LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

Studienabschlussarbeiten
Sozialwissenschaftliche Fakultät

Freiin von Blomberg, Pia Victoria:

Cybersecurity in the European Union: The Securitization of Chinese 5G Providers

Bachelorarbeit, Sommersemester 2023

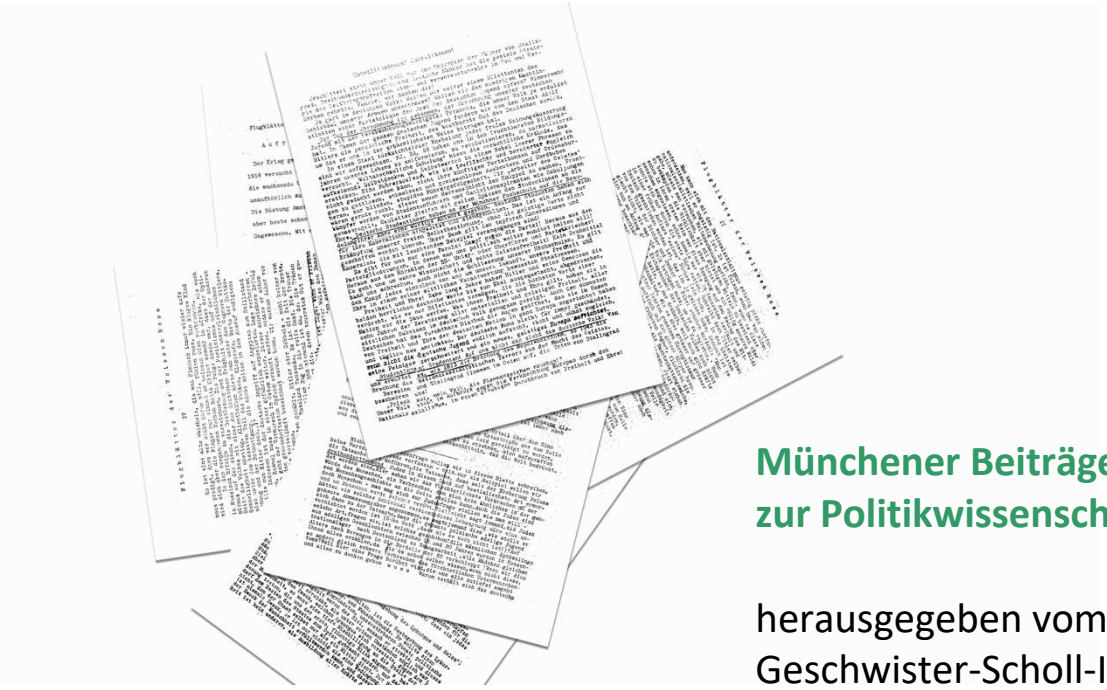
Sozialwissenschaftliche Fakultät

Ludwig-Maximilians-Universität München

https://doi.org/10.5282/ubm/epub.105955

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

GESCHWISTER-SCHOLL-INSTITUT
FÜR POLITIKWISSENSCHAFT



Münchener Beiträge zur Politikwissenschaft

herausgegeben vom
Geschwister-Scholl-Institut
für Politikwissenschaft

2023

Pia Victoria Freiin von Blomberg

Cybersecurity in the European Union: The Securitization of Chinese 5G Providers

---

Bachelorarbeit bei
PD. Dr. Moritz Weiß
2023

Abstract

While most new technology is considered an opportunity for market leadership or otherwise improved capabilities at first, associated cybersecurity risks often show themselves with time. As soon as they do, policymakers are expected to react. This is especially true when regarding critical digital infrastructure. From early on, fifth-generation networks (5G) were predicted to vastly exceed all previous generations in regard to capabilities and areas of application. During the initiation of the implementation of this telecommunication infrastructure, claims against one of the major 5G providers in the EU, namely the Chinese company Huawei, came to light. A securitization of Chinese 5G providers in Europe ensued, leading to the classification of Huawei as a so-called "high-risk supplier". But how did this happen when the EU and China once committed to reciprocal open market access and Huawei used to be a major provider during the earlier generation networks?

We consider this question with the help of two theoretical approaches. One focuses on the external influence on the EU from the U.S., and the other on the internal influence on the EU from EU member states with domestic 5G providers. The latter refers to Finland (Nokia) and Sweden (Ericsson), as they might be more willing to push for the securitization of foreign 5G vendors. Nordic countries have generally surpassed other EU states in 5G technology, giving them possibly the needed authority to influence the EU in this regard. This thesis will employ Theory-Testing Process-Tracing to figure out which of those theoretical approaches hold explanatory power. The empirical analysis leads to the conclusion that the external influence of the U.S. has been decidedly more relevant for the securitization of Chinese 5G providers in the EU than the influence of EU member states with domestic 5G providers. This is important, as it demonstrates the dominant role of the U.S. in cyberspace, allowing for them to induce policy alignment with other major global powers such as the EU.

Acronyms

4G networks	Fourth generation networks
5G networks	Fifth generation networks
5G-PPP	Public-Private-Partnership on 5G
6G networks	Sixth generation networks
6G-IA	6G Smart Networks and Services Industry Association
CSIRT	Computer Security Incident Response Team
ENISA	European Union Agency for Cybersecurity
GCI	Global Cybersecurity Index
NIS Cooperation Group	Network and Information Systems (NIS) Cooperation Group
PT	Process-Tracing

Content

1 Introduction

It is September 2015, the day of the EU-China High Level Economic and Trade Dialogue in Beijing. The European Union (EU) and China have just signed a so-called "milestone agreement", committing to joint research and development of 5G technologies as well as reciprocal open market access (European Commission, 2015). Fast forward to 2019, the European Parliament publishes a report called "Security threats connected with the rising Chinese technological presence in the EU and possible action on the EU level to reduce them" (European Parliament, 2019b). Years of discussions about 5G security ensue, warnings about foreign vendors persist, and by 2023, the EU Commission has deemed the Chinese companies Huawei and ZTE "high-risk suppliers" (Breton, 2023), making restrictions and exclusion of their services and products within the EU legitimate. The Commission also wants to "avoid exposure to Huawei and ZTE" (Breton, 2023) in European telecommunication, and an EU-wide mandatory ban on Huawei's products and services concerning telecommunication infrastructure is still on the table (Espinoza and Gross, 2023). But what happened to cause this rather drastic shift? How have Chinese 5G providers become a matter of (cyber)security?

To approach this question, a shared understanding of the term *cybersecurity* is needed. Lewallen (2021, p. 1038) gives a concise definition. He states:

> "Cybersecurity […] is a policy problem or set of related policy problems whose dimensions expand and change based on changes to technology that either introduce new vulnerabilities or expose new users, objects, and interests to existing vulnerabilities."

One of the most prominent changes to technology has come in the form of evolving mobile telecommunication networks. Currently, Europe is facing the implementation of the fifth generation (5G) of those networks, which aims for "high data rate, reduced latency, energy saving, and massive device connectivity" (Ericsson, 2021, p. 20). While still lacking behind international competitors, the EU's adoption of 5G has steadily improved in the last few years (GSMA, 2023). From the EU's perspective, 5G technology is considered a "game changer" (European Commission, 2016, p. 2), since the capabilities and areas of application of those networks exceed all previous generations. According to the EU's Network and Information Systems (NIS) Cooperation Group (2019, p. 28), this broadened potential also leads to "interdependencies between 5G networks and many other systems in critical areas (e.g. health, autonomous vehicles, power, gas and water supply, defence)". Some label 5G infrastructures "the most critical infrastructures we have ever seen" (Friis and Lysne, 2021, p. 1181), as the breakdown of those networks would impact the functioning of society and economy severely.

The protection of critical infrastructure - including telecommunication infrastructure - is commonly considered crucial for national security (Dunn Cavelty and Suter, 2009, p. 1), which demonstrates the extreme significance of the subject.

In the EU, different entities responsible for securing the cyberspace exist. One of them is the European Union Agency for Cybersecurity (ENISA), which mostly provides expertise and guidelines on the topic of 5G security (ENISA, 2023). Important are also the NIS Cooperation Group quoted above, which ensures information exchange among EU member states, and European institutions, which request and support the work of those entities. Especially the European Commission and the European Parliament will be relevant in the course of this thesis, as their recommendations, reports and resolutions make it possible to trace attitudes of the EU toward certain topics. However, it is too simple to attribute responsibility for European cybersecurity to official EU entities only. Specifically critical digital infrastructure relies tremendously on public-private partnerships, as much of the critical digital infrastructure is provided and serviced by the private sector (Boeke, 2018, p. 451). Huawei, Ericsson, and Nokia have been the main vendors of telecommunication equipment within the EU for quite some time (NIS Cooperation Group, 2019, p. 10), which makes the case of Huawei an especially interesting study when referring to a change toward Chinese telecommunication providers in Europe. While the Chinese company ZTE will also be mentioned sporadically, the distinguished market position of Huawei leads to a focus on the latter.

Up until now, much literature regarding Huawei and 5G has addressed the legitimacy and reasoning of policy against Huawei or the differences in implementation across countries (e.g., Friis and Lysne, 2021; Kleinhans, 2019). Less researched is the process behind the securitization of the company, and more often than not, the process is only drawn back to influence from the United States (U.S.). A possible influence of EU member states with domestic 5G providers, which might be quicker than others to call for securitization of Chinese 5G providers, has been disregarded. Wishing to rectify this, the posed research question of this bachelor's thesis is:

How can the EU's securitization of Chinese 5G providers be explained?

