chinese competition – starting with a brief history of the Chinese growth miracle.

Table 2. 5G contracts, revenue and market prescence of major suppliers.[45]

Supplier	Number of commercial 5G contracts	Market Share (2018)	Revenue 2019 ($USD billion)	Employees	Countries
Huawei	91	29%	122	188.000	170
Ericsson	86	13.1%	23.9	99.417	150
Nokia	63	15.7%	25.9	103.000	130

[43] From (Bekkers, Verspagen, & Smits, 2002)
[44] (Drahokoupil, McCaleb, & Szunomár, 2017)
[45] From (Tirkey, 2020)

2.4 The rise of the Chinese economy and outwards FDI

The economic development of the Chinese economy over the past decades has been extraordinary, with an average growth rate of almost 10 percent annually since the country opened up its economy in 1978.[46] During this time, China has transformed from predominantly being an agrarian society to the economic powerhouse it is today, currently ranked as the second largest economy in the world.[47] China's growing integration into the global economy is also shown in the more active pursuit of memberships in multilateral organizations, with membership in the World Trade Organization in 2001, and increased involvement in activities of the world bank and the international monetary fund.[48] The rise of China as an economic power has changed the dynamics of the global economy, but also the previous power relations in geopolitics.

China's economy was heavily characterized by export-led development and labour-intensive manufacturing in its initial phase, sometimes referred to as the "miracle-growth period",[49] with the export ratio growing steadily from the late 1970's to the early 2000's. The remarkable economic development was also accompanied by large inflows of foreign direct investments, identified as a critical driver behind China's staggering growth rates and the main form through which the economy accessed global capital.[50] This is not least shown when the Chinese economy in 2002 surpassed the US as the largest recipient of FDI in the world.[51] China put forth at the time a myriad of policies so at to attract foreign investors to establish Sino-foreign joint ventures to absorb technology and improve domestic capabilities.[52] The policies worked and attracted European firms such as Alcatel and Siemens.

But while inwards FDI has been a crucial component in the Chinese growth miracle, an increased focus has also been put on outwards FDI starting in the 1990s, making important contributions to the country's continued growth.[53] Some authors have even talked about two *fundamentally different eras* in the Chinese economy, as it has changed from an large recipient of incoming foreign direct investment to an large contributor of outgoing foreign direct investment.[54] The 1990s also saw China's telecommunications industrial policies changed to having an explicit goal of fostering domestic companies

[46] (World Bank, 2020)
[47] (Zheng, 2019)
[48] (Zeng, 2019)
[49] (Naughton, 2019)
[50] (Zheng, 2019)
[51] (Perkowski, 2012)
[52] (Wu, Murmann, Huang, & Guo, 2020)
[53] (Wang, Wen, & Han, 2011)
[54] (Naughton, 2019)

that could compete with the foreign firms both at home and abroad. Ironically, the state led effort to foster 'national champions' would prove to be most successful in the case of the private company Huawei (see subchapter 2.5).

The emergence of outwards Chinese FDI was part of their "Going out" slogan, a term first coined by former president Jiang Zemin in 1997 and later becoming part of China's Five-Year plans, setting the direction for the areas in which the Chinese government wanted their companies to invest. Outwards FDI is a symbol of economic power, and The Going Out policy was indeed a strategy combining the wish to bring economic benefits and continuous growth to China with a geopolitical ambition to regain China's international respect and strengthen their political position. It also led to the internationalization of Huawei in the late 1990s (see subchapter 2.5). Today, the outwards investments by China is also centered around the Belt and Road initiative (BRI), a global development strategy adopted by the Chinese government in 2013 to "improve connectivity and cooperation on a transcontinental scale".[55] Sometimes also referred to as the New Silk Road, it aims to connect China and its economy with other countries along the ancient silk and maritime roads through investments in infrastructure and logistics in Central Asia, Africa and Europe.[56] The Chinese investments in infrastructure projects in Africa in particular have led to headlines and debates about the BRI, as a large proportion of Africa's infrastructure projects are now backed by Chinese funding. *"Right now you could say that any big project in African cities that is higher than three floors or roads that are longer than three kilometers are most likely being built and engineered by the Chinese"*.[57]

Another recent policy behind the increased outwards FDI by China is the "Made in China 2025" objective, launched in 2015 as an industrial policy plan aiming to make the country self-sufficient across several industries by 2025 through a strategy combining government subsidies, national champions and foreign acquisitions. From a non-existent actor 15 years ago, China is now one of the largest FDI senders in the world. These policy and strategy initiatives have also led to an increase of Chinese FDI directed towards Europe. While the US is still the largest direct investor in Europe, the Chinese investments have seen an almost exponential rise over the past decade, and interestingly enough especially since 2008. The increased inflow of Chinese FDI can indeed be connected to the Eurozone crisis, as the supply of European assets for sale was high following the financial crisis, with European policymakers actively trying to attract Chinese investments

[55] (World Bank, 2018)
[56] (OECD, 2018)
[57] (Shepard, 2019)

initially. This coincided with the Chinese demand to gain access to the European market to gain access to technological and managerial know-how, but also to increase brand reputation for Chinese companies and the opportunity to circumvent trade-barriers. The majority of Chinese FDI in Europe has taken the form of mergers and acquisitions, accounting for 97 percent of the value of China's FDI activity in Europe and the US in 2016.

Related to the Chinese strategies of investing in foreign companies with advanced technologies, but also to the overall rise of China as a major geopolitical power with a developed economy and industry, the Chinese government has also actively pursued leadership in tech and artificial intelligence. After previously most being seen as an imitator of Western frontline developments in tech, they are now pushing to become leaders in critical future fields such as blockchain, AI and 5G.[58] In 2017, the government revealed a new three-step plan for AI, aiming to have a world leading industry worth $150 billion by 2030.[59] The strategy is first and foremost challenging the US for world leadership in artificial intelligence, with worries in the US that China will catch up and surpass them in developing frontline technology for both civilian and military use (Foreign Policy). Through a combination of government subsidies, directed support towards national champions - such as Huawei - and foreign acquisitions, China is thus making its mark not only in developing countries but across Europe. For the first time within telecommunications, China is leading rather than playing catch-up.[60] This this has indeed spurred a reaction, which is discussed in subchapter 2.6. As mention, one particular company became a successful product of the expanding Chinese economy and its growth policies.

2.5. Huawei technologies

The rise of Huawei is commonly described as both swift and improbable and mirrors that of China more generally.[61] Over the last thirty years, the Chinese firm has transformed from a small, domestic producer to become the largest telecommunication equipment vendor in the world. In 2018, the firm made global sales of over USD 100 billion, with operations in more 170 countries and around 180 000 employees, out of which roughly half are focused on research and development[62]. According to Huawei themselves, the

[58] (Karpal, 2019)
[59] (Kharpal, 2017)
[60] (Woyke, 2018)
[61] (Johnson & Groll, 2019)
[62] (Huawei, 2020)

firm provide telecom equipment to 37 of the top 50 largest mobile operators globally.[63] Similarly, about half of the 4G equipment on the European market is provided by Huawei. As such, Huawei has surpassed Swedish Ericsson and Finnish Nokia to become the largest telecom equipment vendor in the world. Considering this rapid rise to a global leadership position, the story of the rise of Huawei is indicative of that of China more broadly. This story will be described chronological below, outlining the rise of Huawei from its founding in the late nineteen-eighties to more recently becoming the largest telecom supplier, one of the most contested firms in the 21st century and the centre of controversy in the 5G debate.

Huawei was founded in 1988 by Ren Zhengfei, an ex-deputy director with the *People's Liberation Army's* (PLA) engineering corps, at a time when the Chinese telecom sector was significantly underdeveloped[64] and made up of state-owned local enterprises. At the time of Huawei's founding, China was completely reliant imports for its procurement of telecom equipment and most of the major telecom vendors at the time – such as Alcatel, Nokia, Ericsson and Motorola – had a presence in the country.[65] For the first few years of its operations, Huawei's business primarily consisted of reselling imported telecom equipment while simultaneously trying to reverse engineer the different imported components. Alongside significant investments in research and development, this helped in developing its own manufacturing capabilities. By the year 1990, Huawei had begun its own commercialization of telecom components and rapidly became the *avantgarde* out of some 200 domestic firms which had employed the same strategy. What differed Huawei from its domestic competitors was that it fervently abstained from establishing international joint ventures with foreign firms and rather developed its technologies in-house. This was in contrast both with Huawei's competitors and the industrial policy of China, encouraging firms to establish joint ventures to gain access to foreign technologies. Rather, Huawei believed that it would be better served and less dependent if it performed its own operation.[66]

By the mid-1990s, Chinese leadership started taking notice of Huawei when the firm won its first major contract to supply a telecommunications network to the PLA, which was later to be described as *"small in terms of our overall business, but large in terms of our relationships"* (Gilley, 2000). What exactly led Huawei to win the contract over local up-and-coming suppliers like the state-owned enterprise Zhongxing Telecom has been a

[63] (Drahokoupil, McCaleb, & Szunomár, 2017)
[64] (Peppermans, 2016)
[65] (Gilley, 2000)
[66] (Wu, Murmann, Huang, & Guo, 2020)

topic of discussion. Zhengfei would later in a conversation with Jiang Zemin, the Chinese president and secretary general of the Communist party at the time suggest that: *"[telecommunication equipment] was related to international security and a nation that did not have its own [production] was like one that lacked its own military*".[67] According to accounts, Secretary Zemin concurred.

As mentioned in the previous subchapter, the Chinese government began to explicitly support its telecom industry by means of industrial policy in 1996, effectively touting Huawei as a 'national champion'[68]. The Shenzhen government, along with the state-owned Shenzhen Development Bank and China Construction Bank declared the Huawei to be a *"key development project*". Subsequently, the banks would support the firm with financial resources, as well as extending credits to buyers of its products.[69] Huawei's chief executives themselves have previously acknowledged the need for government protection policy, '*Huawei was not prepared for such an intensified competition when the company was just established'*[70] *"The rivals were internationally renowned companies with assets valued at tens of billions of dollars. If there had been no government policy to protect [nationally owned companies], Huawei would no longer exist."*[71] The firm would continue to snare network contracts and now turned its attention to foreign markets.

2.5.1 Huawei in Europe

By the early 2000s Huawei had become the undisputed market leader in China and set its target on the European markets. The firm would first establish operations by opening a research facility in Kista, Sweden - the backyard of the Swedish telecom giant Ericsson. In quick succession, Huawei would then enter several Eastern European markets, including Romania, Hungary, the Czech Republic and Poland.[72] The market strategy was rather simple: pursue price leadership and long-term relations with cash-strapped mobile network operators through the provision of credit and favourable payment conditions.[73] Being able to provide these types of terms played a significant role for example in Huawei's expansion in Poland, where network operators did not pay until several years after the projects were completed. The firm's price leadership was significant in the early years, offering equipment similar to that of Ericsson and Nokia at about 30 per cent lower prices.[74] Huawei was now gaining ground rapidly and started winning major contracts

[67] (Gilley, 2000)
[68] (Gilley, 2000)
[69] (Gilley, 2000)
[70] (Fan, 2006)
[71] (Fan, 2006)
[72] (Pawlicki, 2017)
[73] (Pawlicki, 2017)
[74] (Pawlicki, 2017)

across Europe with large mobile operators such as *British Telecom* and the Dutch operator *Telfort*. By 2004 was Huawei involved in 14 of the 19 3G networks that were build out globally[75], and by 2007 the firm had secured contracts with all major network operators in Europe.[76]

The true wake-up call for Europe came in 2009 however, when the Swedish-Finnish multinational mobile network operator *TeliaSonera* chose Huawei for the buildout of one of the world's first 4G networks in Norway.[77] This was an unexpected choice coming from the firm which was owned by the host countries of Europe's two telecom giants. Not only did Huawei complete what was then one of the most advanced networks ahead of schedule – they also did so under budget.[78] All of this had seemed extremely unlikely ten years ago, arguably being a latecomer into a highly consolidated industry. Yet Huawei had come of age and was now a force to be reckoned with – being highly competitive not only in terms of price but also in terms of quality. By the year 2010, Huawei has increased its sales in Europe by over USD 3 billion, which was a 17 percent increase from the year prior[79]. While Huawei had arguably been a controversial topic ever since first coming to Europe in 2000, the above developments would by the mid-2000s reach its culmination. In the United States, where Huawei entered around the same time as Europe, lawmakers prohibited the firm from bidding in multiple telecom network projects citing *"national security concerns"*.[80]

Chinese policymakers and company officials denied the accusations however that they were 'dumping' the firm's products on European markets. "We are not winning business on price anymore", said a Huawei chief executive. The investigation was later dropped after Beijing and Brussels came to an agreement which *inter alia* included China taking measures to facilitate Ericsson and Nokia in achieving a greater market share in China. That would however not succeed, as Ericsson saw its market share in China fall from around 26 per cent to around 7 percent over the course of 2011 to 2016. Huawei's market share in Europe, however, rose from 2,5 percent in 2006 to 25 percent in 2014.[81]

[75] (Ahrens, 2013)
[76] (Drahokoupil, McCaleb, & Szunomár, 2017)
[77] (Telia, 2010)
[78] (Johnson & Groll, 2019)
[79] (Peppermans, 2016)
[80] (Rogers & Ruppersberger, 2012)
[81] (Peppermans, 2016)

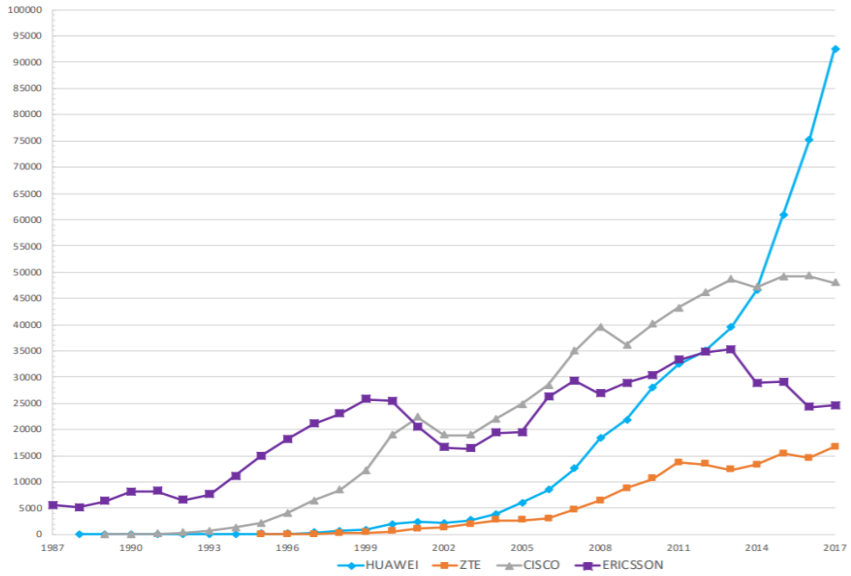


Figure 1. Huawei, ZTE, Cisco and Ericsson sales in $USD million.[82]

2.5.2 Huawei and Chinese espionage

One of the most insistent associations of Huawei has been that of cyber espionage**.** Ever since its founding, suggested government ties and linkages to the PLA have been a major point of concerns – especially in the US. While officials in Australia and New Zealand have also raised concerns, the accusations and mistrust campaign towards Huawei has primarily been an American endeavour.[83] The source of arguably most negative sentiments toward the firm came with a 2012 US House Intelligence Committee[84] report which suggested Huawei was a threat to *national security* due to, among other things, cyber espionage. For example, the report stated that it had obtained documents from former Huawei employees which suggested that the firm supplied services to a 'cyber warfare unit' of the PLA. This evidence was never made public, however.[85]

The concerns of espionage define the debate about Huawei just as much now as it did eight years ago. As seen from the responses by both US and European technology companies, mobile network operators and officials - while being ostensibly unanimous in that there is a need to exercise caution - not everyone agrees with the opinion of US officials. In a Bloomberg interview with Microsoft's president Brad Smith, when asked about Huawei's situation in the US, he suggests that US lawmakers have been vague as to

[82] From (Wu, Murmann, Huang, & Guo, 2020)
[83] (Neate, 2019)
[84] (Rogers & Ruppersberger, 2012)
[85] (Bryan-Low, Packham, Lague, Stecklow, & Stubbs, 2019)

explaining the threat of Huawei. "*Oftentimes, what we get in response is, 'Well, if you knew what we knew, you would agree with us'",* Smith explained. *"And our answer is, 'Great, show us what you know so we can decide for ourselves'.*[86] Similar positions have come from European officials as well, such as Germany's Federal Office for Information Security, which suggested that if in fact the US had concrete it ought to share it. If that had been the case, then Germany said it would potentially reconsider its position.[87]

In addition, Chinese cybersecurity law enacted in 2017 fuels the concerns of how the Chinese government could use domestic companies for espionage. The law states that Chinese companies need to provide the government with information needed for national security interests, and have made foreign governments worried about their data privacy.[88] Concerns regarding cyber espionage thus underpin a significant part of the debate regarding Huawei, much due to the ostensibly clear links to the Chinese government and the People's Liberation Army. While ever present, concerns and debates were arguably exacerbated in January of 2019 when a Polish sales director for Huawei was arrested by Polish authorities suspected of espionage.[89] While it seems impossible to gauge the threat of cyber espionage, it has in any case been conflated with the debate of Huawei and thus underpins many of the discussions which will be outlined in this thesis.

2.6 FDI in the EU: A change in stance

While European countries overall have welcomed the Chinese investments historically, and at points even actively promoted these activities, recent years have seen the tide change.[90] To fully understand the EU view on Chinese investments in general - and Huawei's increased presence in particular - it is useful to also understand the economic and political context in Europe regarding foreign investments. Unlike trade policy, FDI policy has historically been governed nationally in EU countries with member states striking their own bilateral trade deals with third countries.[91] This changed with the Lisbon treaty in 2009, where exclusive competence for FDI to the EU was transferred to the union. In principle, this means that the Commission is now responsible for negotiating new bilateral investment agreements with third countries and regulating inbound FDI from foreign countries.[92] Just like trade, the EU will speak with one voice on FDI policy. Working this large transfer of competence out in practice has been a slow process however, partly

[86] (Bass, 2019)
[87] (Spiegel, 2018)
[88] (Rühlig & Björk, 2020)
[89] (Plucinska, Qing, Ptak, & Stecklow, 2019)
[90] (European Commission, 2019)
[91] (Meuniér, 2014)
[92] (Meuniér, 2014)

due to a low support of the radical shift from member states,[93] and the difference between EU countries on how much foreign investments they have allowed previously is an important factors in the Huawei case, as will be seen later in this paper.

In examining EU's stance on Chinese investments, it is also useful to understand how the financial crisis in 2008-2009 affected the Union and its member states. Both public and private assets became available in the wake of the Eurozone crisis, with few European buyers ready to invest at the time. European policymakers saw Chinese investments as beneficial in both long- and short term, and therefore started to proactively attract Chinese investments through promotion efforts and incentives. Short term, these investments were a solution to save European companies from bankruptcy, preserve jobs and increase state financials through privatization programs, whereas the long term gains focused on potential access to the coveted Chinese market.[94] Chinese investments were welcomed both on regional, national and EU-level, not least shown at the 2015 High-level Economic and Trade Dialogue where China committed to contributing to a €315 billion investment plan for Europe set up by then president of the EU Commission Juncker.[95]

The result of the convenient match between the European supply of assets and Chinese pursuit of investments in Europe led to a large increase of FDI from China in countries such as Portugal, Ireland, Italy, Greece, Spain and Cyprus, all severely hit by the Eurozone crisis. But Chinese investments have also focused on "core member states" Germany, France and the United Kingdom, with the value of FDI from China increasing tenfold in Germany between 2015 and 2016. The UK and Germany accounted for 46% of Chinese investments in Europa in 2016.[96] Although European assets were available in quantities after the Eurozone crisis, it should be noted that Chinese acquisitions still came as a result of public battles where the Chinese investors ended up paying a premium over other interested parties in a bidding process.[97] The fact many European countries already have a substantial level of Chinese investment, especially following the financial crisis, is an interesting factor in explaining the dynamics of the Huawei debate in Europe. With that said, the "open arms" welcoming foreign investment that could be observed after the financial crisis did not last forever.

[93] (Meuniér, 2014)
[94] (Meuniér, 2019)
[95] (Tzogopoulos, 2016)
[96] (Meuniér, 2019)
[97] (Meuniér, 2019)

A combination of factors has however led to a changing stance among the EU member states and their perception of Chinese investments in Europe in recent years, some of them connected to the overall populistic turn in European politics, with a general scepticism about globalization and investments from foreign countries. As the underlying reasons behind EU's policy towards Chinese investments and the change in perception of these will be the main topic of this paper, we will leave the analysis of this for later. It should however be mentioned that other factors contributing to a changed stance in the EU member states includes concerns about the Chinese companies' ties to the government, the technological transfer from European companies and the lack of reciprocity for EU investments in China, but also geopolitical concerns of China as a rising superpower. National security concerns have been another frequently mentioned risk with the Chinese investments, especially when the investments regarded European infrastructure. The above-mentioned points were part of the background of the development of an EU screening mechanism for foreign investments into the union.[98]

The proposal to create an EU-wide framework for the screening of FDI into the Union was first presented by EU Commission President Juncker in his 2017 State of the Unions address, and is widely believed to have been prompted by the increased Chinese presence in the EU[99] - especially in critical infrastructure sectors. The proposal has been criticised and controversial through the whole drafting process, but was finally adopted by the European Parliament and by the Council on 19 March 2019 after 17 months of deliberations.[100] The framework will among other things create a cooperation mechanism where Member States and the EU Commission can exchange information and raise concerns related to specific investments, set certain requirements for Member States who wants to adapt (or already has) a screening mechanism on national level, and allow the Commission to issue opinions when an investment poses a threat to the security or public order of more than one members state.[101] With this in mind, it is not difficult to understand the long process of getting the proposal accepted, as it gives other member states and the Commission more to say in individual states' FDI decisions. The member states and the EU Commission will use 18 months from the adoption of the proposal to take the necessary steps to make sure the EU can fully apply the Investment Screening Regulation by 11 October 2020.

[98] (Lehne, 2020)
[99] (BBC, 2019)
[100] (Stearns, 2019)
[101] (European Commission, 2019)

> "*This new framework will help Europe defend its strategic interests. We need scrutiny over purchases by foreign companies that target Europe's strategic assets. I want Europe to remain open for business, but I have said time and again that we are not naïve free traders."*
>
> - Jean-Claude Juncker, September 2017[102]

2.7 Chapter conclusion

Having provided an extensive background and historical context for the Huawei debate, it is useful to briefly stop and consider how an understanding of the previous chapter will be useful in the subsequent analysis of this paper, but also to briefly discuss how a section on previous literature can be approached in a grounded theory research design. First of all, it can now be concluded that the background chapter has provided the reader with an insight into (1) The technical aspects of telecom networks; (2) The characteristics of the telecom market in the European Union; (3) A brief background on the Chinese economy and its investment activities; (4) An outline of Huawei's rise to its current position, including reports of government ties; and (5) The investment climate in the EU and its stance on Chinese investment, particularly in the context of the financial crisis.

All of these elements are important to understand the complexity and context of the current Huawei debate, and will be referenced frequently throughout the subsequent parts of this thesis. As this thesis aims to add nuance to the discussion on Chinese investments in critical infrastructure in the European Union, stepping away from what seems to be an overly simplified and binary debate, it would simply not be sufficient to approach the issue with *one* of the above perspectives. To fully understand the complexity and considerations of all the stakeholders in the debate, transcending fields of technology, business, politics and international relations, the broad background is therefore a key part of this paper. Leaving out one of the above perspectives would lead to the risk of missing important aspects, direct or indirect, in the later analysis.

[102] (European Commission, 2019)

3. METHODOLOGY

3.1 Reader's guide

The following chapter discusses the methodology and research design of this paper. The first discusses the relevant epistemological and ontological considerations of this paper. The subsequent chapters then outline the grounded theory methodology used in this paper, with relevant matters of data collection, coding category development discussed throughout [103]

3.2 Research philosophy

Before going over the methodological considerations of this research, it is useful to discuss the epistemological and ontological underpinnings of this thesis and their implications. *Ontology*, defined as the study of being, concerns the questions of what entities that exists and what the world really is made of, while *epistemology* is the study of "what knowledge is" and what it means to know something. Ontological and epistemological issues tend to emerge together, and writers in the research literature sometimes struggle to keep the two terms apart conceptually.[104] Following the reasoning of Crotty (1998), the term *ontology* is reserved for the occasions when we need to talk about "being", and put more in-depth focus on the actions and consequences in the relation between the subject and object, instead of focusing on the ontological question of whether a *"real world"* exists outside the human consciousness.[105] That said, and acknowledging that the realism embraced by objectivism and the subjectivism's close relation to nominalism are the extremes on a continua, this paper builds on an understanding of issues as constructed in social interaction where actors create partially shared meanings and realities.