This paper will approach the question from two points of view, specifically the external influence on the EU from the U.S., and the internal influence on the EU from EU member states with domestic 5G providers. This research paper will employ Theory-Testing Process-Tracing to answer which is more relevant in explaining the securitization of Chinese 5G providers in the EU. To do this, the thesis will start with an insight into the utilized concept of securitization

as well as an overview of 5G in the European Union and the changing role of Chinese 5G providers. The theoretical framework, which provides the basis for the later deducted causal mechanisms, illustrates the relations and linkages in securitization in general terms and then adapts the findings to the case of interest. A description of the chosen method - Theory-Testing Process-Tracing - and the expected empirical data for each step of the causal mechanisms is given. The empirical analysis follows, and ultimately leads to the conclusion that the external influence of the U.S. has been decidedly more relevant for the securitization of Chinese 5G providers in the EU than the influence of EU member states with domestic 5G providers. This is important as it demonstrates the dominant role of the U.S. in cyberspace, enabling the country to influence policy alignment with other major global powers such as the EU.

2 The Securitization of Chinese 5G Providers

Myriam Dunn Cavelty and Andreas Wenger (2020, pp. 17–22) suggest that current research on cybersecurity politics can be clustered into three research areas. The first one focuses on the practices of states regarding cyber conflicts and acknowledges cyberspace as a new sphere of strategic relevance. The second cluster zeroes in on actors other than the state itself, such as cybersecurity companies and intelligence agencies. It is interested in the role those actors play in regard to national cyber policy and practice. The third cluster addresses securitization. Thematic focus points are often the practices and actors behind the construction of issues as threats, the nature of securitized issues, and the corresponding policy responses. This paper falls within the last cluster.

2.1 Securitization

Some of the most prominent authors concerning the concept of securitization are associated with the Copenhagen School, such as Ole Wæver, Berry Buzan, and Jaap de Wilde. Their book "Security: A New Framework for Analysis" (Buzan *et al.*, 1998) is considered one of the principal works on securitization, and much of their individual literature has shaped the understanding of securitization (e.g., Wæver, 1999). This paper draws upon their concepts but adapts them to the topic of cybersecurity.

In international relations, the term *security* is linked to power politics. Security issues are posed as existential threats or emergencies and therefore legitimize a wide range of otherwise not necessarily appropriate responses (Buzan *et al.*, 1998, p. 21). "Securitization" is a more extreme form of politicization. While politicized issues are part of public policy and require government action at some point, securitized issues require - corresponding to the definition of security - immediate and substantial action. The goal of studying securitization is to "gain an increasingly

precise understanding of who securitizes, on what issues (threats), for whom […], why, with what results, and, not least, under what conditions" (Buzan *et al.*, 1998, p. 32). The Copenhagen School stresses the difference between securitizing moves and securitization (Buzan *et al.*, 1998, pp. 23–26). Securitizing moves describe the discourse or speech-acts in which certain issues are framed as existential threats or rather matters of security. Securitization, however, is conditioned by the *acceptance* of those security issues by the audience.

Criticism of this approach has often focused on the understanding of security as a speech-act. The Copenhagen School considers securitization to be based on discourse on security matters, which in reality often does not represent existing security situations but rather *constructs* security issues. Balzacq (2005, p. 172) considers this equalization of security and speech-act to be highly problematic since neglecting contextual factors leads to inadequate grounds for the analysis of "real-life" situations. While refuting other criticism regarding this approach of the Copenhagen School, Michael Williams takes this assessment even further and states that not only context but also the "communicative and institutional processes of securitization at work in contemporary politics" (Williams, 2003, p. 528) are overlooked. This paper aims to acknowledge this criticism by tracing the exact processes through the hypothesized causal mechanisms.

According to Buzan *et al.* (1998, pp. 7–8), there are five *sectors* of security - economic, societal, environmental, military, and political security – which are distinguishable by their specific types of interaction. Two of them are especially relevant for this paper, namely the political and the economic sector. The political sector "is about relationships of authority, governing status, and recognition" (Buzan *et al.*, 1998, p. 7), existential threats most often target the sovereignty or the ideology of the referent object. In contrast, the economic sector consists of "relationships of trade, production, and finance" (Buzan *et al.*, 1998, p. 7). A major concern for economic security has been caused by the shift from inefficient self-help principles to the reliance on external actors, especially concerning supply chains. Now, this dependency could be used to enforce political interests, for example by withholding materials or products (Buzan *et al.*, 1998, p. 98). As acknowledged by Wæver (1999, pp. 335–336), a cross-sectional insight is needed to understand the circumstances in which the political actors were and therefore more accurately observe specific political occurrences.

2.2 5G in the European Union and the Changing Role of Chinese 5G Providers

The topic of mobile telecom networks has only recently been securitized (Friis and Lysne, 2021, pp. 1174–1175). While 4G networks were only regarded in a technological context, the change to 5G networks has opened up a door for security debates concerning Chinese 5G providers such as Huawei. Radu and Amon (2021, pp. 1–2) determine three reasons for this development, namely an intense competition about market leadership in 5G technology, a growing concern about foreign stakeholders in critical infrastructure, and the potential of 5G in regard to the digital economy. While the USA was openly positioning against China and Chinese 5G providers such as Huawei, the EU was more cautious. Friis and Lysne (2021, p. 1185) state that "Europeans seem to have avoided a macrosecuritization of China, while joining the US in the niche securitization of 5G". But is this statement true? Has there been a securitization of 5G in the EU, and does this securitization apply to the niche of Chinese 5G providers also?

To answer this preliminary question it is helpful to outline the EU's efforts towards the 5G rollout and to point out the role of China and Chinese companies along the way. The first major efforts of the European Union toward 5G date back to 2013. Back then, the European Commission launched a Public-Private-Partnership on 5G (5G-PPP), which aimed at ensuring a 5G rollout by 2020 and was funded with more than 700 million euros (European Commission, 2016, p. 2, 2022). The money was mostly allocated through the Horizon 2020 program, created to further research and innovation in the EU. Projects that are now considered success stories by the Commission are for example 5Gwireless (European Commission, 2018) and SILIKA (European Commission, 2019b), which ran from 2015 to 2018 and 2016 to 2020 respectively and focused on improving existing technology and infrastructure to make way for 5G communications. In 2016, the European Commission published an action plan regarding 5G technology, in which they considered the new technology an opportunity for development and leadership. The plan insisted on establishing "a European 'home market' for 5G" (European Commission, 2016, p. 2) as well as a common European approach to financing, research, and the implementation of 5G. The word "security" is only mentioned twice in the entire document, once in a paragraph about strengthening the role of the public sector in regard to 5G technology and later in the paraphrased key point of said paragraph, which reads:

> "**Action 7 - The Commission encourages Member States** to consider **using the future 5G infrastructure** to improve the performance of **communications services used for public safety and security**, including shared approaches in view of the future procurement of advanced broadband public protection and disaster relief systems. Member States are encouraged to

> include this consideration in their national 5G roadmaps." (European Commission, 2016, pp. 9–10; emphasis in original)

Notably, the usage of 5G is framed as a means for more security, while there is no notion of security risks associated with this new development. During this time, China is a key partner in the EU's efforts to develop 5G networks. Signing a milestone agreement in 2015, both parties committed to, amongst other things, joint research programs and open market access (European Commission, 2015). If there had never been a securitization of 5G networks in Europe, one could have expected this viewpoint of the EU to last. 5G technology would still have been majorly seen as an overwhelmingly positive opportunity, and stakeholders and policymakers would have (at least publicly) held little or even no regard for threats regarding network security. Back in 2016/17, the market position of Huawei was rather strong. Some analysts rumored that the company would surpass Apple in the smartphone market within a year (Kharpal, 2016), and Huawei's 5G market position was also rather promising. The company provided 4G networks in many EU countries and held a global leadership position in 5G technology (Friis and Lysne, 2021, p. 1177). If the EU's securitization of 5G did not also pointedly apply to the niche of Chinese 5G providers (including Huawei), one would expect this trend to go on until today.

Instead, the position of Huawei began to waver. On March 19th, 2019, the European Parliament passed a resolution titled "Security threats connected with the rising Chinese technological presence in the EU and possible action on the EU level to reduce them" (European Parliament, 2019b). The Parliament expressed concerns about the possibility to exploit weaknesses of 5G networks and questioned if claims about embedded backdoors[1] in the 5G equipment of Chinese vendors were true. It also explicitly referred to the Chinese State Security Laws and criticized the obligation of all connected entities to support Chinese efforts to safeguard national security, considering that the definition of national security is rather vague and could potentially be used for broader purposes. The companies Huawei and ZTE were mentioned by name in a reference made to Czech claims of security issues regarding their products. By March 26th, about a week later, the European Commission had prepared recommendations for member states to strengthen their security in regard to 5G networks. Amongst other things, an instrument allowing member states to screen foreign direct investments into critical infrastructure and technology was implemented (European Commission, 2019a, p. 3). Another recommendation for member states was to review regulations imposed on equipment vendors, especially

[1] Backdoors give users access to systems or networks, making it possible to surpass implemented security measures.

regarding "the overall risk of influence by a third country, notably in relation to its model of governance" (European Commission, 2019a, p. 4). Even though Chinese 5G providers were not explicitly mentioned, this choice of phrasing does seem to represent the claims against Huawei. By October 9th, 2019, the Network and Information Systems (NIS) Cooperation Group had published a report about the "EU coordinated risk assessment of the cybersecurity of 5G networks" (NIS Cooperation Group, 2019). At this point, 5G technology, especially from Chinese providers, had become a matter of security. Considering the rather short time between each of those publications, it seems as if the topic of security risks regarding Chinese 5G technology presented itself as a substantial threat and required, at least from the perspective of European policymakers, immediate attention. The acknowledgment of this particular security issue in official EU policy papers seems to base on EU-wide acceptance of the fact that foreign 5G vendors, especially "untrusted" Chinese providers, might pose a security risk.

Up until now, the securitization of Chinese 5G providers, represented by the companies Huawei and ZTE, has become even more clear. In 2022, for example, a special report of the European Court of Auditors openly mentions "[s]ecurity concerns on the context of EU-China cooperation on 5G" (European Court of Auditors, 2022, p. 9). The idea, that "EU citizens and companies using advanced and innovative applications enabled by **5G and future generations of networks** should benefit from the highest security standard" (European Commission, 2020, p. 8, emphasis in original) has become an accepted sentiment. The EU toolbox for 5G security has been implemented, providing risk assessments and measures against threats (European Commission, 2021). As of June 2023, the EU has confirmed action taken by EU states against Huawei to be legitimate and the EU Commission stressed the wish "to avoid exposure to Huawei and ZTE" (Breton, 2023) in Europe's telecom infrastructure. Both Huawei and ZTE are now considered "high-risk vendors" (Sawall, 2023), and a mandatory ban on Huawei's products for 5G infrastructure in all EU member states is still in discussion (Espinoza and Gross, 2023).

One might still argue that the lack of uniformly implemented regulations such as bans throughout the EU speaks against the securitization of Chinese 5G providers. However, Buzan et al. (1998, p. 25) argue that securitization does not necessarily require the *adoption* of emergency responses to the perceived security issue. There only has to be a large enough consensus to *enable* measures that would otherwise be considered illegitimate. The fast response to first claims of security risks in 5G technology perpetuated by Chinese vendors as well as the links between Chinese telecommunication companies, 5G, and security risks stated

in surprisingly undiplomatic terms are certainly measures that would have otherwise been deemed illegitimate by the European Union, which cultivates a strong (trading) partnership with China (European Commission, 2019c). Together, the policy proposals, reports and EU-wide measures to minimize risks posed by Chinese 5G vendors allow the conclusion that there has been a securitization of 5G providers, and furthermore, a niche securitization of 5G providers with Chinese origin in the EU, even if it is far from the hostile position the U.S. has taken (see chapter 5.1).

3 Theoretical Framework

The understanding of security is formed in a social process rather than existing as a mere fact or condition (Williams, 2003, p. 513). This paper wishes to test whether the external or internal influence holds more explanatory power for the securitization of Chinese 5G providers in the EU by examining whether certain causal mechanisms were present in the securitization of Huawei. The first theoretical approach intends to explain the securitization in the EU through external, or rather U.S. American influence. The second wishes to draw the outcome back to the internal influence of EU member states with domestic 5G providers.

3.1 Overarching Theory: Linkages in Securitization

While Buzan *et al.* (1998, pp. 7–8) identify five different sectors of security, it can be difficult to differentiate between them. Economic securitization, for example, seldom exists in its pure form in the strict interpretation of the liberal view. If an issue becomes securitized rather than only politicized, this is most likely due to its effects in other security sectors (Buzan *et al.*, 1998, p. 99). The political sector is even inherently intertwined with each of the other sectors, as existential threats are always defined and later securitized through political acts. This is why economic security must rather be considered “political-economic” security (Buzan et al., 1998, p. 141). For the sake of conciseness, no hard distinctions between both sectors will be made in this thesis. The securitization of Chinese telecommunication infrastructure, or rather the providers behind it, might be based on either political or economic security concerns. The former would refer to a threat to basic principles, the latter to dependencies on other states and possibly vulnerable supply chains. In the case of Huawei, it is most likely that both concerns were raised at some point. This thesis is therefore limited to answering whether the external or internal influence on the EU was more relevant for the securitization of Huawei, while the reasoning of involved actors, meaning whether they primarily referred to economic or political concerns, is not the focus of this paper.

Buzan *et al.* (1998, pp. 155–160) illustrate "linkages" or "chain reactions" between different actors and entities. Their idea is that an "external power […] makes reference to some general principles and points to threats to international stability; by doing so, it tries to mobilize others in support of its actions" (Buzan *et al.*, 1998, p. 159). The audience, whom the securitizing actor is trying to convince to take action, later becomes a performing actor themselves (Bright, 2012, p. 869). In the hereby utilized understanding, the term *external power* refers to a power other than the intended audience. This means that EU member states with domestic 5G providers can be also external powers if they wish to influence the EU, since they are then securitizing actors, not the audience. Since this paper aims to single out the relevant explanation for securitization in the EU, the action for which countries try to gain reinforcement must also be securitization. Buzan *et al.* (1998, p. 160) note that those linkages within the political sector are usually based on principles, not power, since principles are more easily conveyed. The securitizing actors in the political sector are either leaders or institutional structures (Buzan *et al.*, 1998, p. 146).

Based on this knowledge, we can now deduct a general causal mechanism from the first theoretical approach. A more thorough explanation of causal mechanisms and Process-Tracing in general will follow in chapter 4.1.

Figure 1: General Causal Mechanism

X	**Causal mechanism** (Influence on Securitization in EU)					**Y**
Capabilities of External Power	⟶	External Power *securitizes* an issue in the national context	⟶	External Power *urges* its allies to realize a threat and support/adapt their action based on principles, therefore initiating securitization within the EU	⟶	Securitization in the EU

This general framework for the influence on securitization in the EU will now be adapted to the two theoretical approaches.

3.2 Influence of the United States

Friis and Lysne (2021, p. 1177) state that the "securitization of Chinese 5G must […] be seen in this broader context of American securitization of China in general." Acknowledging this statement, the first theoretical approach aims to highlight the role of international relations and transnational security concerns (or the "external influence") regarding the securitization process in the EU.

When adapting the illustrated general model to the case, one must answer four questions: who is the external power? What is the action for which they try to gain support? Who is supposed to be mobilized? And last, what are the principles of relevance? The external power of the first approach is the U.S., represented by its leading policymakers. The choice of focusing on the U.S. influence stems from the knowledge that the country has sizeable relative power in the international system due to their capabilities in cyberspace (X_1). Even before the topic of Huawei gained major attention in 2018/2019, the Global Cybersecurity Index (GCI) 2018 awarded the U.S. the second place for commitment to cybersecurity globally (ITU, 2019, p. 16). The U.S. considered it crucial to maintain its "technological leadership" (The White House, 2018, p. 25), which others dubbed "U.S. cyber dominance" or "cyber superiority" (e.g., Austin, 2014, pp. 142–144). They are successful in doing so, seeing that the country is considered the only tier one country in regard to cyber capability (IISS, 2021, pp. 9–10). It is also the most powerful country concerning information and communication technology (IISS, 2021, p. 18). As pointed out in the overarching theory, the action they are trying to gain support for is the securitization of Chinese 5G providers in the national context, meaning in the United States. As the outcome considered in this thesis is the securitization of Chinese 5G providers in the EU, the EU is also the party that is supposed to be mobilized by the U.S. policymakers.

Figure 2: Adapted Causal Mechanism – External Influence on Securitization in the EU

X	**Causal mechanism** (External Influence on Securitization in EU)					**Y**
Relative power of U.S. in international system due to capabilities in cyberspace	⟶	U.S. Policymakers *securitize* Chinese 5G providers in the national context	⟶	U.S. Policymakers *urge* its allies to realize the threat stemming from Chinese 5G providers and support/adapt the securitization based on arguments relating to EU principles, therefore initiating securitization within the EU	⟶	Securitization of Chinese 5G Providers in the EU

The principles, which the U.S. policymakers can utilize to trigger a chain reaction, should be shared by the U.S. and the EU. Otherwise the action might not be reciprocated by the referent object – meaning the entity at risk, in this case, the EU and its citizens - and no securitization in the EU would have been seen. The European core values threatened by issues regarding cybersecurity, or rather network security, are the "global and open cyberspace, […] the rule of law, fundamental rights, freedom and democracy" (European Commission, 2020, pp. 1–2). On an individual level, specifically the fundamental right to personal data protection is assumed to

be violated by Chinese 5G providers (European Union, 2012). On the EU level, the core concern regarding the political security sector is the integral position of 5G technology in European critical infrastructure (European Commission, 2021). Regarding its external relations, the EU fears that the exploitation of cyberspace is undermining international security (European Commission, 2020, p. 2).

3.3 Influence of EU Member States with Domestic 5G Providers

Friis and Lysne (2021, pp. 1184–1185) also recognize that an increasing securitization of 5G was also seen in European states, which then made the European Union conscious of the issue. This line of thinking puts the EU member states in the focus of analysis and will be followed during the second theoretical approach. The aim is to provide an additional perspective on the securitization process by examining the role of EU member states and their concerns (or the "internal influence") on the European securitization of Chinese 5G providers.

In this second theoretical approach the term *external power* refers to EU member states with domestic 5G providers while the action is now the securitization of Chinese 5G providers within Sweden and Finland. Since the outcome of this paper is fixed, the target of the mobilization is still the EU and the principles are the same. The choice of pointedly analyzing the influence from those certain EU member states results from the assumption that they have capabilities in regard to 5G technology (X_2), giving them more authority in the field compared to fellow EU states without major 5G companies. Within the EU, the biggest European 5G providers are Ericsson and Nokia (European 5G Observatory, 2022), which are of Swedish and Finnish origin respectively. Reports allege that the Nordic countries assumed leadership positions in telecommunication infrastructure, outperforming other EU states (GSMA, 2023). This might also give them the necessary experts and knowledge to be the first EU states to realize 5G security risks. Both countries have lobbied for advantages of their respective companies before when applying for financial contributions from the European Globalisation Adjustment Fund in 2017 (European Commission, 2017a, 2017b), showing that they do share some kind of relation to their domestic 5G providers. Sweden and Finland might be therefore be quicker to push for securitization than other EU member states because they have the capabilities to become self-reliant in regard to critical telecommunication infrastructure. The EU's securitization of Chinese 5G providers would entail less severe consequences for them than for other, more dependent EU states, lowering their cost of action against the major provider Huawei immensely.