Some authors argue that the ontological and epistemological stands taken by the researchers are unchangeable, while others rather view it as jackets, which can be taken on and off – thereby saying that there can be different types of knowledge and that it can be accessed in different ways.[106] The two traditions are ideal types, and researchers might consequently not feel comfortable in either camp. They should therefore rather be thought of as extremes on a continuum, where researchers might find their place

[103] (Moses & Knutsen, 2012)
[104] (Crotty, 1998)
[105] (Crotty, 1998)
[106] (Moses & Knutsen, 2012)

somewhere in between.[107] A distinction between *naturalism* and *constructivism* is often made, where the naturalistic or positivistic tradition assumes that there is a real world independent of our existence. Furthermore, it emphasizes how certain knowledge can be attained through discovering and revealing the patterns through thinking, observing and recording experiences meticulously, and that they can be described in a clear, correct and objective manner.[108] The epistemology of this thesis, *constructivism*, rejects the objectivist view of human knowledge and the notion of an objective truth waiting to be discovered. Instead, truth or meaning comes into existence "in and out of our engagement with the world"[109] or, as stated by Crotty; *"meaning is not discovered but constructed"*. Constructivists are less interested in the common structure of explanation as they are in mapping the different forms of explanation, and the origin in the variance. Constructivism is also the perhaps most frequently invoked epistemology in qualitative research designs.[110]

Given that the aim of this thesis is to understand the debate and the risks associated with Huawei debate to provide the EU with 5G infrastructure, the constructivist understanding of how different actors can construct meaning in different ways, even though they are observing the same phenomenon, is central. It is essential in studying the European Union and its member states approach to Huawei, as the risks associated with the Chinese vendor are viewed and perceived differently depending on the actor observing them. The meaning of the risks is constructed by the individual actors and deemed a main explanation as to why the different member states and actors differ in their policies and stances on Huawei. From a constructivist viewpoint, meaning and by extension *truth* can therefore neither be described simply as "objective" or "subjective". Truth is constructed in the interaction with the world and the objects in it.[111] Or, as put by Crotty; *"Because the essential relationship that human experience bears to its object, no object can be adequately described in isolation from the conscious being experiencing it, nor can any experience be adequately described in isolation from its objects"*.

[107] (Moses & Knutsen, 2012)
[108] (Crotty, 1998)
[109] (Crotty, 1998)
[110] (Crotty, 1998)
[111] (Crotty, 1998)

3.3 Research strategy

Having discussed matters of ontology and epistemology, this chapter outlines the research strategy of this thesis – the way which it acquires knowledge and through what methods. [112] This thesis employs a grounded theory methodology as to explore the perceived risks inherent in the Huawei debate in the European Union. This choice can largely be explained by two factors; (I) As explained in more detail in subchapter 3.4, the previous applicable theoretical literature on the topic is scarce (see subchapter 3.4) partly due to the fact that the issue has appeared during the last eighteen months and is relatively unstudied, and can therefore be argued to not sufficiently capture the *prima facie* dynamics of the debate; (II) Following the previous point, hypothetical-deductive or similar approaches could prove inadvisable in this research setting, as they would most likely limit the scope and thus the analytic insight of the research.. Grounded theory, an approach characterized by the construction of theory through methodical gathering of data, is thereby a natural starting point.

Grounded theory encourages researchers to constantly interact with their data. Accordingly, at the core of the method is the iterative process of moving back and forth between empirical data and emerging analysis, continuously making the collected data more focused and the analysis successively more theoretical.[113,114] What is advocated is therefore a development of theories and concepts rather than deducing testable hypotheses from existing theory[115]. This is thus in stark contrast to hypothetic-deductive approaches of research. Grounded theory therefore entails a systematic qualitative analysis to generate new theories, making is particularly suitable when little is known about a topic or a subject is relatively unstudied,[116] an important aspect in choosing the appropriate research method for the topic of this paper.

There are a number of principles which defines the grounded theory approach that are still useful in understanding the method, such as *(1) simultaneous involvement in data collection and analysis*, *(2) constructing analytic codes and categories from data*, not from preconceived logically deduced hypotheses and *(3)* using the *constant comparative method*, which involves making comparisons during each stage of the analysis. Other characteristics include *(4) advancing theory development during each step of data collection and analysis* and *(5) memo-writing* to elaborate categories, specify their

[112] (Moses & Knutsen, 2012)
[113] (Bryant & Charmaz, 2010)
[114] (Glaser & Strauss, 1967)
[115] (Charmaz, 2006)
[116] (Tie, Birks, & Francis, 2019)

properties, define relationships between categories, and identify gaps. These principles have been adapted also in this research, and the simultaneous collection of data on and analysis of the Huawei case has been key in developing the theoretical concepts of this paper.[117]

Since the early work of Glaser and Strauss, an extensive literature has developed the theory further and discussed its applications on research designs. While central components such as the simultaneous data collection and analysis stand as a constant characteristic and is an important part of this paper, Glaser and Strauss invited their readers to use Grounded theory methods flexibly and in their own way already in their original publication from 1967. This view, combined with the words of Charmaz (2006) seeing grounded theory methods *"as a set of principles and practices, not as prescriptions or packages. …I emphasize flexible guidelines, not methodological rules, recipes, and requirements. Grounded theory serves to learn about the worlds we study and a method for developing theories to understand them"*[118] will guide the methodological considerations of this paper. The rest of this chapter will go through the steps of grounded theory in consecutive order to explain each part of the process in more detail.

3.3.1 Data collection

While this thesis concurs with the common grounded theory dictum 'all is data'[119], the quality and the selection of data are naturally a matter of great importance. Researchers commonly use a variety of methods in their data collection, ranging from fieldnotes and interviews to textual analysis of reports and government documents. For this paper, textual analysis of expert reports, policy documents, articles, EU publications and journals have been the main sources of data. An advantage of the grounded theory method compared its quantitative counterparts is the ability to add new pieces of data to the research at any time during the process - even in late stages of the analysis – providing flexibility and an opportunity to pursue new leads that emerge throughout the research process.[120]

A central part in grounded theory is to analyse data with an open mind and, to the largest extent possible, without preconceived beliefs about the research topic. With that said, most students and academics already have a solid foundation of knowledge in the chosen academic area of study that can serve both as an advantage and as a liability. Pre-existing

[117] (Charmaz, 2006)
[118] (Charmaz, 2006)
[119] (Glaser, 2002) in (Charmaz, 2006)
[120] (Bryant & Charmaz, 2010)

assumptions and perspectives can be a useful guideline in the data collection and initial analysis but should not lead to researchers ignoring aspects which conflict with earlier perceptions. The notion of *sensitizing concepts*[121] can serve as a guideline here, stating that grounded theorists often begin their studies with guiding interests and general concepts, providing a loose frame to those interests. Put differently, sensitizing concepts provide a place to *start*, not an *end*[122] and can be very useful in the initial development of concepts if they are not forced upon the data. By incorporating the words and thoughts of the subjects under study, in this case the stakeholders in the Huawei debate, sensitizing concepts can be used to explain how they perceive and explain their world. [123]

This is also in line with the practice of *purposive sampling*, where researchers initially select data sources purposely to find answers to the research question. The initial data is thereafter analysed and coded before further data collection is carried out.[124] Purposive sampling is a strategy used in this paper as the researchers already have a relatively comprehensive overview of the literature at hand. As will be seen later in the thesis, the purposive sampling enables the researches to present a chapter with preliminary finding, chapter 4, which thereafter will guide the subsequent analysis. While remaining open to the data and by dispensing concepts that prove to be irrelevant, the prior knowledge of the researchers will be an advantage in the data collection and analysis. As an additional safeguard, several guiding questions to avoid preconceptions in the data has been included in the coding template for the data analysis. The coding template can be found in Appendix 2 and a more comprehensive discussion on preconception in the context of this thesis can be found in subchapters 3.3.34 and 7.3.2.

While all qualitative research includes some type of textual analysis, a clear distinction can be made between *elicited text*, where the researchers have been part of shaping the content, and *extant texts*, consisting of varied documents that the researcher had no hand in shaping. This paper will exclusively focus on the latter, usually including public records, government reports, organizational documents, media coverages and other literature. The fact that extant texts differ from elicited text in that the researcher does not affect their construction poses challenges in the interpretation and analysis of the data, as both the researchers and readers may believe that the data is a reflection of reality and an objective truth. It should therefore be noted that all authors of extant texts have a specific purpose in mind when publishing their respective content, and they do so in social, economic,

[121] (van den Hoonaard, 2012)
[122] (Charmaz, 2006)
[123] (van den Hoonaard, 2012)
[124] (Tie, Birks, & Francis, 2019)

historical, cultural and situational contexts. Although the authors of such publications may themselves assume their texts are reflecting objective facts, researchers should always be aware of the risks associated with treating them as such. Differently put, attention must not only be given to the data itself, but also its origin, the actors involved in shaping them as well as their intention.

Just as in any research design, sufficient data is important to give a full and nuanced picture of the issue at hand, providing a strong foundation for the analysis. As put by Charmaz, "A novice may mistake good, but limited, data for an adequate study".[125] To address any concerns about insufficient data, we let the following questions by Charmaz guide us in our data collection:

1. *Have I collected enough background data about persons, processes, and settings to have ready recall and to understand and portray the full range of contexts of the study?*
2. *Have I gained detailed descriptions of a range of participants' views and actions?*
3. *Do the data reveal what lies beneath the surface?*
4. *Have I gained multiple views of the participants' range of actions?*
5. *Have I gathered data that enable me to develop analytic categories?*

Although the sample size in a grounded theory study needs to be large enough to be representative, there is no intrinsic value in collecting more data than necessary - it may even be counterproductive. With excessive data, large files tend to get unanalysed and researchers may lose important processes in their area of study if the sheer volume of data gets overwhelming.[126] Another guideline for determining the right amount of data comes from Charmaz; " *Most methodology authors advise learners that saturation is reached when the learner hears nothing new. When analysing texts, there is always a risk of not paying enough attention to the context. A strategy to better understand the context is to use several sources and multiply types of document types".*[127] This purposeful sample is indeed using a variety of sources, all complied in the table below:

[125] (Charmaz, 2006)
[126] (Glaser, 1998 in Bryant & Charmaz, 2010)
[127] (Charmaz, 2006)

Table 3. Overview of texts included in the purposive sample.

Author	Title	Year	Type	No. of Pages
Stiftung Neue Verantwortung	*5G s. National Security – A European Perspective*	2019	Report	19
European Parliamentary Research Service	*5G in the EU and Chinese Telecom Suppliers*	2019	EU Document	2
The Kosciuszko Institute	*The future of 5G or Qou Vadis, Europe?*	2019	Report	13
European Union Agency for Cybersecurity	*Threat Landscape for 5G Networks*	2019	EU document	78
Stiftung Neue Verantwortung	*Whom to trust in a 5G World*	2019	Report	23
Swedish Institute of International Affairs	*What to Make of the Huawei Debate?*	2020	Report	30
NIS Cooperation Group	*EU coordinated risk assessment of 5G*	2019	EU document	33
Eurasia Group	*The Geopolitics of 5G*	2018	Report	18

3.3.2 Coding and memos

In the data collection, researchers at some point need to stop and ask analytical questions about the data to further the understanding of the studied issue. This process is called *coding*, a core process in classical grounded theory methodology where the conceptual abstraction of data and its reintegration as theory takes place (Holton). In essence, coding is the process of naming segments of data with a label that *"simultaneously categorizes, summarizes, and accounts for each piece of data"*, and is the first step towards an analytic interpretation of the dataset.[128] When researchers find concepts or elements that are repeatedly occurring or of certain significance, these pieces of data are tagged with codes. As more data is collected and reviewed, these codes can be grouped into concepts, and then categories - which in turn lay the basis for a new theory. Put differently, *"coding is the pivotal link between collecting data and developing an emergent theory to explain these data. Through coding, you define what is happening in the data and begin to grapple with what it means"*.[129]

[128] (Charmaz, 2006)

[129] (Charmaz, 2006)

The goal of the coding process is to constantly compare the data to reach *theoretical saturation*, a stage in the process that has led to an *interchangeability of indicators* where no new meanings or dimensions can be found in the data (Holton). The coding process in usually entails at least two stages, *(I) an initial phase* involving thorough examination of the texts with an open mindset to provide initial codes that can later be pursued in future data collection, and *(II) a focused, selective phase* where the most significant or prominent data is pinpointed in order to develop categories. The coding of data is a way to understand what's happening in our data and make sense of it,[130] or as stated by Holton[131], *"coding gives the researcher a condensed, abstract view with scope and dimension that encompasses otherwise seemingly disparate phenomena."*

The coding process should however be adapted to the task and data, and while keeping an open mind is important in developing new insights, coding is partly play and a way to engage with the data to gain deeper understanding.[132] Coding the data is followed by categorization, allowing researchers to conceptualize key analytic features of the data and communicate a meaningful picture of these.[133] The process from initial coding to categories can broadly be described in the picture below, and the template guiding our coding process can, as previously stated, be found in Appendix X, including guiding questions to avoid preconceptions. The researchers found that a certain degree of saturation in the collection of data occurred already after the purposive sampling, as the coding largely points to similar factors explaining the Huawei debate as put by experts and stakeholders. This enables the creation of risk categories that guided the subsequent analysis.

Another part of a grounded theory process is *memo-writing*, a pivotal intermediate step between the collection of data and the first drafts of a paper[134] and the methodological link through which the researcher transforms data into theory.[135] The continuous writing of memos throughout the research process lets the researcher explore, but also theorize, emergent patterns while simultaneously increasing the level of abstraction. The ideas formulated in the memos will ultimately be what the researcher shares in the finalized product.[136] Putting ideas on paper is also a way of getting new insights and developing categories for your data.[137] Memo writing will be used in this research to link the coding

[130] (Charmaz, 2006)
[131] (Holton, 2010)
[132] (Charmaz, 2006)
[133] (Dey, 2010)
[134] (Charmaz, 2006)
[135] (Lempert, 2010)
[136] (Lempert, 2010)
[137] (Charmaz, 2006)

to the analysis writing process and serves as a middle step in the analysis of the data and the final writing of the thesis.

3.4 Previous literature and grounded theory

While an extensive background is useful to set the scene for the discussion, the inclusion of a chapter on previous literature requires some more consideration - especially with the grounded theory approach chosen for this paper. As the grounded theory method in many ways builds on the researcher's ability to approach the data with an "open mind", the appropriate approach to a traditional literature review has long been a debate among scholars.[138] Researchers have repeatedly questioned the utilization of existing literature within the research study and in their original publication *The Discovery of Grounded Theory*, Glaser and Strauss, the founders of grounded theory, encouraged researchers to delay their literature review until after the analysis to avoid preconceptions.[139] This view is however contested, and contemporary research is somewhat divided between scholars promoting an approach where researchers should enter the field without formal review of previous literature and others noting the importance of understanding the discourse surrounding their topic.[140]

Acknowledging this divide, and given that this research employs a constructivist grounded theory approach where the resulting theory "*depends on the researcher's view; it does not and cannot stand outside of it*", this paper has not engaged in an extensive and formal literature review before the data collection process. But this also comes from the characteristics of the Huawei debate. As the discussion on Huawei and European 5G implementation has largely emerged during the past twelve months, it became evident early on in the research process that few academic articles have been written to address the issue. Therefore, one must look to related fields such as literature on *critical infrastructure*, *political risk* and *investment theory* to find a theoretical base for the discussion.

As the literature on *political risk* centres around how the government and political environment in a country affects business activities,[141] it could be a natural starting point in analysing foreign investments in infrastructure – especially when a large portion of the concern around these investments are based on distrust in the host country's government. Some scholars even *define* political risk as "unwanted government

[138] (Ramalho, Adams, Huggards, & Hoare, 2015)
[139] (Glaser & Strauss, 1967)
[140] (Ramalho, Adams, Huggards, & Hoare, 2015)
[141] (Matthee, 2011)

interference with business operations",[142] which is a core issue in the debate about Huawei and investments in critical infrastructure. Unfortunately, however, a brief overview of the previous literature on political risk shows that the theories cannot seamlessly be applied to the case of Huawei and 5G investments in Europe. Historically, this body of literature concerns how governments or companies can assess the host country environment to make a decision on whether to invest or not. This is not the case of the Huawei debate, as the EU rather is concerned with a risk assessment of the investing party and its home government - in many ways an unprecedented situation.

Information security and critical information infrastructure protection studies commonly discuss proactive and reactive security measures towards external threats[143] yet seldomly considers those from actors in a buyer-vendor relationship. The literature therefore has less to say when it is a supplier that represents a risk, leaving much of the literature mute.[144] Approaching the Huawei debate solely based on these literatures would thus make it difficult to capture actor dynamics and the various political aspects of the issue. A similar observation as in the case of political risk can be made for the literature on international business. While the literature on investment decisions and FDI truly is extensive, the situation where a developing country is investing in a developed region (or in this case, Union) is somewhat unstudied - largely due to the fact that it has not been observed before.

As the above bodies of literature seem to not sufficiently address the debate surrounding Huawei and 5G implementation - partly due to the nature of the issue – a traditional previous literature section will not be provided. At the same time, previous theoretical arguments and expert texts are part of the data sample of this paper, allowing the researchers to draw on it in whenever necessary in the subsequent analysis. This is done to provide the most complete account of the Huawei debate possible, leaving no stone unturned. As the proverb goes, *"a dwarf standing on the shoulders of a giant may see farther than the giant himself"*[145]

3.5 The iterative research process

As a final note of the chapter on methodology and research design, it is useful to briefly mention how the analytical part of this thesis is structured as a reflection of the research process. As previously mentioned, grounded theory is characterized by its iterative

[142] (Sottilotta, 2013)
[143] (Giannopoulos, Filippini, & Schimmer, 2012)
[144] (Lysne, 2018)
[145] (Burton, 1932)

process, moving back and forth between analysis and data.[146] This allows the researchers to continuously develop new categories, and in the case of this thesis, get closer to the formation of a framework. The iterative process will be evident in the subsequent two chapters, as they reflect how the understanding of the issue is gradually increasing. By first coding the purposive sample of data, a number of preliminary findings become evident – which in turn allows the initial forming of categories. These categories will thereafter be a starting point in the continued collection of data and further analysis of the literature. Chapter 5 is therefore representative of a second phase in the analysis process.

The data from the purposive sample will be used throughout all stages of the analysis but will also be complemented by additional data collection when needed. The new data collected will often be the result of the researchers looking to increase understanding of specific tracks or specific aspects of the debate that is coded in the earlier data collection. While some of the key findings of this thesis appears early in the research process, others may well be final pieces of the puzzle. This is also indicative of the increased knowledge that will be obtained from the research, as some of the more fundamental aspects of the Huawei debate become evident when the researchers are able to see new nuances of the debate and have a better overview of the issue. With that said, the reader is hereafter encouraged to explore the topic of this thesis in parallel with the researchers, gradually increasing the level of abstraction as new findings and themes emerge in the data collection. Or as put by Charmaz;

> *"At each phase of the research journey, your readings of your work guide your next moves. This combination of involvement and interpretation leads you to the next step."*[147]

[146] (Bryant & Charmaz, 2010)

[147] (Charmaz, 2006)

4. PRELIMINARY FINDINGS

4.1 Reader's guide

This chapter provides an overview of the preliminary findings from the purposive sample. The first part of this chapter outlines the premises, recurring themes and main arguments identified in the debate by a variety of actors. The themes are presented to provide the reader with a foundational understanding of the nuances and rationales of the discussion that will later be examined in more detail in the analysis. The preliminary findings is an important step in the process of coding and making sense of the data, and an illustration of the process can be found in Appendix 2. The purposive sample enables the formation of a first set of categories that emerges as key themes in the coding, and these categories - later also referred to as *risks* - will be presented in the second part of the chapter. Forming categories after an initial round of coding is done in accordance with the grounded theory approach and the initial categories will be guiding the subsequent analysis of this paper.

4.2 Key themes

As a starting point, it is useful to briefly set the scene for the analysis by highlighting key themes from the debate and provide answers to some of the 'big questions' of 5G, as understood by policymakers, experts and other stakeholders. What is immediately apparent is the sense of urgency and immediate concern. The reason why discussions regarding foreign presence in telecommunication networks is happening *now*, despite the fact that Chinese vendors have provided ICT technology in Europe for decades, is primarily explained by the transformative aspects of 5G (see background chapter 2.2 and subchapter 2.2.1) which contrasts to the implementation of prior generations of mobile networks and telecom technology.[148,149] This has in turn led to concerns over European reliance on Chinese technology, particularly that provided by Huawei, and a constant phrasing of the arguments in the debate behind not granting Huawei access to European markets as concerns over *"national security"*.[150]

[148] (Albrycht & Świątkowska, 2019)
[149] (Triolo, Allison, & Brown, 2018)
[150] (Kleinhans, 2019)

4.2.1 National Security Concerns

The use of national security as the main motivation behind denying Huawei market access is immediately apparent and consistent throughout the whole debate. The national security aspects often focus on the Western worries about Huawei's allegedly troublesome history of espionage and close government ties. At the same time, given the role 5G will play in our future societies with increased interconnectedness and an inherent dependency on technological solutions hinging on 5G for critical functions in society, the use of national security is problematic. While the debate seldom defines national security more accurately than referring to the risk of *exploitation or shutdown of central societal functions*, it can be argued that everything relating to the introduction of 5G technology poses a national security risk. In some ways, that waters down the whole concept of national security in the debate[151]

4.2.2 Geopolitical Implications

The 5G deployment is understood to come with clear implications for the geopolitical landscape and power structures. But the relation goes two ways; Just as the geopolitical environment, including the ongoing trade conflict between the US and China, is an important part in shaping the development of next-generation mobile standards and its deployment in different regions, the development of 5G will in turn also shape the future economic, technological and geopolitical competition between the superpowers of today[152,153,154] . Every major issue of 5G has been politicized, and the debate about whether to allow Huawei into Western markets has come to represent a broader *battle between political and economic systems*[2]. The importance of the "tech war" and its implications for global dominance should be understood in the context of the central role technology will play in our future societies, with some experts describing how the *"power, might and agency"* global actors possess is now measured in their technological potential.[155]

The geopolitical aspect can also be observed in the diplomatic pressure that is present in the discussion, where both China and the United States are actively trying to sway EU member states to take a stance in the debate. The European Union is depicted as being caught in the "middle of a geopolitical power struggle", forced to make a choice between

[151] For a discussion on the concept of national security, see chapter 7.4.
[152] (Albrycht & Świątkowska, 2019)
[153] (Kleinhans, 2019)
[154] (Triolo, Allison, & Brown, 2018)
[155] (Albrycht & Świątkowska, 2019)

"going East or going West".[156] Member states' differences in relations vis-á-vis China and the US, alongside discrepancies in their economic and technological capabilities and resources, ostensibly makes it difficult to find a common EU approach. The difficulty for the EU to find a common position in the Huawei debate is consistent throughout the literature.[157]

4.2.3 Huawei and China as one unit, metaphors and protectionism

What is immediately apparent is how China and Huawei are used interchangeably.[156] In a sense, Huawei seems to be used as a unit in which multiple European concerns regarding the emergence and governance of China are projected. A highly aggressive language is used throughout the debate, with frequent and recurring references to the notion of 'war', 'battleground' or 'race'. The 'battle' takes place over place over several 'arenas' and several different proxies for technology leadership are used. These include the number of 5G patents filed, participation in 5G pilot projects and seats in standard-setting bodies.[158]

Concerns about Huawei's alleged government ties to the and Chinese industrial policy are also frequently voiced. These are primarily referenced in in terms of their impact on EU industry, suggesting state support leads to an unlevelled playing field which will over time lead to European firms being outcompeted. The increased Chinese investments in the EU is, just as discussed in subchapter 2.4, another key theme in the literature and has led to new discussions on how the EU industry can be protected. Phrasings such as "new forms of industrial policy"159 and "protectionism light"160 are just a few examples of how this is reflected in the literature. Although the large EU vendors in telecom, Nokia and Ericsson, overall seem surprisingly quiet in debate, they have openly called for EU backing to support innovation and a level playing field in Europe. 161

4.2.4 Matters of dependency

In both the industrial and technical aspects of the debate, there is a common sense that the EU is afraid of getting too *dependent* on China and Chinese vendors. This seems to be the case both in having an EU tech sector that is competitive enough to tackle Chinese competition, but also to not let a Chinese vendor into the core of 5G networks. Not being

[156] (Albrycht & Świątkowska, 2019)
[157] (Rühlig & Björk, 2020)
[158] (Triolo, Allison, & Brown, 2018)
[159] (Huotari & Kratz, 2019)
[160] (Rühlig & Björk, 2020)
[161] (Matos, 2019)

dependent on China is closely related to the concept of EU *autonomy*, which emerges as a key concept in the literature. Few, if any, of the experts and policy makers neither directly nor indirectly advocate an outright ban of Huawei, suggesting that it would have little impact on the most explicitly voiced concerns in the debate alongside various consequences. At the same time, many of the reports and documents highlight how Chinese presence in telecommunications networks, and thereby increased overall dependency on China, stands in contrast to realizing European autonomy[162] and stronger European independency.