Figure 3: Adapted Causal Mechanism – Internal Influence on Securitization in the EU

X	**Causal mechanism (**Internal Influence on Securitization in EU)					Y
Capabilities of EU members Sweden and Finland in regard to 5G technology	⟶	Swedish and Finnish Policymakers *securitize* Chinese 5G providers in the national context	⟶	Swedish and Finnish Policymakers *urge* fellow EU members to realize the threat stemming from Chinese 5G providers and support/adapt the securitization based on arguments relating to EU principles, therefore initiating securitization within the EU	⟶	Securitization of Chinese 5G Providers in the EU

4 Method and Data

While the theoretical framework provides the basis for the analysis, the method supplies the tool to adequately examine the observed phenomenon. This paper follows a X-centered approach, since the goal of the selected method is to test if and to what degree the chosen theories can explain the observed outcome.

4.1 Theory-Testing Process Tracing

The method of choice is Theory-Testing Process-Tracing (PT), which "enables inferences to be made about whether a causal mechanism was present in a single case along with whether the mechanism functioned as expected" (Beach and Pedersen, 2019, p. 15). Important is the temporal character of the Process-Tracing method, as the causal sequences inherently follow a temporal sequence of events as well (Collier, 2011, p. 824). Furthermore, the deterministic understanding of causality utilized here implies that there is no randomness if our model is well defined (Beach and Pedersen, 2019, pp. 27–28). The term *causal mechanisms* "refers to relatively parsimonious mechanisms that are generalizable to a bounded population of cases" (Beach and Pedersen, 2019, p. 22). While the case of relevance in this bachelor thesis is Huawei, it can be expected that the findings are also applicable to the cases of other Chinese 5G providers in Europe. As the analysis will show, restrictions or expulsion of Huawei's technology and services from infrastructure are commonly justified with ties and responsibilities of Chinese companies toward the Chinese state, making it fairly certain that action against Huawei (and ZTE) would be reiterated toward other Chinese 5G providers. It might even be possible to further generalize some of the results to Chinese companies located within the technological sector that are not 5G providers, as the securitization of Chinese 5G

technology has led to an awareness of the risks of foreign stakeholders in (critical) infrastructure. To prove this assumption, another analysis of the topic would be needed. But how does one develop a concise model for Theory-Testing PT?

According to Beach and Pedersen (2019, pp. 14–15), three consecutive steps are relevant when using Theory-Testing PT: *conceptualization*, *operationalization*, and the *collection of evidence.*

1. *Conceptualization* refers to the deduction of causal mechanisms between our variable of interest X and our outcome Y from existing literature and theorization. They should mention the acting entity as well as the activity itself.
2. The *operationalization* of the causal mechanism is done by linking each section of the hypothesized mechanism to expected observations. Which observations can be expected if the causal mechanisms were indeed present in the case at hand?
3. The *collection of evidence* now serves as the empirical analysis of the case. This step aims to adjust our confidence in whether the previously hypothesized causal mechanisms were present, party present, or even not at all relevant.

This is the entire conceptualization of the paper:

Figure 4: Adapted Causal Mechanisms – Entire Model

<table>
<tr><th>X_1</th><th colspan="5">Causal mechanism (External Influence on Securitization in EU)</th><th>Y</th></tr>
<tr><td>Relative power of U.S. in international system due to capabilities in cyberspace</td><td>⟶</td><td>U.S. Policymakers securitize Chinese 5G providers in the national context</td><td>⟶</td><td>U.S. Policymakers urge its allies to realize the threat stemming from Chinese 5G providers and support/adapt the securitization based on arguments relating to EU principles, therefore initiating securitization within the EU</td><td>⟶</td><td rowspan="3">Securitization of Chinese 5G Providers in the EU</td></tr>
<tr><th>X_2</th><th colspan="5">Causal mechanism (Internal Influence on Securitization in EU)</th></tr>
<tr><td>Capabilities of EU members Sweden and Finland in regard to 5G technology</td><td>⟶</td><td>Swedish and Finnish Policymakers securitize Chinese 5G providers in the national context</td><td>⟶</td><td>Swedish and Finnish Policymakers urge fellow EU members to realize the threat stemming from Chinese 5G providers and support/adapt the securitization based on arguments relating to EU principles, therefore initiating securitization within the EU</td><td>⟶</td></tr>
</table>

4.2 Empirical Data

Theory-Testing Process-Tracing relies on observable manifestations for each part of the theorized causal mechanisms. Put into the context of the study, those manifestations are considered evidence, as they support the assumption that the causal mechanism was present in the analyzed case (Beach and Pedersen, 2019). There are four types of evidence (Beach and Pedersen, 2019, pp. 99–100). Pattern evidence consists of statistical regularities, sequence evidence regards the predicted chronological order of events. Trace evidence "is evidence whose mere existence provides proof that a part of a hypothesized mechanism exists" (Beach and Pedersen, 2019, p. 100), such as the existence of multilateral forums on the topic of Chinese 5G providers. Account evidence pertains to the records of discussions or oral statements. In this paper, the initially predicted evidence includes trace and account evidence, stemming from primary and secondary sources.

To illustrate the predicted evidence for each part of the causal mechanisms, they will now be listed comprehensively. This is equivalent to step two of using Theory-Testing PT, namely the operationalization.

Securitization of Chinese 5G Providers in the EU (Y)	Predicted Observations
- Outcome - (Already analyzed in chapter 2.2)	- Stricter regulations or corresponding policy proposals against Chinese 5G providers - Reports from official EU bodies on the topic of Chinese 5G providers - EU-wide measures to minimize risks posed by 5G technology, especially concerning foreign providers

External Influence on Securitization in the EU	Predicted Observations
Relative power of U.S. in international system due to capabilities in cyberspace (X_1) (Already analyzed as part of the theoretical framework in chapter 3.2)	- Statements of U.S. officials and/or experts about U.S. power in cyberspace - Reports from experts about U.S. power in cyberspace
U.S. Policymakers *securitize* Chinese 5G providers in the national context	- Statements of government officials, intelligence agencies, and/or technology experts, warning against Chinese 5G providers within the country - Policy against Chinese 5G providers, e.g., bans on their product
U.S. Policymakers *urge* its allies to realize the threat stemming from Chinese 5G providers and support/adapt the securitization based on arguments relating to EU principles, therefore initiating securitization within the EU	- Statements of U.S. policymakers towards other states, ideally the EU (e.g. in NATO - Meetings or other security-related forums) - Bi- or multilateral meetings between U.S. and EU, addressing China, Chinese telecommunication companies, and/or 5G technology - U.S. Programs and projects aimed towards exerting influence - Statements made by EU institution/EU policymakers that imply influence by U.S.

External Influence on Securitization in the EU	Predicted Observations
Capabilities of EU members Sweden and Finland in regard to 5G technology (X_2) (Already analyzed as part of the theoretical framework in chapter 3.3)	- Existence of major 5G companies in those countries - Past state interference for advantages for those companies to show relation - Expert statements about 5G capabilities within those countries
Swedish and Finnish Policymakers *securitize* Chinese 5G providers in the national context	- Statements of government officials, intelligence agencies, and/or technology experts, warning against Chinese 5G providers within the country - Policy against Chinese 5G providers, e.g., bans on their product
Swedish and Finnish Policymakers *urge* fellow EU members to realize the threat stemming from Chinese 5G providers and support/adapt the securitization based on arguments relating to EU principles, therefore initiating securitization within the EU	- Statements of Sweden and Finland about 5G and associated risks - Initiation of talks/forums for the topic of (Chinese) 5G providers and associated risks - Statements made by EU institutions/EU policymakers that imply influence by Sweden and Finland

Having completed steps one and two of Theory-Testing PT, specifically the conceptualization and the operationalization, the next part will focus on the collection of evidence, meaning the empirical analysis.

5 Empirical Analysis

The objective of the following chapters is to test the explanatory power of the deducted causal mechanisms based on the expected evidence for each part. It is important to note that there are certain limitations when testing two theories regarding their explanatory power. Since social phenomena are usually the result of multiple, simultaneously existing causes, Theory-Testing Process-Tracing can only analyze whether the theorized causal mechanisms were actually present and if they occurred as anticipated (Beach and Pedersen, 2019, p. 89). Other explanations or causes might still be valid. Furthermore, while the topic of cybersecurity has become more prominent in the last few years, it is still not necessarily the most openly dealt with. Accompanied by the fact that the decision on policy regarding Huawei also carries a geopolitical component for the countries in question, many intelligence reports and similarly confidential or impactful documents might not be publicly accessible.

5.1 U.S. Influence on Securitization in the EU

When regarding the relationship between the U.S. and Huawei, the term *national security* plays a dominant role. As the next chapter will show, actions against the Chinese company were always justified by claims that Huawei's way of conducting business as well as vulnerabilities in their products threaten national security. The understanding of national security, at least in strong, liberal-democratic states such as the U.S., is primarily focused on protecting the subjects

of the state from external threats. It can also apply to "domestic activities deemed unacceptable and threatening by a great majority of the populace", such as domestic terrorism (Buzan et al., 1998, p. 146), but in the case of Huawei, the first interpretation is applicable.

Having established this, we can now move on to the analysis of our first theoretical approach. Did the external influence of the U.S. leverage the process of securitization in the EU? The hypothesized causal mechanism has been separated into two steps. We first expect U.S. policymakers to securitize Chinese 5G providers in the national context, then to see them trying to garner support for their action by appealing to EU principles. The outcome is the securitization of Chinese 5G providers in the EU.

5.1.1 Securitization of Chinese 5G Providers in the United States

The history between U.S. policymakers and Huawei is long. A detailed overview can be attained in the report "Huawei and U.S. Law", prepared by the Congressional Research Service in 2021 (Mulligan and Lindebaugh, 2021). Due to the constraints of this paper, only a few events will be highlighted. One of the earlier mentions of Huawei in U.S. politics can be seen in an investigative report on U.S. national security, published in 2012 and titled "Issues Posed by Chinese Telecommunications Companies Huawei and ZTE" (Rogers and Ruppersberger, 2012). In more than 30 pages regarding Huawei alone, the authors criticized a lack of cooperation during the conducted investigation as well as the absence of transparency concerning possible ties to Chinese governmental institutions. Furthermore, they claimed to have found evidence for unlawful behavior by the company. Over time, there was a growing interest in the U.S. Congress in regard to the protection of critical infrastructure (Lewallen, 2021, p. 1042), which also includes the topic of telecommunication.

Especially the Trump administration targeted Huawei, claiming that their products present a security threat. According to them, the company might be mandated by the Chinese government to share confidential information as well as create backdoors as entry points for espionage (Mulligan and Lindebaugh, 2021, p. 2). Introduced in 2017, the National Defense Authorization Act for Fiscal Year 2018 prohibited the Department of Defense from purchasing products and services from Huawei and ZTE (Thornberry, 2017). On May 15th, 2019, former president Donald Trump declared a national emergency. Titled "Executive Order on Securing the Information and Communications Technology and Services Supply Chain" (Trump, 2019), the order claimed increased capabilities and efforts of foreign adversaries to exploit weaknesses in information and communications technology. In a ruling coming into effect a day later, Huawei Technologies Co., Ltd. and 68 non-U.S. affiliates of Huawei were added to the Entity List. The

reasoning states that "[t]he U.S. Government has determined that there is reasonable cause to believe that Huawei has been involved in activities contrary to the national security or foreign policy interests of the United States" (Bureau of Industry and Security, 2019b, p. 22961). The affiliates were accused of the same wrongdoing. Being on the Entity List meant that the company was now subject to special license requirements while being exempt from most license exceptions. More non-U.S. affiliates of Huawei were added in following rulings (e.g., Bureau of Industry and Security, 2019a). The national emergency declared in 2019 was further aggravated in 2021 when a new Executive Order pinpointed the origin of the threat to China and called for "aggressive action against those who develop or control Chinese connected software applications to protect our national security" (Trump, 2021, p. 1250). While this specific order was revoked by President Biden in June 2021, the emergency declared in 2019 is still ongoing (Biden, 2021).

It is safe to say that there has been an American securitization of Chinese 5G providers and the predicted evidence of the first step of the causal mechanism has been found without exception. There are statements and reports made by government officials warning against Chinese 5G providers and Huawei within the U.S., as well as policies against their products. The topic of Chinese 5G providers was not only politicized but also securitized when it was regarded as a substantial threat requiring immediate and considerable countermeasures.

5.1.2 U.S.-American Tries to Create Awareness in the European Union

> „No administration has been tougher on China than this administration. […] We confronted untrustworthy Chinese technology and telecom providers. We convinced many countries - many countries - and I did this myself, for the most part - not to use Huawei because we think it's an unsafe security risk. It's a big security risk. I talked many countries out of using it. If they want to do business with us, they can't use it." (Trump, 2020)

As illustrated before, the Trump administration was not afraid to openly position themselves against Chinese influence of any kind as well as the usage of products of the Chinese company Huawei. But did they actively try to influence other nations to join their cause? If so, we expect three groups of observations. The first one consists of statements of U.S. Policymakers towards other states, ideally the EU. The second regards bi- or multilateral meetings between the U.S. and EU, addressing China, Chinese telecommunication companies, and 5G technology. Third, one might expect to find official programs or projects regarding 5G technology, aimed towards exerting influence on other countries. A bonus would be to discover statements made by EU institutions or EU policymakers that confirm the suspected influence from the U.S. themselves.

The prime example of U.S. policymakers making statements about Chinese 5G providers is already cited above. In it, former president Trump openly assumes responsibility for the policy other countries asserted towards Huawei. Mike Pompeo, his former secretary of state, made a similar declaration about a year prior. He expressed global U.S. efforts to make other nations aware of the perceived risks associated with Huawei technology, while also establishing that the U.S. will not share any information with countries that do make use of their equipment (Pompeo, 2019). While a lot of similar statements could be cited here, those statements from two of the highest-ranking U.S. policymakers leave no room for interpretation and make additional observations of official statements futile. Nevertheless, it might be interesting to observe statements from the European side. In 2020, the British government told Huawei that their decision to ban the company party resulted from geopolitical aspects and pressure from former U.S. president Trump (Helm, 2020). While the United Kingdom is no longer a part of the EU, other countries in Europe will likely have received similar treatment.

There have been numerous bi- and multilateral meetings between the U.S. and European countries as well as representatives of the European Union. One of the first influential multilateral meetings regarding security in 5G took place in Prague in 2019 and gave the U.S. a platform to provide their insights (U.S. Department of State, 2020). The discussions "regarding the important national security, economic, and commercial considerations that must be part of each country's evaluation of 5G vendors" (U.S. Department of State, 2020) resulted in the so-called "Prague Proposals", providing guidance for the 5G rollout, especially in regard to the sectors policy, technology, economy and security (Government of the Czech Republic, 2019). The EU-US Justice and Home Affairs Ministerial Meetings in the same year (Council of the EU, 2019a, 2019b) further affirmed "that the deployment of 5G network infrastructure needs to be addressed as a matter of priority, as it might pose significant security risks" (Council of the EU, 2019a). A year later, a delegation of the EU Parliament's Committee on Civil Liberties, Justice and Home Affairs headed toward the U.S. to discuss different topics with American policymakers and other stakeholders. The topics included cybersecurity and 5G, as well as supply chain security with a special focus on Huawei (European Parliament, 2020, p. 14). Furthermore, the Center for Strategic & International Studies formed a working group consisting of experts from Asian, European, and U.S. companies and research centers. They aimed to develop different criteria (e.g., Political and Governance Criteria, Business Practices Assessment Criteria, and Cybersecurity Risk Mitigation Criteria) for the trustworthiness of telecommunication networks. This was done at the request of the Department of State, making

the working group evidence for the wish of U.S. policymakers to create awareness of security issues regarding 5G (CSIS Working Group, 2020).

The U.S. has had multiple programs and projects regarding 5G technology, which are either openly targeted toward gaining international influence or at least provide the opportunity to do so. One initiative is the "Digital Connectivity and Cybersecurity Partnership" for foreign countries, which wishes to "promote exports of United States ICT goods and services and increase United States company market share in target markets" while also aiming to "promote the diversification of ICT goods and supply chain services to be less reliant on PRC imports" (U.S. Congress, 2021, p. 3102). The most influential program has been the "Clean Network", which was developed by the Trump administration in 2020. Designed as a program to ensure principles like data privacy and trust in digital applications, it very openly labeled the Chinese Communist Party as a "malign actor" (U.S. Department of State, 2020). Even after the Trump administration has ended, there have been tries by U.S. policymakers to implement even more targeted measures. On February 24th, 2023, for example, Representative Andy Barr introduced a bill called "Countering the PRC Malign Influence Fund Authorization Act of 2023" in the House of Representatives (Barr, 2023). The fund should hold about 300 million dollars per fiscal years 2023 to 2027 and has the goal to counter Chinese influence globally.

Besides all those manifestations that support the first theoretical approach, the EU has also confirmed the hypothesized influence itself. The resolution of the European Parliament already mentioned in chapter 2.2, which unmistakably links the terms China, 5G, and security, states:

> "[The European Parliament] [e]xpresses deep concern about the recent allegations that 5G equipment developed by Chinese companies may have embedded backdoors that would allow manufacturers and authorities to have unauthorized access to private and personal data and telecommunications from the EU" (European Parliament, 2019b).

The fact that this resolution refers back to the U.S. claims against Huawei implies a causal relationship. This quote allows us to make the founded assumption that awareness of EU policymakers for the topic has been (at least partially) caused by U.S. influence. All predicted evidence, including statements of U.S. policymakers, multilateral meetings, and U.S. programs and projects regarding the topic, has been found during this part of the analysis. The influence of U.S. policymakers, initiatives, and programs has even been confirmed through statements made by EU institutions and policymakers.

5.1.3 Preliminary Conclusion

The temporary aspect of causal mechanisms is fulfilled. No change or securitizing moves can be seen in the EU before the prominent allegations of the U.S. against Huawei came to light around 2018/2019. This was when the securitization of Chinese 5G providers, mainly Huawei, started gaining traction in the United States. As demonstrated in the first part of the causal mechanism, the topic of Chinese 5G providers was considered a major threat and legitimated the permission of bans as well as the declaration of a still ongoing national emergency. The U.S. then moved on to actively mobilize the EU to join them in the securitization of Chinese 5G vendors. To do so, they make use of public statements, bi- and multilateral meetings as well as programs and initiatives. Furthermore, the EU openly refers to the U.S. claims, which inherently implies that the U.S. process has come before the EU process in a temporal and causal understanding. It must be noted that the wish of the U.S. to be a leading and therefore influencing power on standards and the execution of 5G technology is still ongoing, which is why the second part of the causal mechanism also included meetings, working groups, and projects of the U.S. after 2019. All in all, one can fairly confidently agree with the declaration of former president Donald Trump cited above. The U.S. has majorly influenced the EU, urging them towards the securitization of Huawei and Chinese 5G providers in general.