Having Chinese vendors in critical infrastructure is often boiled down to the *trustworthiness* of the vendor and the likeliness for the vendor not to use its legitimate access to 5G networks for malicious purposes.[163] As the implementation of 5G according to most experts will come with inherent security risks[164], and the ability for member states to properly assess these risks seem insufficient, trust in the vendor emerges as a main theme in many of the expert reports on the issue.[165] And, as another key finding and final note of this section, it should be mentioned how the literature is coherent in framing the issue as multi-layered, complex, and increasingly politicized.

4.3 Key stakeholders

Throughout the various discussions and reports concerning the issue of 5G and the Huawei debate a number of key stakeholders emerge: (1) *Mobile network operators* such as Vodafone and Telia, which provide mobile communication services enabled via infrastructure from telecom equipment vendors; (2) *European telecom equipment vendors*; including suppliers Ericsson and Nokia with their purpose of providing mobile network operators with mobile infrastructure; (3) *EU member states*; with their individual resources, market conditions, capabilities and interests; (4) *EU institutions*, including the EU parliament and the EU Commission pursuing a coherent and coordinated 5G agenda for the EU as a whole; (5) *Huawei*, also a telecom equipment vendor and the centre of the debate; (6) *China*, interested in both supporting Huawei's expansion and in realize their geopolitical ambitions. Often, Huawei and China are conflated and seen as one unit of analysis in the debate; (7) *the United States*, trying to influence EU decisions on Huawei

[162] (Albrycht & Świątkowska, 2019)
[163] (Lysne, 2018)
[164] (ENISA, 2019)
[165] (European Parliamentary Research Service , 2019)

and safeguarding their geopolitical power position vis-á-vis China. Figure 2 provides an overview of the relevant stakeholders of the Huawei debate.

Figure 2. Main observed stakeholders in the 5G debate in the EU context

4.4 Towards a first categorization

With the above points providing a scene setter and pinpointing some of the broader arguments and themes in the 5G debate from an EU perspective, attention can now be turned towards the preliminary categorization of the purposive sample. In an iterative and inductive process, continuously analysing and comparing the documents included in the first sample, a number of risks become evident and reoccurring. These *risks* or *challenges* of the 5G build-out in the EU, as highlighted by the stakeholders, largely falls into one of three categories: *(1) technical; (2) industrial; and (3) structural.* These categories will form the basis and foundation for the framework of this thesis and are defined below.

Firstly, the 5G debate is to a large extent built upon accounts of its transformative aspects. It is made clear that the transition from 4G to 5G has greater implications than any prior generations of mobile communications networks and that the introduction of this novel technology *in itself* presents new challenges and risks for the stakeholders. The way in which these networks operate and are structured inevitably lead to new types of IT security and need for risk mitigation. Accordingly, this thesis defines the first category of risks as *technical risks,* which are those *directly relating to the implementation, structure and operation of 5G networks*. These risks are argued to exist irrespective of the vendor providing the network. There is thus merit to further analyse the technical challenges of 5G deployment, what they are and how they challenge the governance of 5G in the European Union. As such, technical risks will represent the first analytic 'track' of this thesis.

Secondly, the implementation of 5G networks in the EU clearly poses challenges for the industry and European businesses. Contrasting to the previous category which is sector-specific, these risks are industry-wide and poses competitive challenges for the European Union. The technological advancements of Chinese vendors, their highly competitive prices, the often-highlighted unfair business practices that seemingly haunt European

businesses and the rather squeezed situation of EU vendors facing a new competitive reality are part of the factors that mentioned in the literature. As such, the second category of risks and challenges are *industrial risks,* which are the perceived risks and challenges from 5G implementation for European businesses at the aggregate. While technical risks are to a degree independent of the various possible outcomes of the current 5G debate in the EU, the industrial risks follow more of a two-track logic. That is, there are certain risks and challenges which comes with a *ban* of Huawei and others that are perceived as coming from *keeping* them in the networks.

Thirdly, there are frequent references throughout the literature to how preconditions and differences in resources and capabilities, both within the EU and the individual member states, complicates the Huawei debate. With dispersed telecommunication markets (see subchapter 2.3) in the EU and MNOs which are at the offset differently reliant on Huawei, combined with member countries having different economic resources and capabilities, a coordinated EU approach is immensely difficult. There are also differences between the 27 EU member states in their diplomatic ties and loyalties to China and the US, which adds another layer of complexity. This is if anything confirmed by the differences in tones amongst the various EU member states as of current[166]. The third category reflects the *structural risks and challenges* in 5G deployment from an EU perspective. These risks are thus not directly related to the issue of 5G, but rather to the (in)ability to mobilize resources and coordinate within the European Union, reflective of the varying preconditions in the EU-27. While the technical risks were sector specific and the industrial risks industry-wide, the structural risks are continuing the climb up an "imaginary ladder", changing the unit of analysis and describing *interstate risks.* Table 3 summarizes the three initial categories that become evident from the purposeful sample, including their definition.

[166] (The White House, 2019)

Table 4. Overview of emergent risk categories

Category	Description
Technological	Risks stemming from the technical implementation of 5g networks, and the vulnerabilities that comes with increased interconnectedness in these networks. Somewhat independent of the vendor providing the networks.
Industrial	Risks with banning or allowing Huawei in EU markets from a competitive perspective. High economic costs and delayed roll-out stand of 5g technology against the risk of seeing Huawei outcompete EU vendors by using unfair business practices.
Structural	Risks stemming from the structural differences between the EU member states - in their resources and regulations, but also in their diplomatic relations to the us and china. The difficulty to coordinate the EU-27 leads to challenges of a more structural nature.

At this stage it is worthwhile to briefly reflect on the nature of this categorization. First, it is important to recognize that these are ideal categories and subject to a degree of simplification. Certain issues with regards to 5G in the EU may be situated between two categories or to some extent reflective of several categories. Therefore, the categories are not meant to be interpreted as mutually exclusive, but rather as instruments meant to bring a level of clarity in what is a truly complex and multifaceted issue. Second, it is worth recognizing that each of these three categories does not exist in vacuum. Rather, they interact in several ways, exacerbating one another and adding layers of complexity. The formation of risk categories is a first step to break down the debate into smaller components. By deconstructing the actual risks highlighted in the literature, this thesis aims to create a more granular understanding of the risks.

However, for analytical clarity and coherence, the three categories are hereafter analysed separately. In accordance with the grounded theory approach of this thesis, where naming segments of data with a label that *"simultaneously categorizes, summarizes, and accounts for each piece of data"* is the first step towards an analytic interpretation of the dataset, the categorization will enable further analysis. Accordingly, the thesis substantiates each of these categories and their sub-components through focused coding by engaging with further literature deemed relevant and insightful given the preliminary findings, while gradually increasing the level of theorization in reflection of how the analysis emerges. [167]

[167] (Charmaz, 2006)

5. ANALYSIS

5.1 Reader's guide

Building on the purposive sample of data and the initial findings in the previous chapter, the following chapter will constitute the main part of the analysis of this thesis. While the chapter is structured around the three main categories of risk identified in chapter 4, the more in-depth analysis of the chapter also gives an opportunity to collect additional data when required in an iterative process, going back-and-forth between writing and coding the data, which is standard practice in grounded theory and described in chapter 3.3. The following three subchapters will further explore each of the identified risk categories while gradually increasing the level of abstraction. The increased level of abstraction is seen as an exploration of underlying concerns or challenges that emerge in the analysis of the risk categories. It should be noted that although the risk categories are separated and to some extent analysed individually, they are by no means mutually exclusive and intertwined in many aspects. This will not least be shown in subchapter 5.5, where all the risk categories are combined and presented in a comprehensive framework - the key finding of this paper and a visualization of the theory that has been derived from the research. The analysis starts by describing the technological risks.

5.2 Technological risks

The initial coding shows that the implementation of 5G networks come with several technical risks. These risks have been highlighted by experts and policymakers through all documents reviewed and are in many ways inherent to 5G technology.[168] As such, these risks to some extent seem to be present regardless of the vendor.[169,170] Nonetheless, and just as the rest of the Huawei debate, even the *seemingly* neutral aspects of the discussion have been politicized - and the same goes for the technical risks. This subchapter provides an overview of the main technical risks that have been identified in the data collection as they are a central part of the debate. An understanding of these risks and how they relate to each other is also important for the subsequent reasoning of why some stakeholders view the risks as exacerbated when talking about a Chinese vendor like Huawei.

[168] (Kleinhans, 2019)
[169] (NIS Cooperation Group, 2019)
[170] (ENISA, 2019)

As described in background chapter 2.2.1 on telecommunications networks, 5G will significantly increase the number of devices that can communicate simultaneously and increase the amount of data in our networks, factors that will both have an effect on the security of 5G networks. The technical risks outlined by the experts in the 5G debate falls into two broad categories: (1) *Risks related to the virtualization of networks*; and (2) *risks related to the increased interconnectivity of devices and sectors*. These categories and specific risks will now be explained separately and in more detail and are summarized in Table 1 below.

Table 5. Overview of identified technological risks by theme

Risk Theme	Risk	Description
Virtualization	Software updates	More frequent software updates necessitate granting access to third parties and exacerbates security assessment challenges
	Blurred boundaries	Software-based systems get rid of prior hardware 'choke point' making it more difficult to restrict access from different parts of the network
Connectivity	Insecure devices	Smart devices with subpar security standards represent net 'points of entry' for cyber-attacks and increases the attack surface of networks
	Increased data volumes	Increased data volumes make it easier for malicious code to get lost in the 'noise'

5.2.1 Virtualization of networks

Virtualization of networks entails the transition from hardware to software which comes with 5G implementation. Whereas previous generations of telecommunication have primarily relied on centralized, hardware-based systems, these are progressively being moved into the cloud.[171] This is deemed a challenge for cybersecurity, as it means that the pieces of hardware which used to represent 'choke points' where cyber hygiene could be assessed - for example the identification and removal of malicious code and viruses - are being removed.[172] As such, virtualization of networks results in two specific risks: (1) *software updates*; and (2) *blurred boundaries between the different parts of the network*.

[171] (Wheeler & Simpson, 2019)

[172] (Wheeler & Simpson, 2019)

Cybersecurity is practiced in a variety of ways, but usually involves an assessment and review of the software code that underpins the systems.[173] Simplified, this is done to check whether the employed telecom equipment contains malicious code or functions that would make the system insecure. In prior generations of telecommunication networks, the software component of the networks would be updated rather seldomly, at least in comparison to what is expected with 5G. As the software requires more frequent updates with 5G, it also entails that mobile network operators must grant third-party actors access to the network in order to update it. Every software update would therefore give the third-party actors an opportunity to change the software code in what has previously been deemed a secure system.[174,175] The software update would in turn require a new cybersecurity risk assessment to prove that no new, malicious code exists in the network. Therefore, the increased number of software updates are understood as representing a 'clean slate' in terms of cybersecurity, and the digital infrastructure component of 5G networks will play a larger role in the operation and maintenance of networks than in prior generations.[176]

Another consequence of the virtualization of networks is how it is expected to blur the boundaries between its different parts, such as between the outer Radio Access Network (for more on RAN; see subchapter 2.2.1) and the inner, sensitive part of the network handling the authentication and storage of mobile networks operators' user data, the core. Operators in Europe are already moving their core networks to cloud environments and there are several industry initiatives to virtualize RAN. Some experts in the literature are stating that the distinction between core and RAN is unsustainable due to virtualization[177,178]. Network functions are not tied to network equipment anymore, but rather to pieces of software blurring the lines between core and RAN and making it increasingly difficult for governments to define what is sensitive parts of a network.[179] Even though a vendor only provides equipment to outer parts of the network, as systems move to the cloud there may still be ways to access the sensitive inner parts, compromising data privacy and security.

[173] (Sullivan & Lucas, 2020)
[174] (Wheeler & Simpson, 2019)
[175] (Kleinhans, 2019)
[176] (Kleinhans, 2019)
[177] (Kleinhans, 2019)
[178] (Lysne, 2018)
[179] (Kleinhans, 2019)

5.2.2 Increased interconnectivity and cyber security

The second theme identified in the debate concerns the *increased inter-connectivity of devices and sectors* under 5G *vis-à-vis* previous generations of telecommunication. Indeed, this is one of the main benefits of 5G, however it is deemed a double-edged sword and reflective of multiple cyber-security challenges. There are mainly two risks which fall within this theme: (1) *Risks relating to the internet of things and* (2) *risks with increased data volumes*. First, as outlined in the background chapter (see subchapter 2.1.1), one of the key benefits of 5G is that it opens 'digital real estate' enabling more smart devices to come online and communicate with each other. This is a prime driver behind discussions of the internet of things. However, once connected and communicating with different parts of the network, these devices represent new 'points of entry' through which cyber-attacks can gain access to other parts of the network.

Experts highlight how this is particularly troublesome given that many of the smart devices, such as watches, fridges, and the like, are subpar in terms of security standards. Different devices have different levels of security. Accordingly, these devices are deemed to represent a threat to privacy and the overall network itself[180], as they are more interconnected than before. But there is another factor exacerbating this risk - the exponential increase in data volume that comes with 5G technology. The sheer increase in data volume poses a real challenge for network security, as more code makes it increasingly difficult to identify irregularities or malicious code.[181] This is spurred on by the increased connectivity of businesses, sectors and devices, all contributing to the exponential increase in data that will be transferred in the new generation of networks.

While the risks of 5G implementation in this chapter are rather technical, they are important in understanding the debate on Huawei. Experts in the debate, as opposed to policymakers and governments that are less nuanced in their stances, seem to agree that these risks are to a large extent inherent to the implementation of 5G networks in themselves, regardless of the vendor. The risks presented above can be derived from the increasing complexity in which telecommunications networks and the actors involved in them operate. Accordingly, much of the argumentation put forth in the debate can be summarized by the notion that "complexity is the enemy of security".[182] A large part of the

[180] (Kleinhans, 2017)
[181] (Wheeler & Simpson, 2019)
[182] (Wheeler & Simpson, 2019)

discussion thus concerns how, if at all, these matters of security can be mitigated or contained.

Yet, what is common across most of the literature, is the understanding that networks will never be completely safe, and that risk assessment is not capable of sufficiently removing the technological risks that comes with 5G implementation. This does not only relate to 5G networks in themselves, but also to the limits of cyber security and to its inherent asymmetry: systems can be declared as insecure through observation, but not the other way around.[183] This 'unfalsifiability of security claims'[184] can express itself in a series of ways. For example, while it is possible to identify malicious code in a system, one can never prove its *absence*.[185] Reviews of source code or IT security certification schemes thus, as previously reasoned, are understood as quickly losing validity as each software update, to an extent, represents a clean slate.[186] Similarly, means of assessing whether hardware has been tinkered with assumes access to a 'golden sample' or unit by which to compare to. These two practices are foundations of cyber security and highlight the certain limitations of current means of assessing cyber security once there is reason to believe that an actor in the system is not to be trusted. Subsequently, if one introduces mistrust into buyer-vendor relationships, many of the methods of risk evaluation and cyber security become mute or less effective.[187] This leads to perceived challenges with regards to the 5G debate.

5.2.3 Towards a conceptualization of trust

Having outlined the practical technical risks stemming from 5G implementation and the difficulties to assess and mitigate these risks in the networks themselves, attention is now turned towards Huawei. Why are these risks so different when the discussion is concerning a Chinese vendor, when a large part of the risks rather points to vulnerabilities in the technical implementation and transition to the next generation of mobile networks itself? A starting point in the analysis of this can be found in a re-occurring theme throughout all the literature, namely the lack of separation between Huawei as a vendor and the Chinese state. The depiction of Huawei in the debate is seldom focused on the company as its own unit, but rather as an indirect or direct tool for the Chinese

[183] (Herley, 2016)
[184] (Herley, 2016)
[185] (Lysne, 2018)
[186] (Rühlig & Björk, 2020)
[187] (Lysne, 2018)

government to control. In other words, China and Huawei are often merged into one unit of analysis.

To some extent, this framing is understandable considering the alleged government ties Huawei often is accused of, not least in concerns over their close relation to the PRC's security apparatus and Huawei founder Ren Zhengfei's background in the People's Liberation Army. These arguments are also often accompanied by concerns over the company's non-transparent ownership structure and the preferential treatment Huawei has received from the Chinese government over the years, including monetary support.[188] Together, they form the ground upon which worries about Chinese espionage or sabotage in Western networks is built (see subchapter 2.5.2). The espionage concerns also tie to the recently imposed Chinese legislation, *China's Cyber Security Law of 2017*,[189] which legally binds Chinese companies to provide the government with intelligence on both domestic and international matters if the security services require them to do so. The fact that Huawei is bound to hand-over sensitive information on international matters becomes particularly sensitive in light of the 5G investments abroad.

While these aspects are central in shaping the debate and should be taken seriously by EU member states, the threat of China taking advantage of technical vulnerabilities in 5G networks to conduct espionage or sabotage is highly questionable in practice, according to some experts. While there are indeed reports of previous Chinese espionage, the channels through which these activities have been carried out is not primarily focused to mobile communications networks. Techniques such as spear-fishing and social engineering are far more common than the use of ICT systems to gather information.[190] The same goes for the argument that China would use Huawei equipment to shut down foreign countries' communications network in case of conflict. The truth is that China, if determined to do so, most likely has the technical expertise and skills to shut down a communications network in a foreign country *regardless of whether Huawei technology was central in building up the EU infrastructur*e.[191] Moreover, both espionage and sabotage would come at an astronomical political economic cost for the Chinese government. In addition, while the technical risks stemming from 5G implementation indeed are important to address and mitigate, it is important to still keep in mind that these vulnerabilities by no means are specific to Chinese vendors. The technical vulnerabilities are inherent to the *deployment of 5G in itself* and the technology it builds

[188] (Rühlig & Björk, 2020)
[189] (Wagner, 2017)
[190] (Albrycht & Świątkowska, 2019)
[191] (Rühlig & Björk, 2020)

upon.[192][193] The reliance of 5G networks will make our economies and societies more vulnerable, no matter who the vendor is[194] and the trustworthiness of the technological equipment is therefore just *one aspect* of the risk assessment of 5G networks.[195]

As previously mentioned, network security and risk assessment of equipment and software used in 5G implementation are insufficient to prove the *absence* of malicious code in already existing products. In addition, even if a risk assessment would be secure enough to prove the absence of malicious code, it could be made irrelevant by a simple software update. Therefore, the decision to allow market access for a company in 5G deployment ultimately depends on *trusting the vendor company* not to abuse its legitimate access for malicious purposes. The fact that the employed 5G networks will be the standard for many years to come also means that the choice of 5G vendor not only hinges on trusting the company *now*, at this specific point in time, but also trusting the company for the foreseeable future.[196]

Huawei is arguably one of the most controversial and audited companies in the world and have focused heavily on making their products secure.[197] This strategy largely misses the point however, as the system can be very secure towards a third-party but still not be secure if the company itself can access sensitive information. *"We cannot assume that security comes with trust. But we cannot assume that trust comes with security either."*[198] The trust in the individual company is not enough to allow access into a Western telecommunications network, as many expert highlights how the reportedly close ties between the Chinese government and Huawei, making the a common unit of analysis, extends the notion of trust also to the Chinese government. Additionally, in the supply chains of today there are very few pieces of electronic equipment without at least one part stemming from a country deemed untrustworthy.[199] Having trust in the company supplying 5G technology thereby stretches beyond the scope of the individual organization.

The notion of trustworthiness therefore does not stop at the level of the vendor, but also includes its home government. If the Chinese government, despite the high political and economic costs, would attempt to exploit Huawei's access to Western telecommunication networks with malicious intent, the ability to do so would to a large degree depend on

[192] (Wheeler & Simpson, 2019)
[193] (Rühlig & Björk, 2020)
[194] (Kleinhans, 2019)
[195] (Kleinhans, 2019)
[196] (Kleinhans, 2019)
[197] (Lysne, 2018)
[198] (Lysne, 2018)
[199] (Lysne, 2018)

the legal and political system Huawei operates in. Huawei has a clear, business-oriented, incentive not to use its equipment for espionage, as it would hurt their operations massively if such an occurrence became publicly known. If Huawei would have the possibility to stop or prevent the Chinese government, they could be deemed more trustworthy. As a large part of the literature describes, the lack of trust in the Chinese legal and political system is a major explanation for why Huawei as a company is seen as untrustworthy.[200] At the same time, the assessment and trust in the Chinese legal and political system differs between EU member states, which largely explains the difference stances taking within the Union. The risk is in the eye of the beholder. The above rationale can be clearly exemplified by the Snowden revelations.

The Snowden documents back in 2014 showed that the US government via the National Security Agency (NSA) had intercepted network devices during shipping, installed software intended for surveillance, and then had the devices delivered to their initial destination and user. After the scandal was revealed, the company whose devices NSA tampered with - Cisco - saw a hefty sales drop in China after the government's encouragement to avoid foreign equipment. Meanwhile, there was no ban on Cisco in European networks. The reason behind this difference and the rather mild reaction in Europe arguably being the trust which European countries have in the US legal and political system. When a Western government exploits a national company's equipment for surveillance purposes, the company in question can make a claim in court. In the years following the Snowden-revelations, American ICT companies pushed the US government to engage in a reform process, including increasing transparency. While there is no reason to view the US government as a role model on these issues, the possibilities for Huawei to take its government to court is unlikely - and the Chinese government has itself done little to address criticized laws on for example cybersecurity and cyber espionage imposed after 2018.[201] These factors are essential in understanding the lack of trust in the Chinese government according to experts - and important underlying aspects of the Huawei debate.

Summing up, it can be concluded that technological risks indeed pose a challenge for the EU, as does the difficulty to sufficiently assess these. While it is important for the EU to address these challenges, it should be remembered that many of the technical risks stemming from the implementation of 5G networks are present no matter the host

[200] (Kleinhans, 2019)

[201] (Kleinhans, 2019)

country of the vendor. Therefore, the risk of granting Huawei market access in critical EU infrastructure depends on the trust in Huawei as a company - ultimately dependent on the trust in the Chinese government and its legal and political system. This is truly a key takeaway from the literature, how trustworthiness in Huawei, China and ultimately the Chinese system links the technological risks to broader, underlying concerns. Because the likeliness that a foreign government coerces one of their vendors to exploit legitimate network access is not a question of technical vulnerabilities. It is rather a question of geopolitics. Figure 3 summarizes the findings of chapter 5.2.

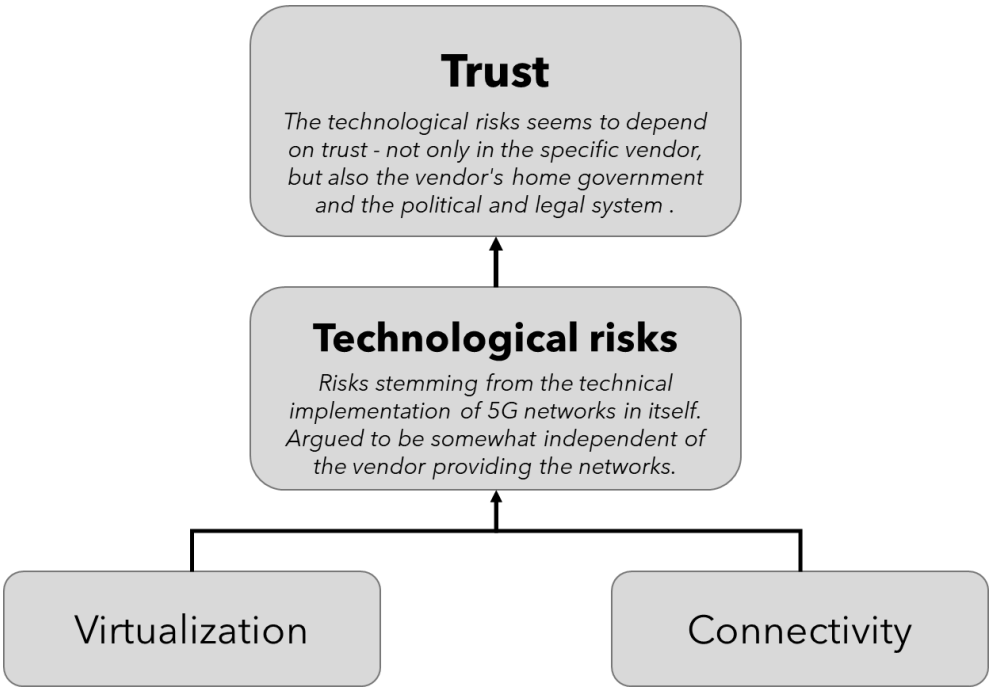


Figure 3. Connecting technological risks to conceptualizations of trust.

5.3 Industrial risks

While the Huawei debate arguably focuses on concerns of Chinese government's potential exploitation of network access, the purposive sample also suggest there to be risks of an industrial and strategic nature. These concern the *future competitiveness and autonomy of European industries*. In contrast to the technical risks outlined and discussed in above chapter, the logic and argumentation seen throughout the debate is two-sided. Industrial concerns are thus discussed as *contingent on the outcomes* of the current debate and whether Huawei and other Chinese telecom suppliers' presence in European networks is to be banned or not. Accordingly, this chapter is characterized by a level of parallel reasoning of how risks and challenges are perceived *depending on outcome*. The following subchapters deconstruct the logics of the two opposing views before analysing their underlying similarities.

5.3.1 Risks of banning Huawei

There is an almost unison agreement amongst European stakeholders that a ban of Huawei comes with a series of consequences. These relate to: *(1) the presumed speed at which 5G may be rolled out in Europe without Huawei; (2) the additional economic costs which it would incur*; *(3) potential industrial repercussions coming from China if Huawei were to be banned*. First, there is an unanimous assessment by policymakers, industry associations and network operators that a ban of Huawei would lead to a significant slowdown in the roll-out of 5G networks. While estimates vary, MNOs such as *Three*[202], *Vodafone*[203] and *Deutsche Telekom*[204] all agree that a direct ban of Huawei would delay the buildout of 5G in Europe, ranging from 18 months up to around five years. Similarly, the *GSMA*, a mobile industry association, suggested that a ban would not only jeopardize the functioning of the current European 4G networks, but also delay the deployment of 5G networks "for years". European policy makers ostensibly concur with the evaluation, with the interior minister of Germany explicitly adding that "*I don't think [Germany] can quickly build a 5G network… without Huawei taking part*".[205] The delay is largely explained by the surge in demand that would occur, creating an order backlog for Ericsson and Nokia. "*Such a delay would widen the gap in 5G penetration between the EU and the U.S. by more than 15 percentage points by 2025*," according industry estimates.[206]

[202] (BBC, 2019)
[203] (Cellan-Jones, 2019)
[204] (Donahue, Nicola, & Parkin, 2019)
[205] (Staudenmaier, 2020)
[206] (Barzic, 2019)

Second, in addition to the expected delays, a ban of Huawei would incur significant economic costs for the European Union and its members states. According to industry estimates, the total costs of 5G deployment in Europe could increase by around €60 billion.[207] More than half of this additional cost would come through higher input costs as a result of significantly lowered competition in the telecommunication equipment markets. Similarly, in case of a ban, multiple operators across Europe would have to replace most of their existing infrastructure – a very costly exercise. As suggested by a Vodafone executive, "*the cost of [banning Huawei] runs into the hundreds of millions and will dramatically affect our 5G business case"*. [208] The costs of banning Huawei thus extend beyond the initial investment to also hamper European operators' ability to turn 5G into viable business cases for their customers. This in turn would affect the development of business models built upon 5G technology.[209]

Third, there are concerns of Chinese repercussions if EU countries would be banning Huawei from their markets. In cases where a ban, whether it would be partial or complete, would be deemed arbitrary, there is a risk of Chinese reciprocity. This would have a multitude of consequences for European industries broadly. In response to a German proposed legislation aimed to exclude 'untrustworthy' 5G vendors, the Chinese ambassador to Germany suggested that *"if Germany were to take a decision that leads to Huawei's exclusion from the German market, there will be consequences. The Chinese government will not stand idly by"*. Policy makers and experts are thus aware of the highly contentious nature of the issue of Huawei and how it relates to EU-Sino relations more broadly (something this thesis will address once more in chapter 5.4). A potential fallout could thus transcend the technological sectors to other sectors central to the European economy, such as the automotive industry, but also have diplomatic ripple effects.

While the above may be understood as the immediate consequences and risks of banning Huawei, policymakers and experts also underscore the long-term ramifications. As suggested in the background (see subchapter 2.2.1), the transformative aspects of 5G are the opportunities it enables in terms of other novel technologies, including autonomous vehicles, artificial intelligence, and machine learning. The implications of an exclusion of Huawei from European markets would, in a worst-case scenario, be Europe falling behind in developing the various products, services and end-solutions which are underpinned by 5G. As suggested by the European Political Strategy Centre, "*failure to*

[207] (Barzic, 2019)
[208] (Cellan-Jones, 2019)
[209] (Cellan-Jones, 2019)

master one technology results in knock-on effects with regard to future technologies.[210] *The longer this vicious circle ensues, the harder it is to catch up down the line*" The outcome of the debate is thus understood as one which will set Europe on a trajectory which has broader implications for the realization of European industrial leadership[211]

5.3.2 Risks of not banning Huawei

In contrast to the above section, there are also several industrial risks highlighted in the literature which stem from allowing Huawei market access. These primarily relate to the expected risk of exacerbating the current trend in which Huawei has a strong foothold and market share in the EU at the expense of European vendors such as Nokia and Ericsson. Provided that dependency on Huawei in European network infrastructure is already rather extensive, in certain countries surmounting to 90 percent[212], there is a fear that the European vendors will be pushed out of the market if the current trend continues (see Table 2). Huawei has become a powerful competitor, able to compete with its European counterparts both in terms of technology and price.[213] The debate highlights fundamental concerns surrounding the competitiveness of Huawei, mainly relating to the alleged support Huawei gets from the Chinese government - which gives the company an alleged unfair advantage according to many Western sources.

The literature suggests a common notion of how the alleged differences in economic and competitive conditions between Chinese and European firms results in risks for the European industry. China's economic policies are continuing to be fundamentally different from market-oriented principles and practices in other OECD countries, and the discrepancies in the promotion of open markets, effective price systems and clear boundaries for state interference are lifted as major concerns contributing to Huawei's possibilities to compete with European firms.[214] The claimed unfair trade practices also include technological transfer and the previous practices of reversed engineering, all mentioned in background chapter 2.5. While the trend of China converging to the liberal business practices of the Western previously has been clearly observable, there are growing concerns that this trend has changed in recent years.[215] This is therefore something the European Union needs to address in order to ensure a fair competitive environment for the EU's own telecom industry, according to some experts. Unequal

[210] (European Political Strategy Centre, 2019)
[211] (Albrycht & Świątkowska, 2019)
[212] (Rühlig, 2020)
[213] (Kleinhans, 2019)
[214] (Huotari & Kratz, 2019)
[215] (Huotari & Kratz, 2019)

market access conditions[216], distorted financing costs for Chinese companies and state interventions affecting operational costs - and thereby also price competitiveness - are all brought up in the debate as threats to the EU industry[217,218] and are argued to spill over into the European business climate.

While European telecom vendors generally have been rather silent throughout the 5G debate, Ericsson has previously voiced their concern that the EU has not done enough to support the domestic industry amid the 5G rollout.[219,220,221] This naturally is seen as standing in sharp contrast to the highly coordinated strategy of China. As such, it is feared that if nothing is done, the discrepancies in competitive conditions and financial realities between Chinese and European firms will only be exacerbated further.[222] The unequal competitive realities have led to renewed interest in policies strengthening the EU's home-grown industry, with some experts using terms as "strategic industrial policy"[223] light and "protectionism light"[224]. The broader question of how the European Union should protect its industry and ensure future competitiveness emerges as an underlying worry in the debate, and this thesis argues that part of the debate about excluding Huawei from the EU market can derived to the notion of *"competitiveness"*.

5.3.3 Towards a conceptualization of competitiveness

While the question of future competitiveness for the EU industry by no means is specific to the introduction of 5G, the Huawei debate has served as a catalyst in putting the topic high on the agenda. Huawei has emerged as a highly competitive rival to the European telecom firms - both in terms of price and technological development. But the fast growth of Huawei has also spurred a broader discussion on how to compete with Chinese companies more generally, especially considering the difference in competitive conditions between the EU and China that has become increasingly problematized, particularly in the tech sector and in industries vital for national security. How should the European Union tackle what they claim to be unfair business practices and state support that the Chinese companies are benefiting from? The literature stresses how these challenges need to be addressed in order to protect the EU industry. But how can be

[216] (European Political Strategy Centre, 2019)
[217] (European Commission, 2013)
[218] (Chaffin, 2013)
[219] (Fildes, 2019)
[220] (Stec, 2019)
[221] (Ekholm, 2019)
[222] (Huotari & Kratz, 2019)
[223] (Albrycht & Świątkowska, 2019)
[224] (Rühlig & Björk, 2020)

better understand why have these become a problem now in the Huawei debate, and not before?

Until recently the EU has broadly welcomed Chinese investment to boost an economy still recovering from the eurozone crisis (see subchapter 2.6).[225] Speculative, part of the reason why the EU previously hasn't raised louder concerns about the government supported businesses and a lack of industrial reciprocity vis-á-vis China has to do with the Chinese competitive position in the global market. Tying to background chapter 2.4, China's economic rise is truly unprecedented, and as the country has emerged as a new economic superpower it has also changed the approach by other states in their interactions with China. Having started as a developing economy in which Western states were very keen on being granted market access, accepting the somewhat unequal terms this relationship was built upon, the tide has now started to change. Official publications from the EU reassert this view, stating that the EU is both concerned with the EU competitiveness on the world stage more generally and at the same time sees a changed, more assertive, stance towards some of the union's strategic trade partners - and perhaps most notably China, in particular.[226]

The European Union has by no means been ignoring the business practices of China before, not least seen in the launch of the investigation on anti-dumping and anti-subsidy already in 2013[227] (see also background chapter 2.5), but the Huawei debate with its framing as a national security issue and potentially large consequences for the EU tech industry seems to be a culmination of growing concerns from the last decade. Reading between the lines – and sometimes explicitly outspoken – China has now become too powerful and competitive to grant special treatment. And the Huawei debate has served as a catalyst that has been just enough to push the European Union over an imaginary line to take action. This changed view on China is also reflected in how the Chinese strategic investments into the EU following the financial crisis in 2007-2008, described in background chapter 2.6, was not at all seen in the same light as the current situation of Chinese investments in critical infrastructure.

While the rise of the Chinese economy and the perceived threat it may pose to European competitiveness can be identified as a key underlying challenge for the EU throughout much of the literature, there are differences in how the stakeholders see it going forward.

[225] (Lehne, 2020)
[226] (European Commission, 2019)
[227] (European Commission, 2013)

From the EU's side, the introduction of an investment screening regulation is one of the actions the EU has taken to address the new competitive climate.

But the issue has also been addressed in official EU publications talking about how the EU will focus on improving market access for EU businesses in China[228] and reinforcing the EU's policy toolbox in addressing unfair trade practices. Although surprisingly quiet in the debate overall, this is also an area where the EU telecom equipment providers have outed their opinion, for example by pushing the EU to be more active in promoting European tech innovation, speaking of the importance of a level playing field vis-á-vis states favouring national champions and calling for an common EU industrial strategy.[229] Similarly, European think-tanks are stressing the need for a coherent "digital strategy" for the EU, with one going as far as saying;

> *"Ultimately, the ability of the EU and European stakeholders to shape rules and standards governing digital technologies (…) also relate to the EU and its Member States' ability to uphold their interests and values over the long term."*[230]

Throughout the literature, a strong tech sector is understood as being key in future industrial dominance, as well as laying the foundation for geopolitical power. Having a cutting-edge industry will not only be beneficial for the tech sector, but have enormous spill-over effects to other sectors as the future industrial practices, as mentioned in background chapter 2.2.1, will be so heavily reliant on artificial intelligence, interconnectedness and new solutions building on 5G networks. The European Union has a history of being at the forefront of technological development, having a position high up the value chain with strong R&D. Chinese vendors are now getting an increasing piece of new patents and setting standards, tying to an outspoken goal of becoming world leading in technology in 2030 (see background chapter 2.4).[231] The fear of China outcompeting the EU industry is therefore not only a worry about unfair business practices but could also be interpreted as an almost existential fear of losing its competitive advantage when Chinese is transforming from a developing to a developed country. And losing a competitive advantage in the tech sector when the future arena for competitiveness seem to be technological advancement is a reason why the Huawei

[228] (European Commission, 2019)
[229] (Matos, 2019)
[230] (European Political Strategy Centre, 2019)
[231] (Kharpal, 2017)

debate has come to represent more than just a decision on whether to include or exclude a specific Chinese vendor from the EU markets.

The industrial risks identified in this thesis can, following the above reasoning, therefore be derived *from two underlying concerns*, both captured in the notion of sustained European "*competitiveness*". The first regards China's increasing economic importance and the opinion that the Chinese companies can no longer be excluded from normal reciprocity practices. As put by the European Parliament;

> *"China should no longer be regarded as a developing country where such measures might still be necessary as part of an economic development policy; its increasing presence in Europe, supported by the MIC25 strategy, should therefore be accompanied by greater reciprocity, non-discrimination, and the openness of its system."*[232]

The second concern regards the future of the EU industry's continued competitiveness in itself - especially in tech - and what policymakers can do to sustain the position of the industry. While some experts are focusing on their own industry, aiming to create a digital sovereignty within the EU, others are reverting to terms like "protectionism light"[233] and the notion of industrial policies for the EU. This discussion is also affected by the overall geopolitical climate of confrontation, increased trade barriers and a "null-sum game" where protectionism seems to have come back in fashion. This tendency is not least shown in the trade war that has been playing out in recent years, and a large part of the literature sees a link between the global competitive climate on markets and in value chains and the increased attention the 5G debate has put on promoting European industry. For the EU to find its place in this new competitive climate, it requires not only a coherent strategy for the tech sector in itself, promoting innovation and letting EU businesses compete on equal terms with foreign vendors, but also to understand the current geopolitical climate on the world markets and the new view on China. Figure 3 summarizes the findings of chapter 5.3.

[232] (European Commission, 2019)

[233] (Rühlig & Björk, 2020)

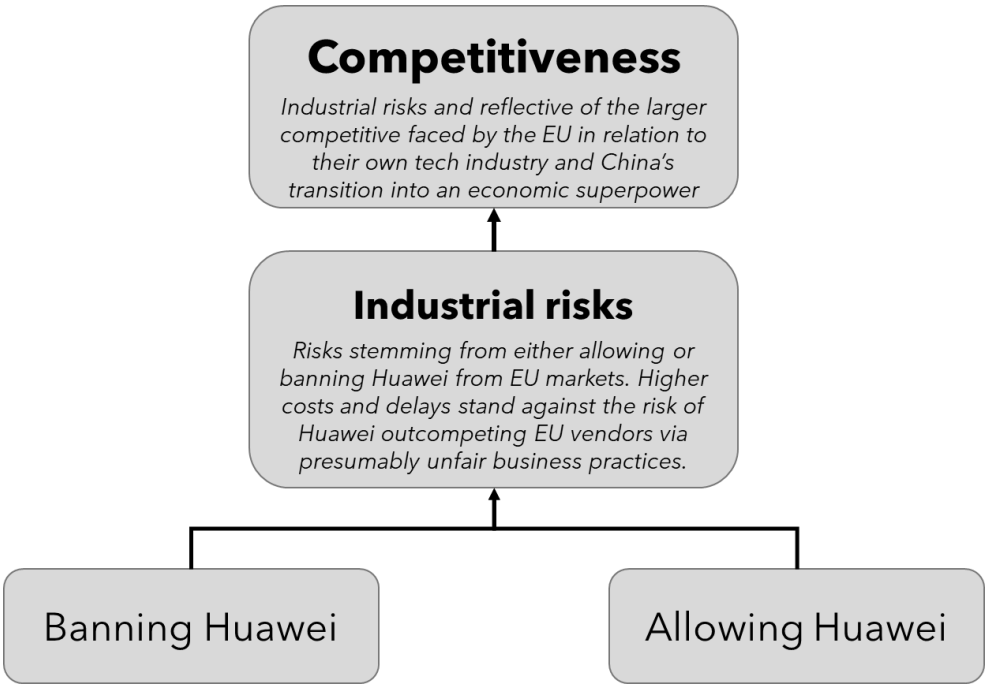


Figure 4. Connecting industrial risks to conceptualizations of competitiveness.

5.4 Structural risks

Having examined both the technical and industrial risks of allowing Huawei a role in the European roll-out of 5G respectively, attention will now be put on the structural risks identified in the debate. If the technological risks were relatively hands-on and sector-specific, the industrial risks lifted the unit of analysis to rather focus on the broader, competitive challenges for the whole EU industry, giving a business perspective on the issue across sectors. The structural risks chapter will continue this journey up an imaginary ladder, as the unit of analysis will now instead focus on the interaction between member states and their respective position within the union and the geopolitical climate - *an inter-state perspective*. A frequently occurring theme in the data highlights how the EU member states are dispersed and fragmented, both in terms of *resources* - economic as well as regulatory - and in terms of their *relations* to states outside the EU, predominantly China and the United States. The structural discrepancies between EU member states in these two areas are important for the discussion on Huawei and 5G, and the analysis of this chapter will therefore use them as a starting point.

5.4.1 Resources and regulation

The conditions in the European Union's 27 Member States vary greatly, and governance and market discrepancies across states are generating additional layers of complexity to the Huawei debate. As made evident by background chapter 2.3, while the EU markets are governed by a set regulatory framework, telecommunication is carried out by the NRAs at the state level - thereby remaining a sovereign right for the individual member states. As of current, there are more regulatory approaches to telecommunication than there are member states in the EU,[234] which translates into significant variations in the approaches to spectrum allocation, auctioning and licensing[235], but also to certification of suppliers[236] - ultimately resulting in a subpar European investment climate. The large number of regulatory approaches and differences across member states leads to a mobile infrastructure buildout that progresses at significantly varying rates across states.

This is not a problem specific to 5G, as it has existed also in prior generations of mobile networks. While the 4G coverage in North America hovers at around 90 percent, Europe is stuck at close to 60 percent[237] which is partly explained by the differences in the lack of a coherent regulatory approach. This has indeed been raised as a concern by market actors from all parts of the value chain, with *Orange* – one of Europe's largest telecom service providers - suggesting that *"we [Europe] are investing less than anywhere else in the world"*.[238] Similarly, the EU has been described *as "…arguably the worst place in the world to invest in telecoms and technology*.[239] As these quotes suggest, the differences and uncoordinated regulatory environment has implications also for the EU investment climate. Once again, a comparison can showcase the situation, as European investments on a per capita basis are *about half of those of the United States*.[240] Although consolidating, European telecommunication services markets are still *heavily fragmented*, with the number of mobile network operators being three times that of the United States and just surpassing that of China.[241] This is a structural problem for the whole union largely stemming from the difficulty to coordinate 27 different sovereign individual member states and their regulatory and market environments.

Discrepancies in telecommunication policy and market structure does however only represent part of the structural challenge. Differences in economic realities and

[234] (van Tetering, 2019)
[235] (5G Observatory, 2020)
[236] (Duchâtel & Godement, 2019)
[237] (O'Brien, 2019)
[238] (Fildes, 2019)
[239] (Fildes, 2019)
[240] (Albrycht & Świątkowska, 2019)
[241] (Issa & Jha, 2019)

aggregate level of dependency on foreign mobile infrastructure further infringes the alternatives of the individual member states. Some member states, such as Germany[242], is already so heavily reliant on Huawei and Chinese technology in the ICT sector that a ban would prove a major hurdle purely based on the economic and resource argument. The same goes for countries like Italy, where Huawei is the leading equipment manufacturer in 5G, and Poland, where all the main operators use Huawei equipment.[243] Excluding Huawei from these markets would not only set back the infrastructural development in these countries, but also come with an enormous economic cost. Other countries, like France and Denmark, would not struggle as much, as other vendors have a more prominent role in the mobile communications sector in these countries.[244] The reasoning of discrepancies between the member states also ties to the different economic realities facing the individual countries, a result that can partly can be traced back to the aftermath of the financial crisis. Huawei is providing a high-quality option for a relatively low price compared to its competitors,[245] which should not be an underestimated factor in the choice of telecom vendor given the tough economic reality in some member states.

The differences in economic resources between EU member states is also an explaining factor behind the decision of some countries, Greece to name an example, to accept large Chinese investments in other infrastructural sectors as part of China's Belt and Road Initiative. (see also background chapter 2.4 and 2.6). This ties to the discussion in background chapter on the situation that followed the financial crisis, but also to the discussion in the chapter 4 with the preliminary findings on how Huawei and China often are seen as one unit of analysis. These infrastructure investments, although not specifically made in the ICT sector, is suggested to create an overall dependency on the Chinese state.[246] Some experts even go so far as to say that China have become better at using the situation and play EU member states off each other, which would risk leading to an increased fragmentation in the EU.[247] Whether an intentional strategy from China or not, the investments are further highlighting the differences in resources and previous dependencies in the EU, perhaps also in terms of loyalties and diplomatic ties, which will be covered in the next section.