5.2 Influence of EU Member States with Domestic 5G Providers on Securitization in the EU

Between 2019 and 2020, most EU member states procured Ericsson and Nokia as their main 5G supplier (European 5G Observatory, 2022). This means that those two companies won the contracts to provide the equipment and services to build and maintain 5G infrastructure in those countries. Media claimed that the European Commission proposed Ericsson and Nokia as alternatives to the Chinese company Huawei (Bellamy, 2020), strengthening the question of the possible influence of Sweden and Finland on the EU discourse.

Knowing this, we can move on to the second theoretical approach. Did the internal influence of EU member states with domestic 5G providers, namely Finland and Sweden, affect the process of securitization in the EU? Here, the hypothesized causal mechanism has been separated into two steps. First, Swedish and Finnish policymakers securitize Chinese 5G providers in the national context, then, they urge fellow EU members to realize the threat stemming from Chinese 5G providers and support and adapt the securitization based on arguments relating to EU principles. The outcome is, once again, the securitization of Chinese 5G providers in the EU.

5.2.1 Securitization of Chinese 5G Providers in Sweden and Finland

In 2020, Sweden banned Huawei and ZTE from providing further 5G technology. The country gave the companies the ultimatum of January 1st, 2025, by which their products must be removed from existing infrastructure. Huawei appealed the ban but was soon dismissed by a Swedish court (Soderpalm and Mukherjee, 2021). This was not well received by China, resulting in what was titled "the worst diplomatic stand-off between Beijing and any EU country" (Lau S., 2021). The decision to ban Huawei and ZTE was apparently conditioned by assessments of the Swedish military and security service. Klas Friberg, who is the head of Sweden's domestic security service, publicly alleged that the Chinese state was heavily involved in intelligence gathering and intellectual theft and urged others to acknowledge this in regard to future 5G infrastructure (Associated Press, 2020). It might be interesting to note that the long-term CEO of Ericsson, Borke Ekholm, opposed a ban on Huawei rather strongly. According to multiple media reports, Ekholm contacted the Swedish Foreign Trade Minister Anna Hallberg to seek support against the measure and indicated that Ericsson might also leave the country if the ban persisted (Alleven, 2021; Lau S., 2021).

Concerning Sweden, all of the predicted evidence for this part of the causal mechanism is fulfilled. There are statements and assessments of intelligence agencies pushing for measures against Huawei as well as actual policies against it. Swedish policymakers identified a substantial threat, which required severe and under other circumstances not necessarily legitimate measures. The sharp opposition of Ericsson CEO Borke Ekholm only strengthens the argument that the ban has indeed been a decision that could not have happened without securitization. The policymakers' acceptance of the threat, once again evident by the country-wide ban, has taken their securitizing moves to the level of securitization. But is this also the case for Finland?

As of June 2023, only the EU member states Denmark, Sweden, Estonia, Latvia, and Lithuania have banned Huawei from providing components for 5G infrastructure, with Portugal and Germany considering harsher laws or even a ban (Espinoza and Gross, 2023). This makes identifying the possible securitization of Huawei in Finland less simple than in Sweden. In 2020, Finland's parliament passed a law allowing the ban of telecom equipment if authorities had grounded suspicions that its usage presents a threat to national security. It did not, in contrast to the Swedish approach, focus on vendors, their country of origin, or certain companies but on the equipment itself (Kauranen and Mukherjee, 2020). The lack of an outright ban on Huawei is something Finland's minister of transport and communications, Timo Harakka, deliberately stressed, which might stem from fears of possible retaliation against

Nokia's position in the Chinese market (The Standard, 2020). This seems to lead to the conclusion that 5G technology has become securitized in Finland, but not Huawei or other Chinese 5G providers themselves. Nevertheless, arguments of national security could still be used against Huawei, which is why the legislation might provide legitimacy for measures against the company. Due to a lack of further material swaying the analysis of Finland in the one or other direction, we have to settle by stating that the confidence in this part of the causal mechanism is weakened. There has been a clear securitization of Huawei and Chinese 5G providers in Sweden, but the case to argue for the existence of securitization of Chinese 5G providers in Finland is much more unconvincing. While 5G security has been recognized and accepted as a pressing issue, Chinese 5G providers have not played a more pronounced role than companies of other countries of origin.

5.2.2 Swedish and Finnish Tries to Create Awareness in the European Union

The causal mechanism inherently relies on the existence of a causal sequence of events. This means that the expectations for this next part of the chain have already been lowered by the lack of clear securitization of Chinese 5G providers in Finland. Expected observable manifestations for this part of the causal mechanism include statements of Sweden and Finland about 5G and associated risks, the initiation of talks or forums as well as (ideally) statements made by EU institutions or EU policymakers that imply influence by Sweden and Finland.

In May 2021, members of the EU Parliament's Committee on Foreign Affairs were able to propose amendments to the draft report about a new EU-China strategy. In the draft version, paragraph 25 called for more strategic autonomy in the EU. The proposed amendment took this way further, adding a call for Chinese firms to undergo security screening before allowing them to invest in certain sectors as well as pointing out the companies Huawei and ZTE by name for not adhering to the EU's transparency standards (European Parliament, 2021, pp. 30–31). While committee members must always consider the European perspective, they are elected nationally and are expected to acknowledge their national context. One example is the Greek representative Demitrios Paicopolos, who pushed for more leniency towards Huawei and permission for Greece to purchase Huawei equipment with a discount if the company offered it (European Parliament, 2019a). The expectation for this part of the causal mechanism is therefore that primarily Swedish and Finnish representatives pushed for the amendment described above. Surprisingly, this is not the case. Out of the eight signatories, none was Finnish, and only one was Swedish. The other seven were Polish, Spanish, Dutch, Bulgarian, Belgian, and Italian representatives. While Finland and Sweden did host the 9th and 10th Computer Security Incident Response Team (CSIRT) Network meeting for the European Union

Agency for Cybersecurity (ENISA) in 2019/2020 (ENISA, 2019, 2020), the place of the conference is decided on a rotating basis and does therefore not equal active tries to initiate or shape the then relatively new discussion surrounding 5G security. There are also no publicly available records of the meetings, meaning that no conclusions can be drawn on the potential influence of both countries. None of the assessable databases of EU institutions show increased efforts of Sweden or Finland to influence the discourse surrounding Huawei. There are no publicized statements by any of the relevant Swedish or Finnish governmental offices in regard to their position towards Huawei or their wishes for EU action. This absence of observable manifestations does of course not mean that both countries lacked support for the EU awareness of the topic. Sweden as well as Finland took action within their national limits (albeit in different severity) and therefore most likely also supported the creation of EU guidelines and policies. What is missing, however, is the predicted dominant position, actively pushing the EU towards the securitization of (Chinese) 5G providers.

Surprisingly enough, the Czech Republic has held a rather strong position against Huawei and Chinese 5G from the beginning. As early as 2018, the Czech national authority for cybersecurity published a warning against the Chinese telecommunication companies Huawei and ZTE, stating that the legal and political circumstances in China could lead to the exploitation of vulnerabilities in their products and services, therefore posing a security risk to its users (Navrátil, 2018). This warning was also referred to by the EU in the resolution “Security threats connected with the rising Chinese technological presence in the EU and possible action on the EU level to reduce them” (European Parliament, 2019b). According to the research of Radu and Amon (2021, p. 6), the Czech Republic was the only EU member state acting before the EU itself. Even the Prague 5G Security Conference on the security of communication networks, which has brought forward the Prague Proposals and is now an annual and rather reputable event, has been initiated and held under Czech leadership (Kovaj, 2023). This paper assumed a more prominent position of EU member states with large 5G providers, but their efforts to influence the discourse toward the securitization of Chinese telecommunication companies seem rather insignificant in comparison to other countries such as the Czech Republic.

5.2.3 Preliminary Conclusion

The analysis of publicly accessible databases as well as governmental and EU websites leads to the conclusion that neither Sweden nor Finland play a dominant role in influencing the securitization of Chinese 5G providers in the EU. Sweden has securitized the company Huawei, even going so far as to ban their equipment and services from existing critical infrastructure until 2025. The case is not as clear in Finland, where a securitization of 5G, but not necessarily

of Chinese 5G vendors has taken place. It is unclear whether there has been an acceptance of the security risks possibly associated with Huawei products and services since no policy papers or official statements about this particular case have been found. Moving on to the EU level, there are no dominant calls for policy measures, lobbying efforts, or other means of influence from either of the countries. Instead, the influence of EU member states on EU policymaking in regard to this topic has largely stemmed from the Czech Republic. Additionally, it must be pointed out that even the national responses of both Nordic countries did not come into effect before 2020, when the first signs of securitization in the EU can be traced back to 2019. While this does not necessarily exclude the possibility of later involvement from the debate, it does seem to suggest that those countries were not the origin of the securitization process in the EU.