[242] (Staudenmaier, 2020)
[243] (Duchâtel & Godement, 2019)
[244] (Duchâtel & Godement, 2019)
[245] (Pawlicki, 2017)
[246] (Ferguson, 2019)
[247] (Lehne, 2020)

5.4.2 Relations

It has already been mentioned how the Huawei debate is often framed in rather aggressive terms, as a *battle between economic and legal systems* and a *race* for future technology. In a way, this rhetoric is stems from the tensions between the US and China which are reflected in the Huawei debate. The conflict between the US and China did not start with the 5G roll-out - and most likely won't end there either - but has come to have an effect also on the EU approach to the Huawei debate. The underlying competition for political and economic power is an important factor shaping the 5G issue, with the EU sometimes described as "caught in the middle of a geopolitical struggle".[248] The Huawei debate is at times framed as if the EU has to "pick a side", and it is therefore important to consider the members states' individual diplomatic relations to China and the United States respectively to understand nuances of the different approaches taken by EU countries. The diplomatic ties EU member states have to China and the US also further highlight the division and fragmentation within the union, making it unlikely that all EU countries would follow the same approach in the 5G roll-out.[249] There is for example a tendency for states who are closer aligned with China on geopolitical matters to also embrace Chinese 5G vendors.[250]

A type of *"diplomatic risk"* or *"increased diplomatic cost"* seems to emerge as a theme in the coding, where countries feel pressured to follow-suit in the 5G debate with the geopolitical superpower they have the closest diplomatic connections to. The decision by individual member states to ban or not ban Huawei seems to come with a threat of other repercussions, a ripple effect beyond the 5G debate in itself. Speculative, the pressure does not by default need to be explicit and outspoken, although the literature also mentions instances when the pressure is more direct[251] - not least seen in the case of the United Kingdom's decision to allow partial access for Huawei and Donald Trump's immediate response to UK Prime Minister Boris Johnson.[252] The US is reported to use "multiple tracks" to convince and pressure European countries to align with their stance in the Huawei debate, and EU countries therefore face a risk of worsening relations with the US if they do not comply with the recommended strategy.[253] Another aspect of this is that existing security operations between EU member states and US risk to become re-

[248] (Albrycht & Świątkowska, 2019)
[249] (Kleinhans, 2019)
[250] (Kleinhans, 2019)
[251] (Triolo, Allison, & Brown, 2018)
[252] (Liptak, 2020)
[253] (Rühlig & Björk, 2020)

evaluated, and in worst case terminated, as the US has voiced concerns about maintaining security cooperation with countries allowing Huawei into their networks.[254]

But the diplomatic pressures can also be observed from the Chinese side, who recently threatened the strategically important Faroe Islands with worsened trade relations if Huawei was not allowed to supply 5G technology to the island nation.[255] This instance was surprising also because it for the first time hinted at the close ties between the Chinese government and Huawei in an official, diplomatic setting - ties that the Chinese government often in the debate try their best to debunk. As most countries are still undecided on the Huawei issue to date, there are few actual examples to draw from when trying to assess the diplomatic risk of granting - or not granting - Huawei market access. Although we haven't seen the direct diplomatic consequences of a Huawei ban in a European country, it could be useful to briefly look elsewhere to find examples. Another Western country, Australia, has seen the consequences of banning Huawei, when their decision to exclude the Chinese vendor from its markets saw many Chinese harbours banning the import of Australian coal as a direct retaliation.[256] New Zealand, with an otherwise important economic relationship with China, has also seen more turbulence in their bilateral relations after their decision to ban Huawei. [257]

So, while the long-term consequences of excluding or including Huawei are difficult to predict, there seems to be a clear risk of worsened geopolitical and economic relations when misaligning on the policies of China and the US.[258] Just as the discrepancies in resources and regulations, the Huawei debate has highlighted how the differences in individual member states relations to the US and China is causing problems for a common EU approach. The fragmentation in all areas, and the difficulties coordinating 27 member states, is apparent when reviewing the structural risks, and one reason as to why there is a growing discussion on how to accomplish a more unified EU agenda. The next section will go more in-depth on this, and how the notion of increased *EU unity* is needed to stand stronger when the individual member states are drawn in different directions.

5.4.3 Towards a common EU approach and unity

The above sections showcase how internal fragmentation, and perhaps also tensions, arising from economic, regulatory and diplomatic discrepancies play an important role

[254] (Albrycht & Świątkowska, 2019)
[255] (Kruse & Winther, 2019)
[256] (Scott & Murtaugh, 2019)
[257] (Scott & Murtaugh, 2019)
[258] (Lysne, Nagelhus Schia, Gjesvik, Friis, & Elmokashfi, 2019)

for the European Union in the Huawei debate. A theme that becomes apparent in the coding is how the lack of harmonization within telecommunications and other technological policy fields actually restricts the EU's ability to address the various challenges of 5G deployment – technical, industrial and geopolitical. It can all be summarized or put together in the notion that there are calls *for a more unified Europe driven by a coherent strategy*,[259] a unity. Such calls can be observed from European industry actors and experts, but also European policymakers. From the side of the industry, it is deemed that fragmentation is Europe's biggest threat;[260] recognizing that policies aimed at realizing the Digital Single Market, which is one of the ways in which the EU has tried to unify or make the Union's strategy on tech coherent, are far from sufficiently implemented. Related to these are suggestions that novel technologies which are enabled by 5G are not sufficiently reflected in innovation and industrial policy.[261] While policymakers themselves seem to recognize this predicament, unifying member states under a single strategic vision is difficult both in theory and in practice.[262]

While there are efforts to coordinate a common EU approach on digitalization in the union, granted that the industry deem it not sufficient, the matters are complicated by the fact that the tech industry has become increasingly important also for security interests, blurring the lines between industrial and foreign policies. *The foreign policies* of the members states within the union is even more difficult to coordinate than industrial policies, not least spurred on by the deepened divisions that could be observed after the migration crises in the late 2000s and mid-2010s respectively,[263] events that undermined the confidence in an EU unified strategy on foreign matters. The introduction of the investment screening framework in 2019 is an excellent example of how tech policy is now deeply integrated in foreign and security policy, but also an important depiction of the difficulty to find a common EU stance on these issues. The proposal, just as described in subchapter 2.6, aimed to create a procedure in which member states could share their concerns over foreign investments in an individual member state market. Although not explicit, it was a direct reference to the increased Chinese presence in critical infrastructure in Europe. The proposal was highly controversial and displayed large discrepancies and internal struggles between the EU countries.[264]

[259] (Gehrke, 2020)
[260] (van Tetering, 2019)
[261] (van Tetering, 2019)
[262] (European Political Strategy Centre, 2019)
[263] (Lehne, 2020)
[264] (Stearns, 2019)

While the investment screening regulation did pass the parliament in the end, the general foreign policy coordination proves trickier in these times. Although the 5G debate has highlighted how the need for a unified EU approach is key going forward, just like the case on trade policy, it seems that the EU heterogeneity is currently too great with member states being committed to their own strategies on foreign matters. Some experts stress that strong EU leadership could be a way to build trust and confidence in the common project and ambitions, but how there are still inherent structural difficulties in the implementation of national foreign policies parallel to the joint union policy - tying also to the previously mentioned fragmentation both in terms of diplomatic relations and resources. The Huawei debate seems to bring this fragmentation into the spotlight even more than before, perhaps because of the multifaceted nature of the ICT sector. When tech is framed as the geopolitical *"battleground of the future"*,[265] it is no longer just an industry-wide lack of coordination, but an inability to agree on a *joint foreign policy* that affects the EU's influence and power in world politics more broadly. This also connects to a broader discussion on sovereignty and EU autonomy. What competences should the member states transfer to the European Union? And how much unity can be reached without agreement on what the right balance between EU sovereignty and the sovereignty of individual member states. This discussion will be revisited in a later.

The difficulty for the EU to position itself and unite behind a common strategy also stems from a changed geopolitical climate, spilling over into the union and contributing to the increasing tensions and fragmentation between member states. The geopolitical climate has become increasingly divided, with two opposite Great powers pulling in different directions. As previously stated, a common theme in the literature is the framing of the Huawei debate, but also the geopolitical power struggle, as if EU has to *"pick a side"* and either *"go East or go West"*.[266] The EU does not seem interested in being forced to make such a binary choice, with some experts recommending the EU to rather find its own trajectory in the triangular relationship with Washington and Beijing.[267] The geopolitical landscape has however made this harder, as increased division, protectionism, polarization and *"war rhetoric"* are tools the normally multilateral-focused European Union has found difficult to navigate. Nonetheless, regardless of whether the fragmentation is discussed in intra-EU relations or whether it's focused on the geopolitical fragmentation, a unification of the EU partnership seems to stand out as the key

[265] (Triolo, Allison, & Brown, 2018)
[266] (Albrycht & Świątkowska, 2019)
[267] (Gehrke, 2020)

underlying challenge to resolve the structural risks highlighted by the Huawei debate. But in finding a pathway to unity, the EU must also consider the geopolitical reality. Figure 5 summarizes the main findings of chapter 5.4.

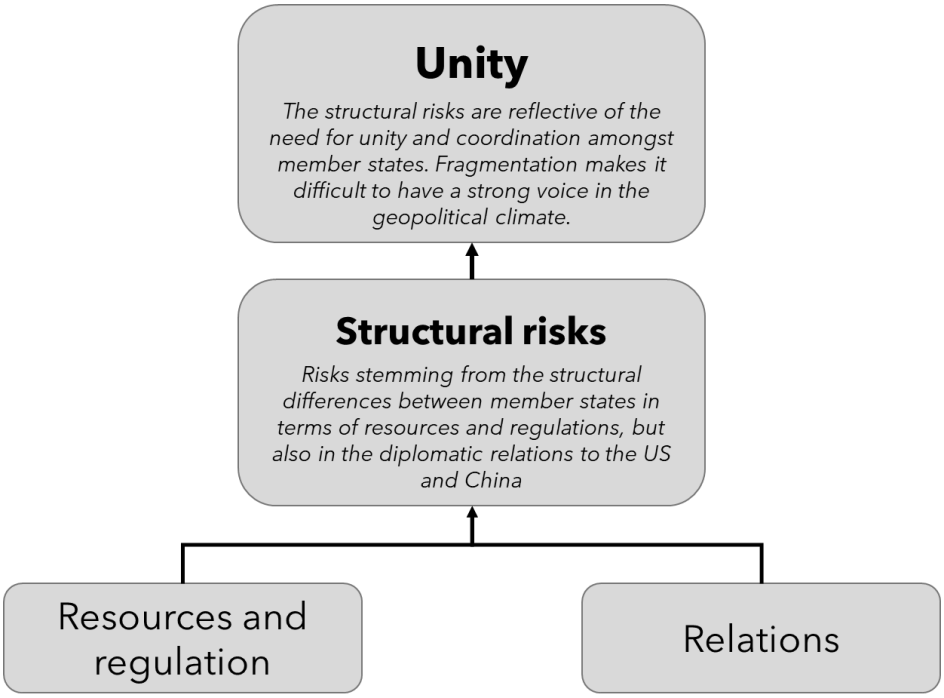


Figure 5. Connecting structural risks to conceptualizations of unity.

5.5 Towards a contingent framework

After a separate and in-depth analysis of the pre-identified categories of risk, going back and forth between the analysis and data, the three more abstract concepts of *trust*, *competitiveness* and *unity* were discovered. Each of the concepts were identified as underlying concerns, challenges and discussions behind the more explicitly framed risks categories of *technological*, *industrial* and *structural* nature. Furthermore, each of the risk categories and their underlying conceptual challenges could be derived from a deeper, more fundamental concern relating to the geopolitical climate. The purpose of this subchapter is two-fold; *Firstly*, the risk categories and underlying concepts will be synthesized into a contingent framework to visualize the different components in a coherent manner. This goal, to create a theoretical and grounded framework to understand the debate around foreign investment in critical infrastructure, has been a clearly stated aim of the paper already from the start. *Secondly*, the analysis will be completed by discussing the ultimate finding that has been derived from the analysis of

this paper - the *geopolitical* aspect that lies behind all the other risks and challenges in the debate. While the geopolitical section is not aiming to provide neither a prediction of how the EU will act on the issue, nor to give recommendations on what EU should do to achieve a better outcome, the intention is rather *to further the understanding of how geopolitical aspects shape the debate and is an important explanation as to why the debate is framed the way it is*.

5.5.1 Unit of analysis and level of abstraction

The framework presented in Figure 5 is two-dimensional, as it separates the *level of abstraction* in the debate, depicted on the y-axis, from the *unit of analysis*, found on the x-axis. As previously outlined, the three risk categories in the framework were identified already in the analysis of the purposive sample of data. Being somewhat practical in nature, explicitly mentioned in much of the literature and without the need for abstract analysis to be categorized, these risks represent the lowest level of abstraction in the framework. While the risks by no means should be thought of as solely objective or unison agreed upon, they are explicitly mentioned as main risks and are thereby also relatively straightforward and hands-on in nature. These risks represent the *micro-level* of abstraction and contrasts to the three underlying concepts, which are not always explicitly mentioned and require a more abstract deductive reasoning to derive. As the underlying concepts are more abstract in nature and require a synthetization of different stakeholder views to be formed, they represent the *meso-level* in the below framework.

Similarly, the *unit of analysis* is depicted along the x-axis. While the bottom left corner concerns the technological risks, all sector-specific in nature, the industrial risks naturally widens the scope of analysis to focus on competitive considerations for the EU businesses. The unit of analysis has thereby been lifted from a specific sector to the whole EU industry. Accordingly, the last category of risk concerns the structural risks stemming from diplomatic relations and the member states differences in resources and capabilities - an inter-state perspective on the debate. Altogether, this creates a two-dimensional framework where the level of abstraction is lifted along the y-axis, from micro to macro level, and the unit of analysis is widened or raised along the x-axis, from sector specific to inter-state, all depicted in the Figure 5 below.

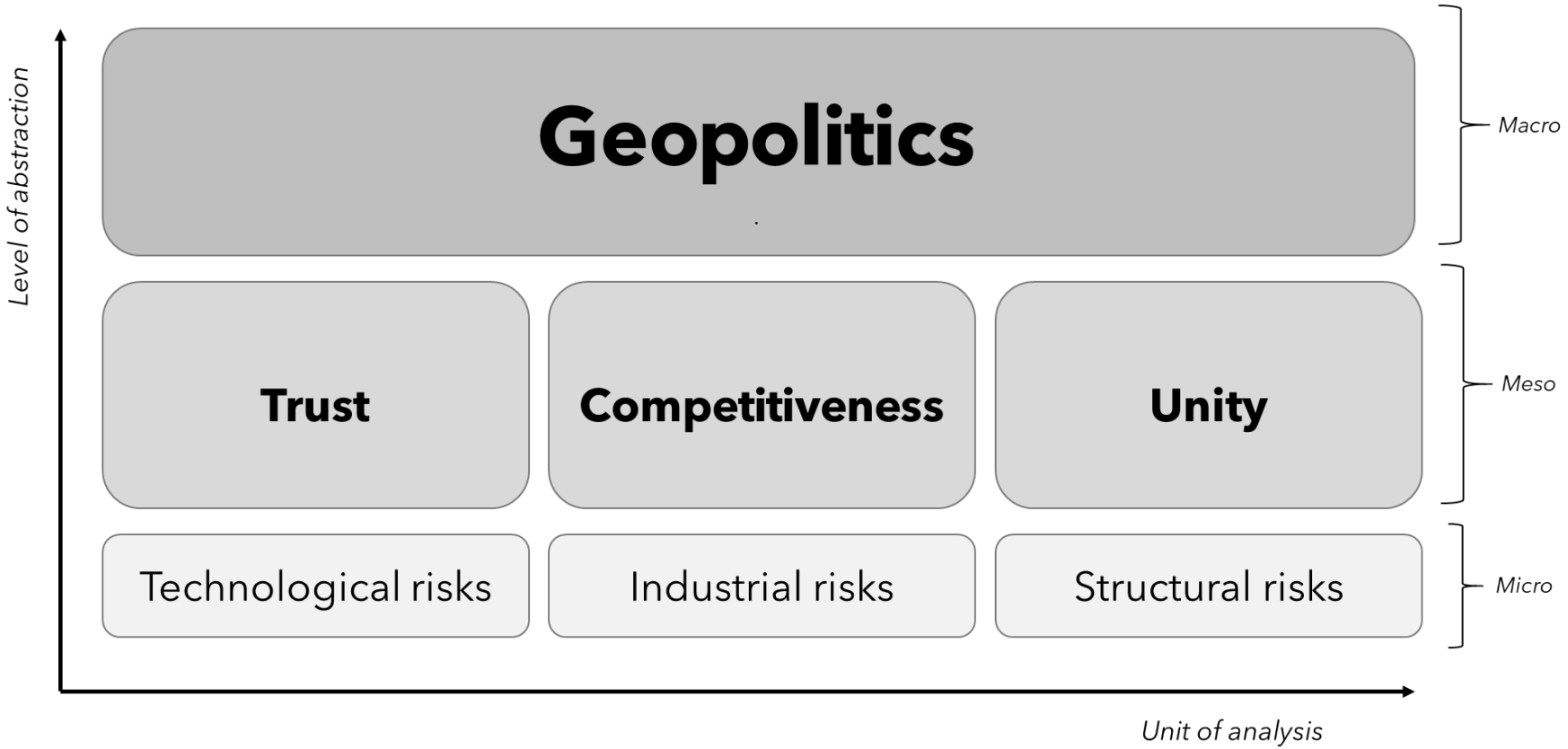


Figure 6. Risks in the Huawei debate along units of analysis and levels of abstraction.

5.6 Meso and macro level linkages

Having mapped both the *micro* and *meso* level discussions of the Huawei debate, it gradually becomes apparent that more or less all of the concerns have a common denominator, joining the three types of risks and the underlying concepts behind them - *geopolitics*. It is simply not possible to isolate any of the three categories without ultimately taking geopolitical considerations into account, as they run as a red thread through all of the analysis, having an impact on the actors' perception of the issue and playing an important role in the actions of the stakeholders. Gradually raising the level of abstraction from meso to macro level in the above framework is thereby a natural progression throughout the analysis, going back and forth between the coding of data and writing memos. Hereafter, a more in-depth analysis of the three meso concepts *trust*, *competitiveness* and *unity* will be provided, including how they respectively link to the macro level geopolitics. Thereafter, focus will be put on a last derived concept from the literature – autonomy – which seem to tie all of the analysis together, linking the different levels and units of analysis together.

5.6.1 The role of trust in geopolitics

The chapter outlining the technical risks identified a number of challenges which relate to 5G deployment in itself, regardless of who provides it. The core of these risks was understood to belong to one of two categories, *virtualization* or *interconnectivity* (see subchapter 5.2). The combination of these categories brought attention to the increased level of complexity inherent to the telecommunications systems, with a higher systemic vulnerability as an inevitable result. As systems will always be characterized by a degree of insecurity and uncertainty, trust needs to be put in the *buyer-vendor relationship*. These discussions – coupled with the unfalsifiability of security claims[268] – lead to the grounded conceptualization of trust as underpinning the debate concerning Huawei. Attention will now first be put on the theoretical dimensions of the trust, to thereafter discuss its role in the geopolitics context which is understood as central to the overarching discussions of Huawei and 5G deployment. Trustworthiness in the Huawei debate is reflected in the two central dilemmas of trust, as suggested by Govier.[269]

Firstly, *trust and vulnerability* are associated with one another - to trust is in a sense to be vulnerable. Theoretically, this association is particularly palpable when reflective of the

[268] (Herley, 2016)

[269] (Govier, 1998)

arguments put forth in the 5G debate. The countless mentions of how 5G is set to enable and transform digital economies and how "complexity is the enemy security" can be derived from notions of societies becoming more inter-connected and vulnerable than previously. This translates into insecurities about the increased vulnerability, and provided that systems never become completely secure, trust must transcend the system to include the provider. As reflected by the Huawei debate, various stakeholders are ill at ease of being that vulnerable towards Huawei and, ultimately, the Chinese state.

The above reasoning segues into the second dilemma of trust as suggested by Govier (1988) reflected in the Huawei debate, which is that *trust is fragile*. It is easy to damage and intrinsically difficult to restore.[270] The framing and type of arguments put forth in the Huawei debate arguably confirms this. The countless allegations of Huawei being used as a vessel for Chinese espionage shows the difficulties of trusting Huawei, provided that China is seemingly not trusted. As such, trust extends beyond the traits and actions of an individual to concern the context which may influence it.[271] The preliminary findings identified how Huawei was used as a common unit of analysis in which broader European woes about China were projected. Similarly, when arguing about the reasons that Huawei cannot be trusted, it is primarily (although not always) rather a matter regarding China than Huawei. As suggested by Mascitelli and Chung[272], that *"[in] the end, Huawei's opportunities and acceptance as a leader in telecommunications will depend on the extent to which some westerns nations are able to separate ideology from commercial interests when dealing with China"*.[273]

Once again widening the discussion from the concept of trust in itself, chapter 5.2 also concluded that the technological risks stemming from the implementation of 5G networks ultimately depends on *trust in the legal and political system of China*,[274] and that the risk assessment of whether a foreign actors, i.e. China, would take advantage of any vulnerabilities in the telecom systems is dependent on geopolitical considerations, rather than the IT security in itself. While the discrepancies between the legal and political system between the EU and China has existed for a long time, it seems to be a particularly sensitive topic as of current - more sensitive than just the inherent sensitivity of doing business with vendors from *"flawed democracies"* without a free and independent judiciary system more generally. Part of this seems to lie in what some experts call the

[270] (Govier, 1998)
[271] (Govier, 1998)
[272] (Mascitelli & Chung, 2019)
[273] (Mascitelli & Chung, 2019)
[274] (Kleinhans, 2019)

strategic mistrust which is seen between China and the Western world today. Although the strategic mistrust, defined as a *"mutual distrust of long-term intentions",*[275] primarily is played out between the US and China at the world stage, this conflict tends to bleed over into EU-China relations as well.

But as the mistrust seems to be more or less institutionalized, and the debate has come to move away from whether or not to ban a specific vendor from European networks, and instead focuses on the battle between political system and the systemic rivalry between China and the Western world, the question is whether overcoming the security concerns will ever be feasible for Huawei. When the product in question, 5G telecommunications networks, are deemed a matter of national security, there will always be a possibility for Western countries to exclude Huawei with reference to security concern - no matter how safe the systems are.[276] The issue will therefore ultimately come down to the approach the EU takes on having a dependency on China, but also how much importance the European Union puts in its own autonomy and the notion of being fully reliant on technological systems stemming from the Western world. Dependency and *autonomy* are, although not always explicitly put, keys in understanding the EU's underlying considerations in the Huawei debate – especially from a geopolitical dimension.

5.6.2 The role of competitiveness in geopolitics

The industrial risks stemming from the Huawei debate led to the identification of some deeper, competitive challenges for the EU in the future development of their industry, but also in its business relations to China. The industrial risks were deemed as reflecting a broader debate on the future competitiveness for the EU industry, a discussion that stretches well beyond the boundaries of the Huawei debate. Addressing questions of lacking reciprocity, government support and an overall unfair business practices were highlighted as keys to achieve this goal in the literature. The theme has clear links to the geopolitical climate of today. As suggested by Albrycht and Świątkowska;

> *"Today, it is obvious that the pillar of power, might, and agency that global actors may have is the technological potential they possess."* [277]

[275] (Mascitelli & Chung, 2019)
[276] (Kleinhans, 2019)
[277] (Albrycht & Świątkowska, 2019)

The global power balances are in a state of change, and the economic growth policies of China, not only in 5G but also in their soft power projections and the pursuit of their global Belt and Road Initiative, is resulting in shifting alliances and a new geopolitical reality. *Novel technology is becoming an important tool for soft power projection*[278] and the 'race for technological leadership' is extended to also entail the possibility of future hard power projection. Ensuring a competitive industry has therefore become understood as vital for the EU not only on economic and innovation grounds, but also to uphold the union's position in the geopolitical order. While the Huawei debate has indeed served as a catalyst for the EU to review its stance on industrial policy, the future competitiveness of the tech sectors expands beyond this specific debate as the industry has potential also for military use and the control of 5G networks gives the opportunity to disrupt network functioning for one's foes.[279] The level of technology has gone from being an industrial and competitive challenge to be a geopolitical concern of power projection. *European competitiveness is therefore in a sense considered a matter of national security*.

The same goes for the calls for increased protectionism and industrial policy on a global scale, as it has come to reflect the current geopolitical climate and China's increasing economic and competitive position. The fact that the EU now for the first time has chosen to simultaneously label China as a "systemic rival" and a "cooperation partner"[280] reflects the growing impatience in EU circles with China's failure to open its markets to European companies in key sectors - and perhaps also how the issue has moved away from just being industrial concerns to rather mirror a broader geopolitical discussion. At the same time, it is indicative of the struggle EU is having in deciding its stance on China. The Huawei debate has thus become a 'battleground' representing all the concerns that have arisen in the last decade when China has gone from being a developing country to the second largest economy in the world. The labelling as a "systemic rival" was not lost in Beijing and seen as a step away from the otherwise soft European position.[281] All of this is clear from the statement sent out by the European Commission. As stated by the European Commission in 2019; *"China can no longer be regarded as a developing country. It is a key global actor and leading technological power. Its increasing presence in the world, including in Europe, should be accompanied by greater responsibilities for*

[278] (Albrycht & Świątkowska, 2019)
[279] (European Political Strategy Centre, 2019)
[280] (European Commission, 2019)
[281] (Brattberg & Le Corre, 2020)

upholding the rules-based international order, as well as greater reciprocity, non-discrimination, and openness of its system."[282]

This is argued to be central to understand why the issue has become so sensitive and politicized in the European Union. It is not only about whether Huawei should or should not be allowed access to European markets from a competitive perspective – it is about how the EU should tackle the risk of being left behind by the Chinese economy and, in turn, risk losing the union's geopolitical power position. While the EU historically has been an advocate of free trade and an open investment climate, the geopolitical trend of increased protectionism and almost a null-sum, mercantilist, approach to international economic relations may be pushing the EU away from its previous positions. Or as put by Gehrke (2020); *"The return of Great Power competition has witnessed trade regulation and state intervention in the economy that is increasingly driven by geopolitical ambition and not strictly by market-oriented calculus*".[283] The Huawei debate therefore indirectly raises questions on how the EU can ensure future technological independency, but also how the union can find a new competitive position in a changing world. Just as in the previous subchapter, the competitive challenges can be captured by the notion of European autonomy. *Autonomy* for the tech industry, but also in pushing China to compete on equal terms.