6 Conclusion

The empirical analysis paints a rather clear picture. The EU's securitization of Chinese 5G providers, exemplified by the company Huawei, can largely be explained by the influence of U.S. policymakers. This means that the relative power of the U.S. in the international system, supported by their capabilities in cyberspace (X_1), is a viable cause of the securitization within the EU. The U.S. has left no doubt for either step of the causal sequence. The securitization of Huawei has been conducted in a rather undiplomatic and often harsh manner, with China being described in terms like "malign actor" (U.S. Department of State, 2020). The same can be said about their mobilization of the EU and other U.S. allies, with former president Donald Trump even declaring himself the reason for action against Huawei (Trump, 2020). The U.S. proclaims its role and the measures taken to ensure compliance from its allies openly, proving that the first theoretical approach of this paper has merit and exists as hypothesized: External influence played a substantial role in the securitization of Chinese 5G providers in the EU. This is entirely different in the second theoretical approach, which assumed that the capabilities of EU member states with domestic 5G providers (X_2) caused the securitization in the EU. This was based on the belief that they would be the first to realize security risks due to their authority on the topic, while also being the first to push for securitization since they - in contrast to other EU states - would have lower costs for action. EU member states did play a role in influencing the EU, as the case of the Czech Republic shows. The ones with domestic 5G providers, however, namely Sweden and Finland, do not stand out with their tries to influence EU politics. They do not position themselves *against* the securitization of Chinese telecommunication companies but they also do not take the expected, dominant position of support.

This paper touches upon the topic of path dependencies at play in the European securitization process. Keeping in mind that past developments (such as the securitization of Chinese 5G vendors in certain countries) can have major implications on current and future progresses (e.g., the securitization of Chinese 5G providers in the EU and the projected 6G rollout in Europe), this paper showed that the direct influence from the U.S., stemming from its position of power, was relevant for the outcome. To take the thought of path dependencies even further, the thesis illustrated the tries of the U.S. to achieve policy alignment in regard to (cyber)security issues. By making the first step of the causal mechanism the securitization of Chinese 5G vendors in the U.S., the influence exerted on the EU has been a question of whether they can sway the EU to align with their securitization. The American role might have been even more influential than illustrated in this paper, as real developments are way more intertwined that the modeled version utilized here. The decision of Sweden to ban Huawei equipment, for example, is most likely not only based on assessments made by the Swedish military and security service but also on the claims made by U.S. officials. The same can be said for Finland, where researchers claimed to see persistent attempts by the U.S. to influence the country's relationship with China (YLE News, 2020).

While the dust around the 5G rollout in Europe is slowly settling, the EU has already launched efforts to ensure leadership in regard to 6G technology. A part of this is close cooperation with the U.S., including the establishment of common principles and participation in bi- and multilateral exchanges (European Commission, 2023). There has also been the creation of the European 6G Smart Networks and Services Industry Association (6G-IA), which wishes to advance 5G technology as well as research regarding 6G. Its board members include representatives from Nokia and Ericsson, but interestingly enough, also a member from the Huawei Technologies Duesseldorf GmbH Munich Research Center (6G-IA, 2022). Despite the classification of Huawei as a "high-risk supplier" and the calls for an EU-wide ban of the company, there has been no final decision to cut ties with the company in regard to telecommunication infrastructure in Europe. It remains to be seen to which degree and in what form the cooperation will advance in the future.

References

6G-IA (2022) *About the 6G-IA,* 24 June. Available at: https://6g-ia.eu/about/.

(2019a) 'Addition of Certain Entities to the Entity List and Revision of Entries on the Entity List', in *Federal Register*. Available at: https://www.govinfo.gov/content/pkg/FR-2019-08-21/pdf/2019-17921.pdf (Accessed: 14 May 2023).

(2019b) 'Addition of Entities to the Entity List', in *Federal Register*. Available at: https://www.govinfo.gov/content/pkg/FR-2019-05-21/pdf/2019-10616.pdf (Accessed: 14 May 2023).

Alleven, M. (2021) *Ericsson CEO lobbied Swedish minister over Huawei ban: Report*: Wireless. Available at: https://www.fiercewireless.com/wireless/ericsson-ceo-lobbied-swedish-minister-over-huawei-ban-report (Accessed: 26 May 2023).

Associated Press (2020) *Sweden Bans Huawei, ZTE From 5G, Calls China Biggest Threat*: Security Week. Available at: https://www.securityweek.com/sweden-bans-huawei-zte-5g-calls-china-biggest-threat/ (Accessed: 26 May 2023).

Austin, G. (2014) 'Managing Asymmetries in Chinese and American Cyber Power', *Georgetown Journal of International Affairs*, pp. 141–151. Available at: https://www.jstor.org/stable/43773657 (Accessed: 20 June 2023).

Balzacq, T. (2005) 'The Three Faces of Securitization: Political Agency, Audience and Context', *European Journal of International Relations*, 11(2), pp. 171–201. doi: 10.1177/1354066105052960

Barr, A. (2023) *H.R.1157 - Countering the PRC Malign Influence Fund Authorization Act of 2023*. Available at: https://www.congress.gov/118/bills/hr1157/BILLS-118hr1157ih.pdf (Accessed: 24 April 2023).

Beach, D. and Pedersen, R. (2019) *Process-Tracing Methods*. Ann Arbor, MI: University of Michigan Press (Accessed: 15 May 2023).

Bellamy, D. (2020) *EU insists European companies could replace Huawei in 5G network*: EuroNews. Available at: https://www.euronews.com/2020/07/25/eu-insists-european-companies-could-replace-huawei-in-5g-network (Accessed: 19 April 2023).

Biden, J.R. (2021) *Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries,* 24 May. Available at: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/09/executive-order-on-protecting-americans-sensitive-data-from-foreign-adversaries/.

Boeke, S. (2018) 'National cyber crisis management: Different European approaches', *Governance*, 31(3), pp. 449–464. doi: 10.1111/gove.12309

Breton, T. (2023) *5G Security: The EU Case for Banning High-Risk Suppliers: Statement by Commissioner Thierry Breton*. Available at: https://ec.europa.eu/commission/presscorner/api/files/document/print/en/statement_23_3312/STATEMENT_23_3312_EN.pdf (Accessed: 20 June 2023).

Bright, J. (2012) 'Securitization, terror, and control: towards a theory of the breaking point', *Review of International Studies*, 38(4), pp. 861–879. Available at: https://www.jstor.org/stable/41681493 (Accessed: 23 May 2023).

Buzan, B. *et al.* (1998) *Security: A New Framework for Analysis*. Boulder, CO: Lynne Rienner Publishers (Accessed: 4 May 2023).

Collier, D. (2011) 'Understanding Process Tracing', *PS: Political Science & Politics*, 44(4), pp. 823–830. Available at: doi://10.1017/S1049096511001429 (Accessed: 17 April 2023).

Council of the EU (2019a) *Joint EU-US statement following the EU-US Justice and Home Affairs Ministerial Meeting* [Press release]. 19 June. Available at: https://www.consilium.europa.eu/en/press/press-releases/2019/06/19/joint-eu-u-s-statement-following-the-eu-u-s-justice-and-home-affairs-ministerial-meeting/ (Accessed: 23 April 2023).

Council of the EU (2019b) *Joint EU-US statement following the EU-US Justice and Home Affairs Ministerial Meeting* [Press release]. 11 December. Available at: https://www.consilium.europa.eu/en/press/press-releases/2019/12/11/joint-eu-us-statement-following-the-eu-us-justice-and-home-affairs-ministerial-meeting/ (Accessed: 23 April 2023).

CSIS Working Group (2020) *Criteria for Security and Trust in Telecommunications Networks and Services*. Available at: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/200511_Lewis_5G_v3.pdf (Accessed: 25 April 2023).

Dunn Cavelty, M. and Suter, M. (2009) 'Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection', *International Journal of Critical Infrastructure Protection*, pp. 1–9. Available at: https://www.files.ethz.ch/isn/106323/PPP_no_silver_bullet.pdf (Accessed: 23 March 2023).

Dunn Cavelty, M. and Wenger, A. (2020) 'Cyber security meets security politics: Complex technology, fragmented politics, and networked science', *Contemporary Security Policy*, 41(1), pp. 5–32. Available at: doi://10.1080/13523260.2019.1678855 (Accessed: 17 April 2023).

ENISA (2019) *9th CSIRTs Network meeting: Meeting*. Available at: https://www.enisa.europa.eu/events/9th-csirts-network-meeting (Accessed: 24 April 2023).

ENISA (2020) *10th CSIRTs Network meeting: Meeting*. Available at: https://www.enisa.europa.eu/events/10th-csirts-network-meeting (Accessed: 24 April 2023).

ENISA (2023) *Empowering 5G Security with Expertise and Tools*. Available at: https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/telecoms/5g (Accessed: 24 April 2023).

Ericsson (2021) *A guide to 5G network security 2.0*. Available at: https://www.ericsson.com/4a66f8/assets/local/security/09172021-a-guide-to-5g-network-security-2.0.pdf (Accessed: 24 April 2023).

Espinoza, J. and Gross, A. (2023) *EU considers mandatory ban on using Huawei to build 5G*: Financial Times. Available at: https://www.ft.com/content/a6900b0f-08d5-433d-bfb0-f57b6041e381 (Accessed: 9 June 2023).

European 5G Observatory (2022) *Supply market trends (vendors): Major procurements, Open RAN, multivendor deployments*. Available at: https://5gobservatory.eu/supply-market-trends-vendors-major-procurements-open-ran-multivendor-deployments/ (Accessed: 26 April 2023).

European Commission (2015) *The EU and China signed a key partnership on 5G, our tomorrow's communication networks* [Press release]. 28 September. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_15_5715 (Accessed: 25 April 2023).

European Commission (2016) *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: 5G for Europe: An Action Plan*. Available at: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=17131 (Accessed: 25 April 2023).

European Commission (2017a) *Proposal for a Decision of the European Parliament and of the Council: on the mobilisation of the European Globalisation Adjustment Fund following an application from Finland – EGF/2016/008 FI/Nokia Network Systems*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017PC0157 (Accessed: 23 May 2023).

European Commission (2017b) *Proposal for a Decision of the European Parliament and of the Council: on the mobilisation of the European Globalisation Adjustment Fund following an application from Sweden – EGF/2017/007 SE/Ericsson*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017PC0782 (Accessed: 23 May 2023).