5.6.3 The role of unity in geopolitics

The notion of European unity was a main takeaway from the literature and seems to be a prerequisite for the EU to find a place in the "new" geopolitical climate that fully reflects its global political power potential. With large differences in resources, capabilities and diplomatic relations to China and the US, this does however pose a challenge for the EU. As some experts argue, the structural changes in the international order require an *"overarching reorientation"* towards tools necessary for defending EU interests, *and "without a strategic frame, the risk of uncoordinated, antagonistic policies is even higher than is already the case"*.[284] The connection to the changed geopolitical climate is clear, and ties to a theme that has been consistent throughout all of the data analysis in this research - *the framing of the EU as caught between two superpowers fighting for world leadership*. The coordination of EU member states is also captured in the quote by Lippert et al. from the German Institute for International and Security Affairs; *"European strategic*

[282] (European Commission, 2019)
[283] (Gehrke, 2020)
[284] (Gehrke, 2020)

action towards China would require a political consensus about European strategic interests there. That would demand a stronger prioritisation of Europe's China policy above and beyond the current foreign policy issues".[285]

Speculative, the difficulties the EU seem to have in *"finding its right place"* in the new geopolitical landscape can be connected to a change in how geopolitics is conducted nowadays. Recent years has seen an increased tendency to use protectionism, harsh rhetoric and seen a withdrawal from international cooperation - perhaps most clearly shown in the global "trade war" that was a continuation of a long-standing US-China conflict over unfair business practices, but perhaps also a reflection of China's rising geopolitical ambitions. *This change away from multilateralism doesn't seem to have benefited the EU*, usually a frontrunner in international cooperation and a strong proponent of international institutions. Some experts are reasoning that the EU needs to bring geopolitics back to the arena where the EU is best equipped to be leading, promoting fair investment, trade and multilateral cooperation.[286] By reverting to these concepts, the EU will have a better chance at influencing the geopolitical discussions and fulfilling its geopolitical power potential.

This also ties to the framing of the issue as a choice between two sides, going East or going West. As EU seems both reluctant and unable to make such a choice, reverting back to its strongest arenas for geopolitical discussions and decisions is sometimes described as a way of finding its own path - becoming a strong "third" voice in what is otherwise framed as a binary power struggle between superpowers.[287] Being able to pursue its own interests instead of reactively responding to an agenda set by the US and China is a theme in the literature, granted that it's sometimes understood between the lines in much of the data collection. Part of the discussion could also be derived from the fact that the EU is losing the United States as an important ally in promoting international cooperation, given the retreat from multilateral institutions seen in recent years from across the Atlantic. Reaching a certain degree of *autonomy* - an independence - is also highlighted as a key in making free choices not affected by political and diplomatic pressures from other states. Just as reasoned in the previous chapters, *autonomy* emerges as a final key concept, and such autonomy require the EU to better unify and coordinate its members states to speak with one voice. If *EU autonomy* was to be

[285] (Lippert, von Ondarza, & Perthes, 2019)
[286] (Gehrke, 2020)
[287] (Lippert, von Ondarza, & Perthes, 2019)

achieved, it would speculative also increase the chances of impact in the current geopolitical climate.

5.7 Closing the circle

5.7.1 European strategic autonomy and sovereignty

Having described how the three meso-concepts of this thesis are tied to geopolitical challenges faced by the EU, to thereafter conclude that *autonomy* emerges as a last theoretical concept of interest, there is reason to take a step back, review the issue as a whole and see how the analysis can be tied together. All of the points made in the analysis, not least those of geopolitical nature, are joined by a common notion of *European autonomy*. This autonomy is an underlying red thread in all of the discussion, reflected in how the EU wants to have a retained, or even increased, autonomy in their *technological* networks, industrial *competitive* decisions and, last but definitely not least, in their *international relations*. Autonomy binds the public discussion of banning Huawei and the broader, inevitable, and almost existential discussion of geopolitical relevance and sovereignty together. It relates to the notion of states power projection, the EU's squeezed position between two superpowers, and the risk of falling behind in areas which the European Union long has considered competitive advantages and proud parts of its identity.

While *autonomy* is indeed brought up in the literature, it is often somewhat hidden in other arguments, and it is not until the whole puzzle has been laid out that autonomy can be properly derived as a concept encapsulating the whole debate. Some experts and scholars do however explicitly mention the term *strategic autonomy*,[288,289] and how the EU's strategy forward depends on how this term has changed in nature. Therefore, this last section analytical section of the thesis will make an attempt to close the circle of the arguments and observations put forward in the research by examining how *European strategic autonomy*, at least to some extent, captures all the anxieties and challenges the EU has been faced with in the Huawei debate on 5G implementation - a debate that has rather come to focus on how EU can ensure its future autonomy in a changing world than the binary choice of allowing a Chinese vendor to provide telecom networks.

Strategic autonomy is not unison defined, but often involves how states can ensure a certain degree of *freedom* or room for manoeuvre, including statements like *"the capacity*

[288] (European Political Strategy Centre, 2019)

[289] (Lippert, von Ondarza, & Perthes, 2019)

of a political entity to pursue its own course in international relations",[290] but also *"the ability to set one's own priorities and make one's own decisions in matters of foreign policy and security, together with the institutional, political and material wherewithal to carry these through – in cooperation with third parties, or if need be alone"*.[291] While definitions differ, the term has previously been tightly linked to defence capabilities and the protection of sovereignty, and the same goes for the occasion when policy documents mention the term – putting focus on EU's capabilities and the need to protect sovereignty. *Strategic autonomy* and *sovereignty* are indeed closely related, but it should be noted that they are not the same - and in some ways strategic autonomy could more be seen as *means to realize sovereignty*.[292]

The expanded understanding of *sovereignty* is another term that, like strategic autonomy, has changed over time, as it traditionally has been characterized by the Westphalian interpretation of sovereignty considering states as the primary units of the international system, whereas strategic autonomy and the realization of sovereignty today also can involve a *collective of states*, such as NATO and the European Union. Sovereignty is a key concept in international relations and political science, and related to states' internal and external *legitimacy*, international recognition and authority and control over a territory – which makes the expanded understanding of sovereignty of particular relevant in this discussion.[293] Interestingly enough, recent years have also seen several countries issue sovereignty claims regarding cyberspace, a further expansion of sovereignty resulting from the modern technologies. There is however no widely accepted and comprehensive cyber sovereignty doctrine in political science yet.

The changed understanding of both strategic autonomy and sovereignty are the important aspects to keep in mind, as this thesis suggest that an expansion of both strategic autonomy and sovereignty is key in understanding the Huawei debate and its complexities. As discussed several times throughout the paper, the importance of technology and the increased reliance on telecommunication networks has expanded the notion of national security. As national security has come to be expanded, the notion of strategic autonomy is also moving away from only concerning defence capabilities to instead include all matters relevant to protect the ability for states to set their own agenda and protect vital interests. In combination with the new, contemporary understanding of sovereignty as a concept that could also be applied to a collection of states, in this case

[290] (European Political Strategy Centre, 2019)
[291] (Lippert, von Ondarza, & Perthes, 2019)
[292] (European Political Strategy Centre, 2019)
[293] (Timmers, 2019)

the European Union, the scene is set for a discussion on how strategic autonomy relates to the Huawei debate and the EU's challenges, today as well as tomorrow.

The notion of protecting European sovereignty and by strategic autonomy has even been mentioned at the highest EU level, with then European Commission President Jean-Claude Juncker addressing it in his 2018 State of the Union speech with the title The Hour of European Sovereignty. In the speech, Juncker argues that the time has come for the EU *"to become more autonomous and live up to our global responsibilities"*, especially in a cybersecurity context. The growing interest in the link between "digital" or "cyber" and strategic autonomy is without doubt spurred by the increased dependency on transformative digital technologies throughout the economy and society, and growth of cyberthreats and incidents this comes with. Some expert even state that cybersecurity threats undoubtfully undermine strategic autonomy.[294] The rising international tensions, especially in the relationships of the West with China, as well as a retreat in a previous American stance on international cooperation, further exacerbate the situation. As put by Lehne (2020); *"This new language of power, strategy, and geopolitics is jarring to many Europeans' ears because it runs counter to the EU's long-held understanding of its place in the world. (…) To a large extent, it was the U.S. security guarantee and global leadership role that afforded the Europeans the luxury of leaving geopolitics behind."* It is argued that the EU needs to take a more active role in the future,[295] reflected in a quote by Angela Merkel in May 2018, stating that:

> *"We Europeans must really take our fate into our own hands."*
>
> - Angela Merkel, May 2018[296]

In December 2018, 18 EU countries jointly stated that the EU "must adapt its trade policy to defend its strategic autonomy", specifically referring to a range of fields including cybersecurity and AI.[297] With this background, widening the understanding of European strategic autonomy and sovereignty, and noting that the terms have been part of the debate also on the highest EU level, we turn to the question of what strategic autonomy actually entails in practice and how it relates to the framework put forward in this thesis.

[294] (Timmers, 2019)
[295] (Lehne, 2020)
[296] (Timmers, 2018)
[297] (Timmers, 2019)

As put by Timmers (2019), the quotes from EU leaders presented above seem to *"articulate a feeling of acute threat to sovereignty and strategic autonomy"*.[298]

The most apparent connection to the framework, seen in the light of realizing strategic autonomy, is that the meso-concepts of this paper *highlight the areas which the European Union need to address in order to shape a strategy for the future aiming to achieve strategic autonomy*, and thereby also increased European sovereignty. The concepts developed in the framework of this thesis can thereby be seen as pillars on which European strategic autonomy is built upon - all important in shaping the future outlook for the European Union. Ensuring trustworthy technological systems, addressing the future competitiveness of the tech industry and attaining unity in the EU project to achieve independence in the relations with the US and China are the main pathways to European strategic autonomy. Although the notion of strategic autonomy emerged as a concept late in the data collection process of this research, it ties neatly to the already developed concepts characterizing the framework of this thesis.

A in important point raised by some experts is how realistic it is for the European Union to even have the ability reach a type of strategic autonomy in the digital age. In reality, the United States and China may very well be the only individual states with sufficient resources to actually achieve strategic autonomy in the key technologies important for future competitiveness and security. This would leave other countries, including the European Union, with no other choice but to build alliances with like-minded parties – even if this goes against the security instincts that would otherwise prevail – to pursue strategic autonomy in the future. This would perhaps also imply giving up some degree of sovereignty for the sake of building partnerships and alliances. This idea ties to the notion of increased interdependency, both with like-minded and not-like-minded countries – and idea that will be explored further in the discussion chapter of this thesis (see chapter 7.5). If full strategic autonomy is unachievable for the European Union, increased interdependencies could be the least risky way forward – despite the counter-intuitive nature of the idea.

5.7.2 The core of the debate

While the notions of European strategic autonomy and the realization of European sovereignty ties fills their role as final concepts that as emerged from the analysis of the

[298] (Timmers, 2019)

debate, it is useful to use this final section of the analysis to also address how well the analysis succeeds in providing an answer to the research question of the paper. The aim of the thesis, as stated in the first chapter, is to provide an increased understanding of the Huawei debate from the perspective of the European union. Breaking down the components and forming a framework is an approach to better understand how the different concerns and risk relate to each other, but also serve to provide an academic account of the full context surrounding the debate. While European strategic autonomy indeed has emerged as the most abstract, underlying concept in the analysis – it can be argued that the term does not sufficiently answer the research question of this thesis. Phrasing it as "realizing European strategic autonomy" improves the situation, as this indeed could be a way of answering the research question and provide an explanation to "What the underlying challenges" of the debate faced by the European Union.

It is important to recognise that realizing strategic autonomy is not an end goal. It is rather a means to achieve a European sovereignty, which also deemed to be at the core of the debate. The Huawei debate has thus come to concern the European Union's role in a changing world and to represent anxieties over its role, cooperation, and existence. These concerns are not evident from current accounts of the discussion of Huawei and 5G implementation. While the thesis does provide a more nuanced understanding of the different aspects and perspectives of the stakeholders in the debate, it has no intentions to provide recommendations or a prediction of outcome. Indeed, the thesis probably raises more questions than it provides answers. Instead, the framework of this thesis is intended to provide a better understanding of why the debate has become so fierce, and what the risks mentioned in the debate actually stems from.

As will be stated again the chapter 7, the research encourages further research on the more abstract and fundamental question the Huawei debate poses for the European Union. Without going into a deeper discussion, it is interesting to briefly touch upon what increased European autonomy and, in turn, sovereignty would mean for the collection of 27 member states. Because while this paper mainly views the European Union as its unit of analysis, the question of European sovereignty also raises question on the sovereignty member states give up to the union. The Huawei debate, with its greater implications and broadened discussions put forward in this paper, has come to concern the very basis of European cooperation and how much sovereignty that should be transferred to the union. Whether it regards trust in China, the decision to welcome Chinese investments into the home market, the differences in regulation and market conditions or the

diplomatic ties to China and the US, it comes down to how much power the European Union itself should have over these issues.

How much power are the member states ready to transfer to the Union, thereby giving up parts of their individual sovereignty? Given that the tone and sense of EU unity has changed over time, and in recent years seen a clear decline, it is no wonder that the Huawei debate has become so intrinsically complex. It is an amalgamation of all the various, highly contested concerns facing the union. But more than anything, it questions the boundaries of European cooperation. These questions are, however interesting and complex, left for the discussion part for his paper though and, perhaps even more so, for another academic publication to explore. The analysis is therefore concluded by stating that the risks and challenges facing the European Union from the Huawei debate widely transcends the boundaries of 5G implementation, and ultimately comes down to almost existential question of cooperation, autonomy, sovereignty and future relevance. This also represents the main finding of this thesis, bringing order to an otherwise fragmented and simplified debate.

6. CONCLUSION

The debate on whether to ban Huawei in the European roll-out of 5G networks is truly complex. In an attempt to address the argued lack of nuance and oversimplification that has come to characterize the debate as of recent, this thesis has analysed a large number of policy documents, government reports, EU publications, think tank reports, news articles and white papers in an attempt to break down the risks and underlying challenges facing the EU in the Huawei debate. Using a grounded theory approach, the data has been coded and analysed with an open mind to avoid preconceptions and gradually increase the understanding of the issue. The result of the analysis was a comprehensive framework outlining the main risks and underlying challenges identified in the debate. The framework that was developed allowed the research to approach the issue along two dimensions, charting the issue by separating both the level of abstraction and the unit of analysis. Three main risks categories were identified, each representing a specific aspect of the Huawei and 5G debate; *(I) Technical risks; (II) Industrial risks and (III) Structural risks*.

* *The technical risks* largely stemmed from the introduction of 5G technology itself. The roll-out of a new generation of mobile telecommunications networks presents several challenges inherent to the technological solutions that have caused some concern in the debate. As the cybersecurity of 5G networks is understood to be insufficient in deeming networks completely secure, the assessment of the technical risks was connected to the *trustworthiness* of the company providing the networks. Trust not only in the vendor itself, but also in China and its legal and political system, enabling the individual vendor to take its government to court if needed, emerged as an underlying challenge.

* *The industrial risks* discussed the competitive concerns associated with either allowing or not allowing Huawei market access in the European Union. Banning Huawei would come with a delay in the 5G roll-out, increased economic costs and the risk of reciprocal punishment from China - most likely translated into decreased market access. On the other hand, not banning Huawei would run the risk of European vendors being pushed out of the market due the strong competition Huawei offers. Concerns that Huawei is not competing on equal terms, receiving government backing and benefiting from other unfair business practices, are however raised. Ensuring future *competitiveness* of the European Union emerged as an underlying challenge.

* *The structural risks* highlight how the discrepancies in between the European Union's member states, both in terms of resources and regulatory environments, leads to an uncoordinated approach. Equally important is the differences in the member states diplomatic relations to China and the US has an important effect on the decision to ban or not ban Huawei from the EU. The need for *EU unity* between the 27 member states emerged as an underlying challenge behind the structural risks.

The underlying challenges *trust*, *competitiveness* and *unity*, where thereafter conceptualized and further examined to increase the understanding of how they affected the European Union and its role in the Huawei and 5G debate. A summary of the challenges can be found below, all joined by their clear link to geopolitics.

* *Trust* in the vendor providing the 5G networks is key, and the lack of trust in China and its political and legal system is the root to scepticism about Huawei. As there seem to be a *strategic mistrust* between the Western world and China, inherent to the relations, and since national security claims can always be used against Chinese vendors due to the technical interconnectedness of our future societies, it is doubtful that Huawei will ever be trusted without political will. The lack of trust seems to rather reflect geopolitical considerations than allowing a specific vendor in 5G networks, and the EU's pursuit of independence and technological *autonomy* emerges as the key to understanding the issue.

* The Huawei debate has highlighted broader questions on how to ensure European competitiveness, both in not falling behind in the own tech sector and in how to handle the industrial relationship with China going forward. In a world where technological development may determine both soft and hard power, a competitive tech sector is crucial. So are the future relations with China, where the EU is struggling to handle the country's transition from a developing economy to a developed superpower. The Huawei debate therefore indirectly raises questions on how the EU can ensure future technological independency, but also how the union can find a new competitive position – challenges captured by the notion of European autonomy. *Autonomy* for the tech industry, but also in pushing China to compete on equal terms.

* Coordinating the 27 member states and finding a sense of EU unity is key to become a strong voice in a geopolitical climate where two superpowers are battling for dominance. Being able to pursue its own interests instead of reactively responding to an agenda set by the US and China, not affected by political and diplomatic pressures, is a question of *autonomy* – and such autonomy require the EU to better unify and coordinate the discrepancies among its member states.

As evident, all the challenges above are linked by its geopolitical nature and the notion of European autonomy. The final chapter of the thesis connected this to the concept of strategic autonomy, as a way of achieving EU sovereignty. The Huawei debate has come to reflect a number of broader concerns, anxieties and woes about the EU project and its role in a geopolitical climate characterized by changing power structures – stretching far beyond the binary decision of allowing a Chinese vendor market access or not. By breaking down the debate into its components, most notably the notion of national security, and forming a framework has enabled a better understanding of how the different concerns and risk of the Huawei and 5G debate relate to each other, but also provided an academic account of the full context surrounding the debate. The Huawei debate has since long expanded beyond the scope of 5G implementation, and instead put focus on the future of the European Union. That is also the context in which the highly politicized discussion should be understood.

7. DISCUSSION

7.1 Reader's guide

This chapter gives an opportunity to discuss the topics of the thesis in a broader context, as well as providing some additional points tying to the research design outlined in the paper. The first subchapter discusses the overall relevance of the thesis and its contribution to the field of research, but also how the findings can be used also in future discussions of similar nature. Thereafter, a couple of methodological considerations are discussed in more detailed, mainly relating to the collection of data. This is followed by broader discussions of a number of key concepts found in the analysis, namely *national security*, *dependency*, *autonomy* and *sovereignty*. The discussion of the latter two concepts are a direct continuation of the last chapter of the analysis. Lastly, subchapter 7.7 outline some of the motivations behind the choice of research topic and a number of interesting areas for future research.

7.2 Putting the thesis in perspective

7.2.1 The Relevance of the thesis

A starting point for the whole research process was the lack of nuance and granularity in the framing of the issue as depicted in the public debate. This concern was to some extent also present when studying the topic more in-depth, and national security was still widely used as the main explanatory variable for a much more complicated debate. Therefore, the aim to break down the otherwise so simplified issue was a main goal of this research. It also ties to the relevance of the thesis, as it - to our knowledge - is the most comprehensive academic product on the issue. The relevance of this paper is further enhanced by the fact that the issue has emerged very recently, and that the discussion in many countries has been peaking during the writing of this thesis. While it made the evaluation of different strategies and the assessment of the actions by the stakeholders difficult, it also enabled the research to be highly topical. The thesis aims not only to break down the debate in more granular elements, but also to go beyond the explicit problematization to discuss underlying concerns, challenges and factors that contribute to the overall complexity.

7.2.2 The relevance of the concepts

Despite a thorough data collection process and analysis of over XXX number of pages, this thesis by no means claim to give an exhaustive or complete account of all the detailed aspects highlighted in the Huawei debate. There is an almost infinite number of factors contributing to the complexity of the issue, and an equal amount of interpretations by the expert writing the literature on the topic. This paper does however aim to give a more comprehensive understanding of the underlying challenges the European Union are facing and that have become evident through the Huawei debate. Some of the challenges stem from the 5G deployment in itself, while some rather can be derived from other factors - but have become apparent in light of the Huawei debate.

The framework presented in the thesis takes a starting point in practical risks relatively specific to the Huawei debate, but as the underlying, more conceptual challenges facing the EU are discovered and developed in the paper, the framework also becomes increasingly useful for foreign investments in critical EU infrastructure more generally. This is particularly interesting considering how the discussion on Chinese investments in strategically important EU sectors most likely will expand to other areas in the coming years, with some of them already becoming part of the debate, such as *artificial intelligence* and *smart cities* to name a few other novel technologies that have emerged as areas of interest from the data collection process. These sectors will likely see similar discussions and dynamics as the Huawei debate, and the framework could therefore relatively seamlessly be adapted to also understand closely related debates of market access for Chinese vendors.

As mentioned earlier in the analysis, the paper does neither aim to predict the outcome of the debate, nor provide recommendations for the European Union, despite its mapping and conceptualizing the issue at hand. It should rather be seen as the to date most comprehensive effort to explain and understand the EU's considerations in the Huawei debate. Linking the Huawei debate to underlying questions of geopolitics is, at least after a brief literature review, by no means a unique conclusion. At the same time, transforming explicit risks into somewhat concrete concepts that fuel the whole debate, only to thereafter provide clear links to different aspects to the geopolitical stumbling blocks of today, is a contribution to an otherwise less colourful body of literature. But while the thesis hopefully brings some new insights to the discussion, it also raises new question

- perhaps most obvious on how the EU should tackle its geopolitical future in the time going forward.

7.3 Methodological considerations

7.3.1 Data gathering

The data gathering process has been a vital part in enabling the thorough analysis this research is built upon, and a wide range of sources is key in achieving a nuanced and comprehensive understanding of all stakeholder stances. While the research has indeed used a variety of different types of documents, including academic reports, policy documents, news articles, think tank reports and white papers by businesses, a typical grounded theory study also often involve a number of interviews. Part of this can be explained by the fact that the method stems from studies in sociology, an academic field where interviews are a natural part of the research design. With that said, interviews are undoubtedly also a useful source in data collection for studies conducted in the field of business, politics and international relations and would most likely be a valuable addition also to this paper given its intrinsic complexity and many different stakeholders. By including interviews with for example European telecom companies or EU policy makers, there could be additional layers to add to an already comprehensive and analytical discussion on Huawei and Chinese infrastructure investments. While interviews were indeed part of the initial research design, two main factors contributed to the decision to ultimately exclude them in the final design:

1. One of the most interesting aspects of the research topic, the fact that the issues are very topical and urgent, was also a liability in securing and scheduling the interviews. Many of the stakeholders that could have given an insight into how the reasoning behind the public debate surrounding Huawei, primarily the European telecom vendors, indicated that the topic was simply too sensitive to discuss on record.

2. In addition to the above points, the covid-19 outbreak in the first half of 2020 made the process of finding relevant stakeholders to interview substantially more difficult. Not only was the practical ability to perform the interviews complicated, the relevant stakeholders were also, quite understandably so, focused on other matters than being available for interviews in a crisis situation.

While interviews could have been a good addition, the indications that was received about the sensitivity of the situation might show that these potential interview subjects

would be restrictive in the information they could provide even if such interviews were to be included in the paper. In addition, several steps have been taken to ensure that the full spectrum of stances, opinions and interests have been included in the report by analysing a variety of different types of sources. To base the analysis on different types of documents coming from the full range of stakeholders with differing angles and takes on the issue is a standard approach in grounded theory to assure that the data is of quality and represents all actors and nuances.

7.3.2 Purposive sampling and preconceptions

Another methodological consideration worth mentioning is the use of a purposive, initial sample of data. While it by no means is uncommon practice in grounded theory to choose an initial selection of data, just as described in subchapter 3.3.2, the choice of sources for this data is important to address since it guides the subsequent coding and can steer the research project in a specific direction. As no coding is done before the pre-selection of data and researchers usually have a relatively good knowledge of the topic at hand, the is a risk that preconceptions could play a role in the selection of initial data, and thereby also shape the rest of the research. Being humble and very aware of this risk, we believe that the good knowledge of the material and issue rather served as an asset than a liability in the data collection. By already knowing the vast number of stakeholders and the many perspectives held by these, the previous knowledge could be a great guide to actually focus on the right set of sources for the purposive sample, just as an awareness of the complexity of the issue can make the purposive sample better equipped to map out the full range of angles.

7.3.3 Unit of analysis and European focus

At some point in the research process, a choice had to be made on what actor to put the main emphasis on. As the complexities stemming from coordinating 27 individual member states and the inherent internal struggles that arise from this situation was a main motivation behind the choice of research topic, an EU perspective was a natural starting point. In addition, the difficulty of data access from primary Chinese sources would have substantially increased the depth of the analysis of the Chinese standpoint. With this said, and despite the apparent overweight of Euro-centric literature in the data collection, the researchers have attempted to remain as objective as possible in the view of the discussion to not play into the other ways so binary framing of the debate. Future research

is indeed encouraged to give a better understanding of the Chinese account of the debate.

A brief additional point on the unit of analysis would be to mention how the terms European Union and "European" often is used somewhat interchangeably in the thesis. While the European Union indeed is the primary unit of analysis, the is a natural overlap with the interests of Europe. The same goes for the *EU and European markets*. This has also led to the mentioning of the United Kingdom as an example to make points in specific sections of the thesis. The researchers acknowledge the difference between the European Union's interests and European interests but deem the distinction somewhat negligible on the occasions when the terms are used interchangeably.

7.4 The use of national security

The inclusion of the term national security has been rather peculiar throughout the research process. On the one hand, national security concern is the perhaps most consistent argument raised in substantially all documents discussing the Huawei debate, an it's more or less impossible not to give the term a somewhat central role in understanding the issue as it is framed by the stakeholders. On the other hand, the very framing of the issue as a national security concern could be a main issue in the whole debate, contributing to the *lack of nuance* and black-and-white framing that characterizes the public discussion. For these reasons, it is worth spending some extra time explaining how the use of national security affects the debate.

As stated, there is perhaps no other term, wording or framing that occurs as frequently across all the studied documents to describe the issue of foreign vendors supplying critical telecom infrastructure as national security. Despite this, there is a surprising lack of definition of the concept in the literature. The lack of definition could arguably be a reason that the term is used so frequently, as the demands to justify its use naturally is lower without a common understanding of what it entails. Speculative, there are a number of reasons why national security is so seldom defined. One factor to take into consideration is that policymakers might be incentivized not to provide a clearer definition, as it would force them to address much more complex questions transcending several areas and spheres of responsibility, adding to the already complicated picture, when these topics are discussed. National security could then be a way of avoiding the complexity, harsher put, a way of *"hiding"*, from the intrinsic, multi-layered nature of the Huawei debate.

But a perhaps even more intuitive reason for the lack of definition of national security in the debate is the changed nature of national security as a concept in itself. As our societies have become increasingly dependent on technology and the networks enabling new types of mobile communication, the definition of critical infrastructure has widened. As critical infrastructure, just as the name suggests, is a vital part in a functioning society, it has historically also been considered a matter of national security. With the introduction of 5G, societies are becoming more dependent than ever before on technological solutions, making the debate about foreign vendors in such technology increasingly sensitive. But in contrast to the introduction of previous generations of telecommunications networks, which undoubtedly also could be categorized as critical infrastructure, 5G technology will take the technological dependency in society to a new, unprecedented level. By becoming the pinnacle of our modern societies, the discussion has shifted and widened to not only concern the most immediate security aspects of the networks themselves, but rather to include all aspects of the value chain and even the home country of the vendors. As almost everything in society will depend on 5G, everything relating to 5G can be labelled national security.

This in turn has two main consequences. Firstly, it implies that Chinese vendors could always be excluded from any part of the value chain in 5G technology due to national security concern - no matter what they do to prevent exclusion. This is also raised as an important part of the analysis (see subchapter 5.2 and 5.6.1). If the political will is to exclude Chinese vendors for critical infrastructure, the extended understanding of national security will always provide a somewhat legitimate justification to do so. The discussion links back to both chapter 5.2 and gives an increased understanding of how the use national security as a term in the debate in itself affects the possibilities from Chinese market inclusion. Secondly, the fact that everything can be labelled as national security does, as stated several times by now, lead to a lack of nuance in the debate. In many ways, the very creation of the framework in this paper shows the lack of nuance in the public debate. Instead of referring to the inclusion of Huawei on European markets as a national security concern, the breaking down of the actual risks and underlying concerns in itself shows how the public debate lacks nuance as all the considerations and concerns in the framework often is captured by the single use of national security concerns. This also explains why national security, although the perhaps most frequently used term in the literature, is used sparsely in the analysis of this paper. The relation can be shown in the slightly edited version of the framework below:

7.5 Widened understanding of dependency

In all of the arguments of the analysis chapter linking meso and macro levels together, it becomes evident that the level of dependency - not only on Huawei but on China - is a key variable. Approaching the issue from the notion of trust, the debate seems to revolve around how the EU can choose to either become less dependent or more dependent on Chinese technology, and how that choice depends on the trust put in the legal and political system. As the technological risks can never be fully assessed and there seems to be what some experts label as *strategic mistrust* between the Western world and China, it is questionable whether it will ever be possible to include Chinese vendors in the EU market in strategically important sectors if the inclusion is solely based on trust in the Chinese legal and political system, just as discussed in subchapter 5.6.1. Further underscoring the point, it is unlikely, to say the least, that the Chinese political and legal system will change in the near future. Given these circumstances, it can be argued that the framing of the issue - often picturing the dilemma as a choice between *being dependent but unsafe or being independent but safe*, is not fully capturing how the dependency actually affects the stakeholders. Just as the rest of the debate, the understanding is binary, too simplified and lacks nuance.

Instead, dependency - or perhaps rather interdependency - could be seen as a rare way of circumventing the trust issues between China and the Western states. As trust is unlikely to appear in the current geopolitical climate, EU states need to find a way to still interact with China. An increased interdependence between the EU and China should not only be seen as an increased risk, but also as a method to *mitigate the risk*. The more China is invested in the EU's economical, technical and political projects, the higher the cost becomes of betraying this relation. With a disconnected EU, fully independent on Chinese vendors and technology, the risks for the Chinese state to ever spy or sabotage for the European Union can be argued to become higher as there is less of a developed relation to tear apart. With a more interdependent relation however, the costs would become exponentially higher.

This line of reasoning may sound counter-intuitive at first but build on a number of premises. The first is that, as argued in chapter 5.2.3, the Chinese state would likely be able to both spy and sabotage for the EU regardless of whether they have a Chinese vendor involved in the European 5G roll-out. Secondly, an increased interconnectedness would imply that the EU also were able to have a reciprocal relationship with China, both

in terms of market aspects and in terms of geopolitical outlook, the latter of which is a major speedbump. Thirdly, it hinges on whether the EU can accept having China as a strategic "partner" overall, given the systemic differences between the parties. There are core differences in areas such as political rule, transparency, democracy and human rights that the EU had increasingly difficult to overlook. At the same time, an increased interdependence could make China more willing to adapt to the EU's positions on other issues.

The interpretation of interdependency can also play a role in the debate when approached from the notion of autonomy. Autonomy, conceptualized and developed into strategic autonomy in the last part of the analysis of this paper, is more or less a direct expression of *independence*. The literature highlights how European autonomy is important on the one hand to ensure that the EU has the industrial capabilities to be competitive in the future, but also to protect itself from the rapidly changing competitive landscape in which China is competing on unequal terms. By becoming more autonomous, a term that easily can be interchanged with "less dependent on China", the debate is once again lacking nuance in the framing of the issue, especially in its interpretation of dependency. Less industrial dependency, also expressed as more autonomy, seems to be a way to counter China's unfair business practices and protect the future EU industry. While the literature indeed lift some of the negative consequences of excluding Huawei from the market in terms of technological setbacks and increased costs, there seems to be a notion implying that leaving China out of the market, becoming independent, is the way for the EU to find its new competitive position in a new, globalized industrial climate where Chinese domination is a looming challenge.

While the protectionist notions or streams should come as no surprise in the geopolitical climate of today, the effect may be the opposite of what's intended. Technological and industrial independency, shutting Chinese vendors out of the European and Western market, could according to some experts eventually lead to two completely separate technological systems. China has already increased their efforts to become independent, and these efforts would likely not slow down if China is shut out from the EU. A decoupling of the markets would therefore not benefit the EU. Instead, in the increasingly intense chase of independence and a desire to be better equipped to compete with China, the result may just end up being that China becomes fully independent themselves - which in turn increases their competitive advantage and the geopolitical division. Interdependence should therefore not just be understood as a complication for European

industry. A controlled interdependence could instead be seen as a key in ensuring that the EU will not fall further behind in the quest for short term gains.

Lastly, the discussion of structural risks and EU unity could also benefit from a more holistic understanding on interdependency as a concept. As discussed in the previous subchapter, the European Union is struggling to adapt to a changed geopolitical climate and become a strong "third" voice in the contemporary powers struggle between the US and China. Part of the reason was speculated to be derived from the fact that the geopolitical discussion has moved away from multilateralism and international cooperation, areas where the European Union usually is a strong proponent for. European unity is seen as a way to strengthen the EU positions, as a common approach is required to retain a strong global position. But this may also mean getting back to the old channels of international politics, strengthening multilateral forums and avoiding conflict with the superpowers instead of seeking it. As put by Gercher, the EU's ability to maintain open trade and investment, a global level playing field and non-confrontational relations with the US and China are some of the factors that could help in fulfilling the EU's geopolitical potential. Increasing interdependencies by *"reverting back"* to multilateralism and open trade and investments is perhaps EU's best way to achieve a stronger position, not by following suit with the superpowers and getting caught up in proving their power by taking harsh, protectionist measures.

7.6 Sovereignty and EU strategic autonomy

As discussed in the final subchapter of the analysis of this paper, covering the concept of autonomy and sovereignty, the Huawei debate has revealed some deeper considerations that the European Union need to tackle for the future. This dos not only regard ow to ensure sovereignty for the union as a whole, but also the relationships between individual member states and how much sovereignty each of the 27 states are to give up to the European Union. While the analysis chapter deemed this discussion outside the scope of this paper, mainly because it goes beyond answering the research question of the thesis, this section allows for a brief return to the topic. As put earlier, the Huawei debate has come to concern the very basis of European cooperation with its greater implications and broadened discussions that has been mapped out in this paper. The question of how much power the individual member states are ready to transfer to the Union is closely linked to that of European strategic autonomy.

Given that the tone and feeling of EU unity has changed over time, and in recent years seen a clear decline, it is no wonder that the Huawei debate has become so intrinsically complex. It is a melting pot of all the various contested concerns facing the union. But more than anything, it questions the boundaries of European cooperation. It reveals splits within the union, for example between the German-French core and a number of Eastern states questioning the legitimacy of increased cooperation. To some extent, Brexit is the most obvious example of how the EU cooperation was considered to be reaching beyond its legitimacy even before the Huawei debate. Before Brexit, the EU cooperation has been able to handle these issues. As put by SWP; *"The (Western) European striving for self-assertion and self-determination under conditions of structural bipolarity was an important driving force in the founding of the European Communities"*. While the Brexit referendum and, to some extent, the actions of the Trump administration has intensified the notion of European unity, there are still as many views on EU cooperation as there are member states. And even though the US withdrawal from its previous commitments on the international scene may have increased EU friendly sentiments, one shouldn't underestimate the almost existential crisis it may have put the EU in, *now missing its most powerful Western ally in international affairs*.

One last factor adding another layer of complexity is the very nature of the Huawei debate and the questions it raises about European cooperation. As stated several times throughout the thesis, critical infrastructure has come to be a matter of national security and, in turn, bordering defence strategy. As the EU project started as a defence cooperation, to then widen its scope to the point where some member states today feel they have given up too much sovereignty in too many areas, the Huawei debate turns this logic upside down. In a future where national security and defence strategy has come to entail also a lot more than just military capabilities due to the increased technical interdependence in society, it makes the question of what areas EU should have exclusive competence even more difficult. Future studies into these areas are however encouraged, both from an interdisciplinary perspective and from a strictly political science point of view.

7.7 Future research

The multifaceted nature of this thesis and the dynamics outlined present various opportunities and directions for future research. Reflective of the general conclusions of this thesis, worthwhile insights may come from addressing similar questions as those of

interest here, but from different perspectives. Some fruitful routes of inquiry are outlined below. First, the highly current and speculative nature of this thesis makes a follow-up study in itself interesting, assessing how differences in stance amongst member states affects led to differences in outcomes in 5G deployment, for example. Of similar interest would be to change the unit of analysis from that of the European Union to an individual member state. While this thesis has argued that the highly complex nature of the debate is most evident from a pan-European perspective, homing in on a single or small sample of member states may provide to see some of these dynamics 'on the ground'. This may provide interesting accounts of how dependencies in legacy telecommunication networks, diplomatic relations and other factors create tensions and differences in outcomes and stances. Process tracing and similar types of within-case analysis may produce interesting insights which add substance and credence to those outlined here.

Equally interesting are inquiries which explores European governance in novel technologies. This thesis has outlined how differences in resources, regulation and relations exacerbated challenges of producing a coordinated approach with regards to 5G deployment and the Huawei debate (see subchapter 5.4). While this translates into an indirect discussion on means and modes of governance in the case of 5G, more direct explorations are truly worthwhile. As suggested throughout this thesis, the Huawei debate will likely not be unique but rather indicative of more fundamental challenges which the EU faces which will resurface in similar contexts. As such, explorations of European governance in areas such as AI or smart grid technologies may produce of how these emergent areas may be better governed.

Lastly, and potentially most interesting, are inquiries which pick up where this thesis leaves of. One of the central points of this thesis is that the Huawei debate can be seen as reflective of concerns of European sovereignty and strategic autonomy and their interactions. The topic of EU fragmentation and the discussion on the boundaries of EU's exclusive competence is by no means a new area of study, and has for example been studied quite extensively when in light of EU's common trade policy, Nonetheless, the main findings of this paper – linking the Huawei debate to questions of European autonomy and future cooperation - would be an interesting topic to further examine. And as stated previously, the discussion on EU's future relevance and existence does neither start nor stop with the Huawei debate.

Bibliography

European Commission. (2018, June 6). *Digital Single Market: Political agreement on the rules shaping the telecommunication markets in the 5G era*. Retrieved from European Commission: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_4084

5G Observatory. (2020, 01 10). *National 5G Spectrum Assignment*. Retrieved from European 5G Observatory: https://5gobservatory.eu/5g-spectrum/national-5g-spectrum-assignment/

Ahrens, N. (2013). *China's Competitiveness: Myth, Reality, and Lessons for the United States and Japan*. Washington : Center for Strategic and International Studies.

Albrycht, I., & Świątkowska, J. (2019). *The Future of 5G or Quo Vadis, Europe?* Krakow: The Kosciuszko Institute.

Barzic, G. (2019, June 2019). *Europe's 5G to cost $62 billion more if Chinese vendors banned: telcos*. Retrieved from Reuters: https://www.reuters.com/article/us-huawei-europe-gsma/europes-5g-to-cost-62-billion-more-if-chinese-vendors-banned-industry-idUSKCN1T80Y3

Bass, D. (2019, September 8). *Microsoft Says Trump Is Treating Huawei Unfairly*. Retrieved from Bloomberg: https://www.bloomberg.com/news/articles/2019-09-08/microsoft-says-trump-is-treating-huawei-unfairly

BBC. (2019, April 20). *How much of Europe does China own?* Retrieved from BBC News: https://www.bbc.com/news/world-47886902

BBC. (2019, March 21). *Huawei ban would delay 5G rollout: Three*. Retrieved from BBC: https://www.bbc.com/news/technology-47482140

BBC. (2019, January 15). *Huawei founder Ren Zhengfei denies firm poses spying risk*. Retrieved from BBC News: https://www.bbc.com/news/technology-46875747

Bekkers, R., Verspagen, B., & Smits, J. (2002). Intellectual property rights and standardization: the Case of GSM. *Telecommunications Policy, 26*, 171-188. doi:10.1016/S0308-5961(02)00007-1

Bloomberg. (2018, April 17). *The U.S. Has Banned Chinese Telecoms Firm ZTE From Buying American Tech for Seven Years*. Retrieved from Fortune: https://fortune.com/2018/04/17/zte-american-tech-ban-sanctions/

Brattberg, E., & Le Corre, P. (2020, February 19). *The EU and China in 2020: More Competition Ahead*. Retrieved from Carnegie Endowment for International Peace: https://carnegieendowment.org/2020/02/19/eu-and-china-in-2020-more-competition-ahead-pub-81096

Bryan-Low, C., Packham, C., Lague, D., Stecklow, S., & Stubbs, J. (2019, May 21). *Special report - Hobbling Huawei: Inside the U.S. war on China's tech giant*. Retrieved from Reuters: https://www.reuters.com/article/us-huawei-usa-5g-specialreport/special-report-hobbling-huawei-inside-the-u-s-war-on-chinas-tech-giant-idUSKCN1SR1EU

Bryant, A., & Charmaz, K. (2010). *The SAGE Handbook of Grounded Theory*. SAGE Publications Ltd .

Burton, R. (1932). *The Anatomy of Melancholy*. London: Dent.

Campbell, K., Cruz, L., Flanagan, B., Morelli, B., Téral, S., & Watson, J. (2019). *The 5G Economy*. London: IHS Markit.

Cave, M., Genakos, C., & Valletti, T. (2019). The European Framework for Regulating Telecommunications: A 25-year Apprasial. *Review of Industrial Organization, 55*, 47-62. doi:10.1007/s11151-019-09686-6

Cellan-Jones, R. (2019, March 7). *Vodafone: Huawei ban will set back 5G*. Retrieved from BBC : https://www.bbc.com/news/technology-47482140

Chaffin, J. (2013, January 31). *EU faces up to China over 'mother of all cases'*. Retrieved from Financial Times: https://www.ft.com/content/e4edbcca-6bab-11e2-8c62-00144feab49a

Charmaz, K. (2006). *Constructing Grounded Theory: A Practical Guide Through Qualitative Analysis* (1st ed.). London: SAGE Publications.

Claici, A., Kastberg Nielsen, C., Geradin, D., Huhn, K., Haag Theilgaard, C., Nordström, D., & Basalisco, B. (2017). Review of the SMP Guidelines. Copenhagen. Retrieved from https://www.copenhageneconomics.com/dyn/resources/Publication/publicationPDF/1/471/1548342153/copenhagen-economics-review-of-the-smp-guidelines.pdf

Clark, P. (2020, 02 25). *The What, When and How of 5G*. Retrieved from Politico: https://www.politico.com/news/agenda/2020/02/25/the-what-when-and-how-of-5g-114485

Crotty, M. (1998). *The Foundations of Social Research: Meaning and Perspective in the Research Process*. SAGE Publications.

Czuczka, T. (2019, December 15). *China threatens retaliation should Germany ban Huawei 5G*. Retrieved from Bloomberg: https://www.bloomberg.com/news/articles/2019-12-14/china-threatens-germany-with-retaliation-if-huawei-5g-is-banned

Dey, I. (2010). Grounding Categories. In A. Bryant, & K. Charmaz, *The SAGE Handbook of Grounded Theory*. Thousand Oaks: SAGE Publications Ltd .

Donahue, P., Nicola, S., & Parkin, B. (2019, January 28). *Deutsche Telekom Warns Huawei Ban Would Hurt Europe 5G*. Retrieved from Bloomberg: https://www.bloomberg.com/news/articles/2019-01-28/deutsche-telekom-is-said-to-warn-huawei-ban-would-hurt-europe-5g

Drahokoupil, J., McCaleb, A. P., & Szunomár, Á. (2017). Huawei in Europe: strategic integration of local capabilities in a global production network . In J. Drahokoupil (Ed.), *Chinese investment in Europe: corporate strategies and labour relations* (p. 275). European Trade Union Institute.

Duchâtel, M., & Godement, F. (2019, June). *Europe and 5G: The Huawei Case Part 2*. Retrieved from Institut Montaigne: https://www.institutmontaigne.org/en/publications/europe-and-5g-huawei-case-part-2

Ekholm, B. (2019, December 2). *It's time to face the facts on 5G in Europe*. Retrieved from Ericsson: https://www.ericsson.com/en/blog/2019/12/Borje-Ekholm-5G-Europe-falling-behind

Eliassen, K. A., Mason, T., & Sjøvaag, M. (1999). European telecommunications policies - deregulation, re-regulation or real liberalisation? In K. A. Eliassen, & M. Sjøvaag (Eds.), *European Telecommunications Liberalisation* (p. 298). London: Routledge.

ENISA. (2019). *ENISA Threat Landscape for 5G Networks*. Brussels: European Union Agency for Cybersecurity.

European Commission. (2013, May 15). *Statement by EU Trade Commissioner Karel De Gucht on mobile telecommunications networks from China*. Retrieved from European Commission: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_13_439

European Commission. (2013, May 15). *Statement by EU Trade Commissioner Karel De Gucht on mobile telecommunications networks from China*. Retrieved from European Commission Press Corner: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_13_439

European Commission. (2019). *Commission Recommendation (EU) 2019/534 Cybersecurity of 5G networks*. Official Journal of the European Union. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019H0534&from=GA

European Commission. (2019, April 10). *EU foreign investment screening regulation enters into force*. Retrieved from European COmmission Press Corner: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2088

European Commission. (2019). *EU-China – A strategic outlook*. Strasbourg: European Commission. Retrieved from https://ec.europa.eu/commission/sites/beta-political/files/communication-eu-china-a-strategic-outlook.pdf

European Commission. (2019). *EU-China – A strategic outlook*. European Commission and HR/VP contribution to the European Council.

European Parliamentary Research Service . (2019). *5G in the EU and Chinese Telecom Suppliers* . Brussels: European Parliament.

European Political Strategy Centre. (2019). *Rethinking Strategic Autonomy in the Digital Age*. Brussels: European Commission.

Fan, P. (2006). Catching up through developing innovation capability: evidence from China's telecom-equipment industry. *Technovation, 26*, 359–368. doi:10.1016/j.technovation.2004.10.004

Ferguson, J. (2019, Novemeber 26). *Europe needs China's billions. But does it know the price?* . Retrieved from The Guardian: https://www.theguardian.com/commentisfree/2019/nov/26/europe-china-billions-strings-attached

Fildes, N. (2019, January 27). *5G: Can Europe match the US and China on mobile networks?* Retrieved from Financial TImes: https://www.ft.com/content/650d3bf8-1e32-11e9-b2f7-97e4dbd3580d

Fildes, N. (2019, February 19). *Ericsson chief warns Huawei fears will add to Europe's 5G delay*. Retrieved from Financial Times: https://www.ft.com/content/08979320-3131-11e9-8744-e7016697f225

Gehrke, T. (2020, February). What Could a Geoeconomic EU Look Like in 2020? *Security Policy Brief, 123*.

Giannopoulos, G., Filippini, R., & Schimmer, M. (2012). *Risk assessment methodologies for Critical Infrastructure Protection - State of the Art.* Luxembourg: Publications Office of the European Union.

Gilley, B. (2000). Huawei's Fixed Line to Beijing. *Far Easterns Economic Reviw*, 94-98.

Glaser, B. G., & Strauss, A. L. (1967). *The Discovery of Grounded Theory. Strategies for Qualitative Research.* Chicago: Aldine.

Govier, T. (1998). *Dilemmas of Trust* . McGill-Queen's University Press.

Gupta, A., & Kumar Jha, R. (2015). A Survey of 5G Network: Architecture and Emerging Technologies. *IEEE Access*, 1206-1232. doi:10.1109/ACCESS.2015.2461602

Herley, C. (2016). Unfalsifiability of security claims. *Proceedings of the National Academy of Sciences of the United States of America, 113*(23), 6415-6420. doi:10.1073/pnas.1517797113

Holton, J. (2010). Coding. In A. Bryant, & K. Charmaz, *The SAGE Handbook of Grounded Theory*. Thousand Oaks: Sage Publications Ltd.

Huawei. (2020). *Huawei Facts*. Retrieved from Huawei: https://www.huawei.com/en/facts

Huotari, M., & Kratz, A. (2019). *Beyond investment screening Expanding Europe's toolbox to address economic risks from Chinese state capitalism.* Güthersloh: Bertelsmann Stiftung.

Husar, B., Komada, M., & Habanova, M. (2019). *Recommendations document on national roaming access terms and conditions, as well as MVNO access terms and conditions.* Bratislava:

PricewaterhouseCoopers Advisory . Retrieved from https://europa.eu/capacity4dev/file/102084/download?token=nOVHKQgy

Issa, M., & Jha, K. (2019). The state of European Telcos: What left Europe behind in the race? *The Delta Perspective*.

Johnson, K., & Groll, E. (2019, April 3). *The Improbable Rise of Huawei*. Retrieved from Foreign Policy: https://foreignpolicy.com/2019/04/03/the-improbable-rise-of-huawei-5g-global-network-china/

Karpal, A. (2019, November 14). *China throws its weight behind A.I. and blockchain as it aims to be the world's tech leader*. Retrieved from CNBC: https://www.cnbc.com/2019/11/15/china-technology-trends-from-blockchain-to-ai-and-fintech.html

Kharpal, A. (2017, July 21). *China wants to be a $150 billion world leader in AI in less than 15 years*. Retrieved from CNBC: https://www.cnbc.com/2017/07/21/china-ai-world-leader-by-2030.html

Kleinhans, J.-P. (2017). *Internet of Insecure Things.* Berlin: Stiftung Neue Verantwortung.

Kleinhans, J.-P. (2019). *5G vs. National Security – A European Perspective*. Berlin: Stiftung Neue Verantwortung .

Kleinhans, J.-P. (2019, December). *Whom to Trust in a 5G World?* Stiftung Neue Verantwortung. Retrieved from Stifung Neue Verantwortung.

Koper, A., & Plucinska, J. (2019, April 16). *Poland to hold off blanket ban on Huawei 5G gear due to cost concerns*. Retrieved from Reuters: https://www.reuters.com/article/us-poland-huawei/poland-to-hold-off-blanket-ban-on-huawei-5g-gear-due-to-cost-concerns-idUSKCN1RS0QI

Kruse, S., & Winther, L. (2019, December 10). *Banned recording reveals China ambassador threatened Faroese leader at secret meeting*. Retrieved from Berlingske: https://www.berlingske.dk/internationalt/banned-recording-reveals-china-ambassador-threatened-faroese-leader

Lehne, S. (2020, February 25). *How the EU Can Survive in a Geopolitical Age*. Retrieved from Carnegie Europe: https://carnegieeurope.eu/2020/02/25/how-eu-can-survive-in-geopolitical-age-pub-81132

Lempert, L. (2010). Memo-Writing in GT. In A. Bryant, & K. Charmaz, *The SAGE Handbook of Grounded Theory*. Thousand Oaks: SAGE Publication Ltd.

Liikanen, E. (2001, July 16). Telecommunications Seminar. Sarajevo. Retrieved from European Commission : https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_01_356

Lippert, B., von Ondarza, N., & Perthes, V. (. (2019). *European Strategic Autonomy - Actors, Issues, Conflicts of Interests.* Berlin: German Institute for International and Security Affairs.

Liptak, K. (2020, February 7). *Trump 'tore into' Boris Johnson over Huawei in phone call, source says*. Retrieved from CNN: https://edition.cnn.com/2020/02/07/politics/donald-trump-boris-johnson-huawei/index.html

Lysne, O. (2018). *The Huawei and Snowden Questions.* Springer International Publishing. doi:10.1007/978-3-319-74950-1

Lysne, O., Nagelhus Schia, N., Gjesvik, L., Friis, K., & Elmokashfi, A. (2019). *Critical Communication Infrastructures and Huawei.* Norwegian Institute of International Affairs.

Mascitelli, B., & Chung, M. (2019). Hue and cry over Huawei: Cold war tensions, security threats or anti-competitive behaviour? *Research in Globalization*(1).

Matos, B. (2019, November 11). *The EU and European innovators must take part in shaping global 5G standards. Here's why.* Retrieved from Ericsson - Articles and Opinions: https://www.ericsson.com/en/patents/articles/eu-european-innovators-shaping-global-5g-standards

Matthee, H. (2011). Political Risk Analysis. In B. Badie, & D. &. Berg-Schlosser, *International Encyclopedia of Political Science*. Thousand Oaks: SAGE Publications, Inc.

Meuniér, S. (2014). Divide and conquer? China and the cacophony of foreign investment rules in the EU. *Journal of European Public Policy, Volume 21,* (Issue 7), 996-1016.

Meuniér, S. (2019). Chinese direct investment in Europe: Economic opportunities and political challenges. In K. Zeng, *Handbook of the International Political Economy of China.* Cheltenham: Edward Elgar Publishing.

Moses, J., & Knutsen, T. (2012). *Ways of Knowing: Competing Methodologies in Social and Political Research* (2 ed.). Macmillan Education UK.

Naughton, B. (2019). China's International Political Economy . In K. Zeng, *Handbook on the International Political Economy of China.* Cheltenham: Edward Elgar Publishing Ltd.

Neate, R. (2019, April 19). *Where is Huawei banned from working on critical networks?* Retrieved from The Guardian : https://www.theguardian.com/technology/2019/apr/19/where-huawei-is-banned

NIS Cooperation Group. (2019). *EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks.* Brussels: NIS Cooperation Group.

Nordrum, A., & Clark, K. (2017). *Everything You Need to Know About 5G*. Retrieved March 17, 2020, from https://spectrum.ieee.org/video/telecom/wireless/everything-you-need-to-know-about-5g

O'Brien, C. (2019, May 15). *Is Europe Losing The 5G Race?* Retrieved from The Innovator: https://innovator.news/is-europe-losing-the-5g-race-fb885b0be172

OECD. (2018). *China's Belt and Road Initiative in the Global Trade, Investment and Finance Landscape*. Paris: OECD Publishing,.

Pawlicki, P. (2017). Challenger Multinationals in Telecommunications: Huawei and ZTE. In J. Drahokoupil, *Chinese investment in Europe: corporate strategies and labour relations* (p. 21.39). Brussels: European Trade Union Institute.

Peppermans, A. (2016). The Huawei Case and What It Reveals About Europe's Trade Policy. *European Foreign Affairs Review, 21*(4), 539–558.

Perkowski, J. (2012, November 5). *China Leads In Foreign Direct Investment*. Retrieved from Forbes: https://www.forbes.com/sites/jackperkowski/2012/11/05/china-leads-in-foreign-direct-investment/#60bbbada1e11

Plucinska, J., Qing, K. G., Ptak, A., & Stecklow, S. (2019, July 2). *How Poland became a front in the cold war between the U.S. and China*. Retrieved from Reuters: https://www.reuters.com/investigates/special-report/huawei-poland-spying/

Ramalho, R., Adams, P., Huggards, P., & Hoare, K. (2015, Septermber). Literature Review and Constructivist Grounded Theory Methodology. *Qualitative Social Research, Volume 16*(Nr. 3).

Reuters. (2019, May 16). *China slams U.S. blacklisting of Huawei as trade tensions rise*. Retrieved from Reuters: https://www.reuters.com/article/us-usa-trade-china-huawei/china-slams-u-s-blacklisting-of-huawei-as-trade-tensions-rise-idUSKCN1SM0NR

Rockman, S. (2019, May 25). *Why 5G Isn't Just Faster 4G*. Retrieved from Forbes: https://www.forbes.com/sites/simonrockman1/2019/05/25/why-5g-isnt-just-faster-4g/#2f17da7843a6

Rogers, M., & Ruppersberger, D. (2012). *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*. Washington, DC: U.S. House of Representatives Permanent Select Committee on Intelligence.

Rühlig, T. (2020). *Who Controls Huawei? Implications for Europe*. Stockholm: Swedish Institute of International Affairs. Retrieved from https://www.ui.se/globalassets/butiken/ui-paper/2020/ui-paper-no.-5-2020.pdf

Rühlig, T., & Björk, M. (2020). *What to Make of the Huawei Debate? 5G Network Security and Technology Dependency in Europe.* Stockholm: Swedish Institute of International Affairs.

Scott, J., & Murtaugh, D. (2019, February 21). *China Restricts Australian Coal Imports in Likely Retaliation to Huawei 5G Ban*. Retrieved from Fortune: https://fortune.com/2019/02/21/china-australia-coal-imports/

Shepard, W. (2019, October 3). *What China Is Really Up To In Africa*. Retrieved from Forbes: https://www.forbes.com/sites/wadeshepard/2019/10/03/what-china-is-really-up-to-in-africa/#298ed0ec5930

Sottilotta, C. E. (2013). *Political Risk: Concepts, Definitions, Challenges*. Rome: LUISS School of Government.

Spiegel. (2018, December 14). *Bundesamt spricht sich gegen Huawei-Boykott aus*. Retrieved from Spiegel: https://www.spiegel.de/netzwelt/netzpolitik/5g-netzausbau-bsi-spricht-sich-gegen-huawei-boykott-aus-a-1243708.html

Staudenmaier, R. (2020, January 18). *Germany's Seehofer warns of 5G delays if Huawei is excluded*. Retrieved from Deutsche Welle: https://www.dw.com/en/germanys-seehofer-warns-of-5g-delays-if-huawei-is-excluded/a-52050565

Stearns, J. (2019, February 14). *Europe's Investment-Screening Plan Clears Final Political Hurdle*. Retrieved from Bloomberg: https://www.bloomberg.com/news/articles/2019-02-14/europe-s-investment-screening-plan-clears-final-political-hurdle

Stec, G. (2019, November 29). *To Huawei or not to Huawei - EU's 5G future*. Retrieved from Friends of Europe: https://www.friendsofeurope.org/insights/to-huawei-or-not-to-huawei-eus-5g-future/

Sullivan, J., & Lucas, R. (2020). *5G Cyber Security: A Risk Management Approach*. London: The Royal United Services Institute for Defence and Security Studies.

Telia. (2010, 1 2010). *TeliaSonera has selected 4G vendors*. Retrieved from Telia: https://www.teliacompany.com/en/news/press-releases/2010/1/teliasonera-has-selected-4g-vendors/

The White House. (2019). *oint Statement from President of the United States Donald J. Trump and President of Romania Klaus Iohannis.* Washington: The White House.

Tie, Y. C., Birks, M., & Francis, K. (2019, January 2). Grounded theory research: A design framework for novice researchers. *SAGE Open Med.*(2019; 7).

Timmers, P. (2018, September 14). *Cybersecurity is forcing a rethink of Strategic Autonomy*. Retrieved from The Oxford University Politics Blog: https://blog.politics.ox.ac.uk/cybersecurity-is-forcing-a-rethink-of-strategic-autonomy/

Timmers, P. (2019). *Strategic Autonomy and Cybersecurity.* EU Cyber Direct.

Tirkey, A. (2020). *The 5G Dilemma: Mapping Responses Across the World.* New Delhi: Observer Research Foundation. doi:https://www.orfonline.org/wp-content/uploads/2020/05/ORF_Monograph_5G_Dilemma.pdf

Triolo, P., Allison, K., & Brown, C. (2018). *The Geopolitics of 5G.* Washington: Eurasia Group.

Tzogopoulos, G. (2016, January 29). *China and Juncker's Investment Plan.* Retrieved May 11, 2020, from https://www.vocaleurope.eu/china-and-junckers-investment-plan/

Wagner, J. (2017, June 1). *China's Cybersecurity Law: What You Need to Know* . Retrieved from The Diplomat: https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/

van den Hoonaard, W. (2012). Sensitizing Concepts. In L. Given, *The SAGE Encyclopedia of Qualitative Research Methods* (pp. 813-814). Thousand Oaks: SAGE Publications. doi: https://dx.doi.org/10.4135/9781412963909

van Tetering, J. (2019, June 12). *Europe's digital future: united and determined to win*. Retrieved from Friends of Europe: https://www.friendsofeurope.org/insights/europes-digital-future-united-and-determined-to-win/

Wang, C., Wen, Y., & Han, F. (2011). Study on China's outward FDI. *Procedia Environmental Sciences*, 543 – 549.

Wheeler, T., & Simpson, D. (2019, September 3). *Why 5G requires new approaches to cybersecurity*. Retrieved from Brookings: https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity/

Wintour, P. (2020, February 15). *US defence secretary warns Huawei 5G will put alliances at risk*. Retrieved from The Guardian: https://www.theguardian.com/us-news/2020/feb/15/us-defence-secretary-warns-us-alliances-at-risk-from-huawei-5g

World Bank. (2018, March 29). *Belt and Road Initiative*. Retrieved from World Bank: https://www.worldbank.org/en/topic/regional-integration/brief/belt-and-road-initiative

World Bank. (2020, April). *The World Bank In China*. Retrieved from World Bank: https://www.worldbank.org/en/country/china/overview

Woyke, E. (2018, December 18). *China is racing ahead in 5G. Here's what that means.* Retrieved from MIT Technology Review: https://www.technologyreview.com/2018/12/18/66300/china-is-racing-ahead-in-5g-heres-what-it-means/

Wu, X., Murmann, J. P., Huang, C., & Guo, B. (2020). The Management Transformation of Huawei: An Overview. In X. Wu, J. P. Murmann, C. Huang, & B. Guo, *The Management Transformation of Huawei: From Humble Beginnings to Global Leadership* (pp. 1-70). Cambridge: Cambridge University Press.

Zeng, K. (2019). Introduction . In K. (. Zeng, *Handbook on the International Political Economy of China.* Cheltenham: Edward Elgar Publishing Ltd.

Zheng, Y. (2019). Foreign Direct Investment in China. In K. (. Zeng, *Handbook on the International Political Economy of China*. Cheltenham: Edward Elgar Publishing Ltd.

Appendix 1. Coding template

BASIC INFORMATION AND CONTEXT

- Name and year of publication
- Author and publisher (including affiliation, type of organization etc.)
- Purpose of publication

KEY GUIDELINES IN EXAMINING THE DATA

- Remain open
- Stay close to the data
- Keep your codes simple and precise
- Construct short codes
- Compare data with data
- Move quickly through the data

GUIDING QUESTIONS IN THE ANALYSIS AND CODING:

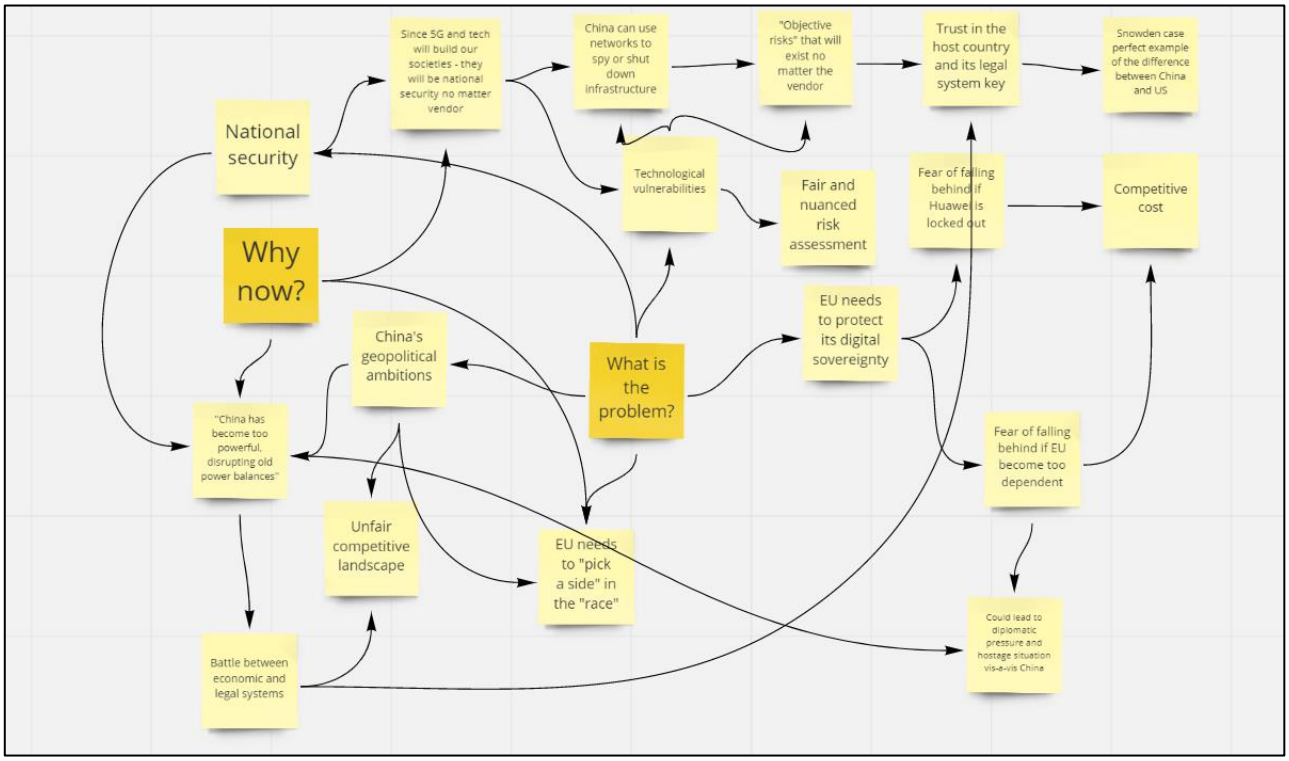
- Breaking down the problematization of the text: o
    - Why is it an issue?
    - For whom is it an issue?
    - What preconceptions might the author(s) have?
    - What meaning and implication are assigned to a phenomenon or factor
    - Are the consequences of the risk unavoidable?
    - Can the risks be mitigated or avoided completely?
- What stakeholders/actors are involved?
- Does the author(s) take a clear stance?
    - o If so, what, and why?

AVOIDING PRECONCEPTIONS

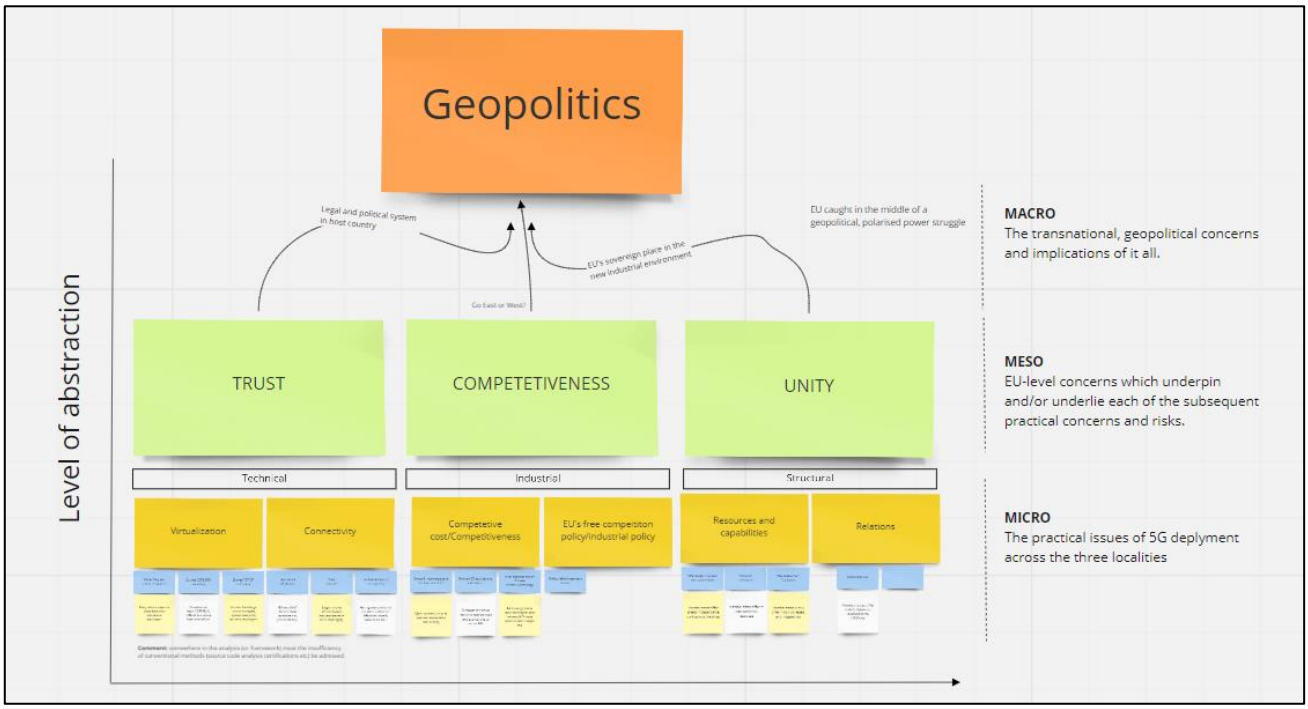
Always ask the following questions before applying a theoretical concept from previous academic literature to your data:

- Do these concepts help you understand what the data indicate?
- If so, how do they help?
- Can you adequately interpret this segment of data without these concepts? What do they add?
- Can you explicate what is happening in this line or segment of data with these concepts?

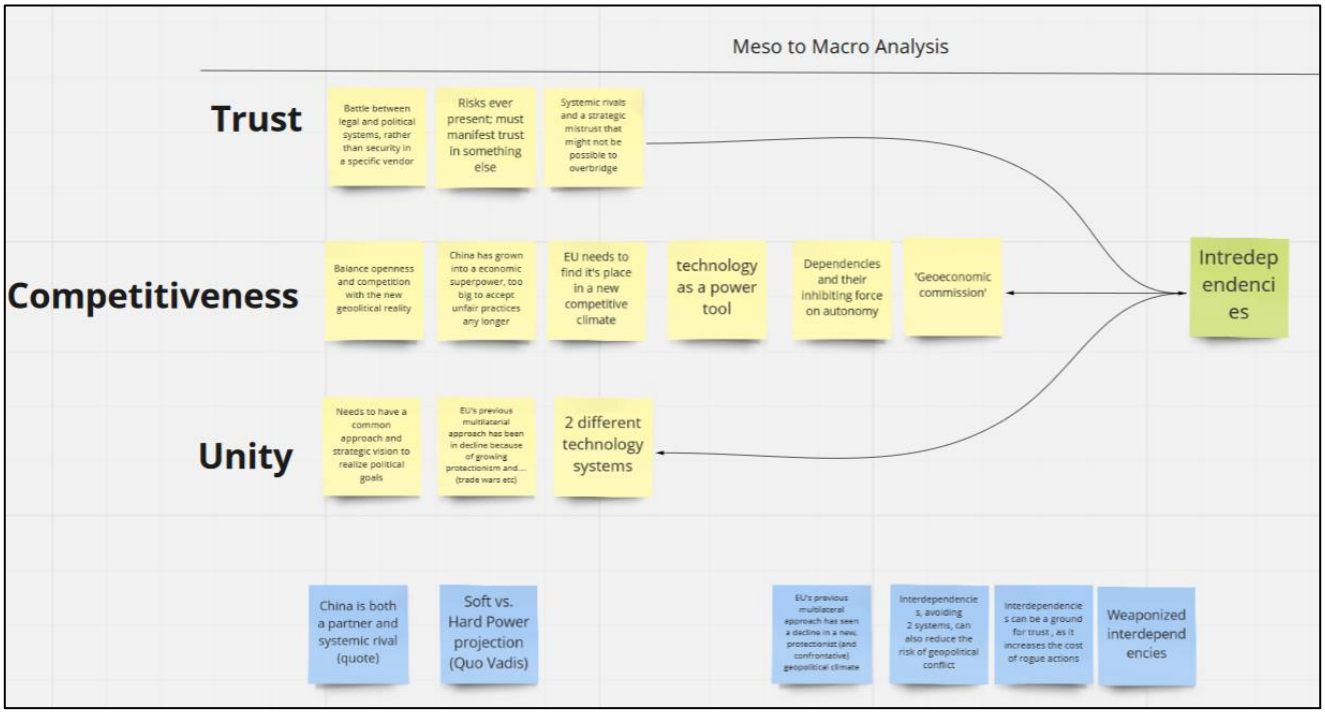
Appendix 2. Excerpts from the coding process



Collection of important concepts and aspects from the coding of the coding of the purposive sample of data. These were part in the process of forming the framework.



Early version of the main framework of the paper, including the different levels of abstraction and units of analysis.



Intermediate step to outline the transition from meso to macro level.