European Commission (2018) *Three technologies bring 5G closer to reality: 5Gwireless*. Available at: https://ec.europa.eu/research-and-innovation/en/projects/success-stories/all/three-technologies-bring-5g-closer-reality (Accessed: 26 April 2023).

European Commission (2019a) *Commission Recommendation of 26.3.2019: Cybersecurity of 5G networks*. Available at: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=58154 (Accessed: 12 April 2023).

European Commission (2019b) *Getting ready for the 5G 'revolution': SILIKA*. Available at: https://ec.europa.eu/research-and-innovation/en/projects/success-stories/all/getting-ready-5g-revolution (Accessed: 26 April 2023).

European Commission (2019c) *Joint Communication to the European Parliament, the European Council and the Council: EU-China – A strategic outlook*. Available at: https://ec.europa.eu/commission/presscorner/api/files/attachment/858891/communication-eu-china-a-strategic-outlook.pdf.pdf (Accessed: 17 April 2023).

European Commission (2020) *Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade*. Available at: https://ec.europa.eu/newsroom/dae/redirection/document/72164 (Accessed: 17 April 2023).

European Commission (2021) *EU Toolbox for 5G Security*. Available at: https://ec.europa.eu/newsroom/dae/redirection/document/64577 (Accessed: 15 March 2023).

European Commission (2022) *5G*. Policies. Available at: https://digital-strategy.ec.europa.eu/en/policies/5g (Accessed: 15 March 2023).

European Commission (2023) *6G outlook*. Available at: https://ec.europa.eu/newsroom/dae/redirection/document/96107 (Accessed: 2 June 2023).

European Court of Auditors (2022) *5G roll-out in the EU: delays in deployment of networks with security issues remaining unresolved: Special Report*. Available at: https://www.eca.europa.eu/Lists/ECADocuments/SR22_03/SR_Security-5G-networks_EN.pdf (Accessed: 12 May 2023).

European Parliament (2019a) *Notice to Members*. Available at: https://www.europarl.europa.eu/doceo/document/PETI-CM-638829_EN.pdf (Accessed: 15 April 2023).

European Parliament (2019b) *Security threats connected with the rising Chinese technological presence in the EU and possible action on the EU level to reduce them*. Available at: https://www.europarl.europa.eu/doceo/document/TA-8-2019-0156_EN.pdf (Accessed: 15 April 2023).

European Parliament (2020) *Mission Report: following the Mission to Washington D.C and Boston, United States of America*. Available at: https://www.europarl.europa.eu/doceo/document/LIBE-CR-654092_EN.pdf (Accessed: 15 April 2023).

European Parliament (2021) *Amendments 351-502: Draft Report - A new EU-China strategy*. Available at: https://www.europarl.europa.eu/doceo/document/AFET-AM-693625_EN.pdf (Accessed: 15 April 2023).

European Union (2012) *Charter of fundamental rights of the European Union (2012/C 326/02)*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT (Accessed: 12 June 2023).

Friis, K. and Lysne, O. (2021) 'Huawei, 5G and Security: Technological Limitations and Political Responses', *Development and Change*, 52(5), pp. 1174–1195. Available at: doi://10.1111/dech.12680 (Accessed: 17 April 2023).

Government of the Czech Republic (2019) *Prague 5G Security Conference announced series of recommendations: The Prague Proposals*. Available at: https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/ (Accessed: 23 May 2023).

GSMA (2023) *European 5G Performance Trails its International Peers*: GSMA. Available at: https://www.gsma.com/membership/resources/european-5g-performance-trails-its-international-peers/ (Accessed: 12 March 2023).

Helm, T. (2020) *Pressure from Trump Led to 5G Ban, Britain Tells Huawei*: The Guardian. Available at: https://www.theguardian.com/technology/2020/jul/18/pressure-from-trump-led-to-5g-ban-britain-tells-huawei (Accessed: 13 June 2023).

IISS (2021) *Cyber Capabilities and National Power: A Net Assessment*. Available at: https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/cyber-power-report/cyber-capabilities-and-national-power---a-net-assessment___.pdf (Accessed: 17 April 2023).

ITU (2019) *Global Cybersecurity Index (GCI) 2018*. Available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf (Accessed: 8 April 2023).

Kauranen, A. and Mukherjee, S. (2020) *UPDATE 1-Finland approves law to ban telecoms gear on security grounds*: Reuters. Available at: https://www.reuters.com/article/finland-5g/update-1-finland-approves-law-to-ban-telecoms-gear-on-security-grounds-idUSL1N2IN1O4 (Accessed: 12 April 2023).

Kharpal, A. (2016) *China's Huawei could overtake Apple this year in smartphones, top analyst says*: CNBC. Available at: https://www.cnbc.com/2017/10/16/huawei-could-overtake-apple-this-year-in-smartphones-top-analyst-says.html (Accessed: 15 May 2023).

Kleinhans, J.-P. (2019) *Whom to trust in a 5G world? Policy recommendations for Europe's 5G challenge*. Available at: https://www.stiftung-nv.de/sites/default/files/whom_to_trust_in_a_5g_world.pdf (Accessed: 23 April 2023).

Kovaj, S. (2023) *Prague 5G Security Conference: Statement by NSC Spokesperson Emily Horne* [Press release]. 3 December. Available at: https://cz.usembassy.gov/statement-by-nsc-spokesperson-emily-horne-on-u-s-support-for-the-third-annual-prague-5g-security-conference/ (Accessed: 8 April 2023).

Lau S. (2021) *Sweden Faces Chinese Blowback over Huawei Ban*: Politico. Available at: https://www.politico.eu/article/sweden-faces-chinese-blowback-over-huawei-ban/ (Accessed: 23 April 2023).

Lewallen, J. (2021) 'Emerging technologies and problem definition uncertainty: The case of cybersecurity', *Regulation & Governance*, 15(4), pp. 1035–1052. doi: 10.1111/rego.12341

Mulligan, S.P. and Lindebaugh, C.D. (2021) *Huawei and U.S. Law*. Available at: https://crsreports.congress.gov/product/pdf/R/R46693 (Accessed: 24 May 2023).

Navrátil, D. (2018) *Warning*. Available at: https://info.publicintelligence.net/CZ-NCISA-HuaweiZTE.pdf (Accessed: 24 May 2023).

NIS Cooperation Group (2019) *EU coordinated risk assessment of the cybersecurity of 5G networks: Report*. Available at: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62132 (Accessed: 17 April 2023).

Pompeo, M. (2019) 'Mike Pompeo on Huawei concerns', *Mike Pompeo: Been making sure countries understand the risk of putting Huawei technology into their IT systems*. Available at: https://www.foxbusiness.com/video/6005194321001#sp=show-clips (Downloaded: 27 April 2023).

Radu, R. and Amon, C. (2021) 'The governance of 5G infrastructure: between path dependency and risk-based approaches', *Journal of Cybersecurity*, 7(1). doi: 10.1093/cybsec/tyab017

Rogers, M. and Ruppersberger, D. (2012) *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*. Available at: https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf (Accessed: 6 May 2023).

Sawall, A. (2023) *5G-Risikoanalysen der EU-Kommission zu Huawei sind geheim*: Golem.de. Available at: https://www.golem.de/news/high-risk-vendor-5g-risikoanalysen-der-eu-kommission-zu-huawei-sind-geheim-2306-175226.html (Accessed: 25 June 2023).

Soderpalm, H. and Mukherjee, S. (2021) *Swedish Court Dismisses Huawei Appeal over 5G Network Ban*: Reuters. Available at: https://www.reuters.com/article/us-sweden-huawei-appeal-idUSKBN29K0VE (Accessed: 15 April 2023).

The Standard (2020) *Finland to shut out Huawei from telecom networks*: The Standard. Available at: https://www.thestandard.com.hk/breaking-news/section/2/160597/Finland-to-shut-out-Huawei-from-telecom-networks (Accessed: 26 May 2023).

The White House (2018) *National Cyber Strategy of the United States of America,* https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (Accessed: 6 May 2023).

Thornberry, M. (2017) *H.R.2810 - National Defense Authorization Act for Fiscal Year 2018*. Available at: https://www.congress.gov/bill/115th-congress/house-bill/2810 (Accessed: 24 April 2023).

Trump, D.J. (2019) *Executive Order on Securing the Information and Communications Technology and Services Supply Chain: Executive Order 13873*. Available at: https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/ (Accessed: 24 April 2023).

Trump, D.J. (2020) *Remarks by President Trump in Press Conference* [Press release]. 14 July. Available at: https://trumpwhitehouse.archives.gov/briefings-statements/remarks-president-trump-press-conference-071420/ (Accessed: 24 April 2023).

Trump, D.J. (2021) *Addressing the Threat Posed by Applications and Other Software Developed or Controlled by Chinese Companies: Executive Order 13971*. Available at: https://www.govinfo.gov/content/pkg/FR-2021-01-08/pdf/2021-00305.pdf (Accessed: 24 April 2023).

U.S. Congress (2021) *Text of Amendments; Congressional Record Vol. 167, No. 87*. Available at: https://www.congress.gov/117/crec/2021/05/19/167/87/CREC-2021-05-19-pt1-PgS2789.pdf (Accessed: 2 June 2023).

U.S. Department of State (2020) *The Clean Network*. Available at: https://2017-2021.state.gov/the-clean-network/index.html (Accessed: 16 April 2023).

Wæver, O. (1999) 'Securitizing sectors? Reply to Eriksson.', *Cooperation and Conflict*, 34(3), pp. 334–340. Available at: https://www.jstor.org/stable/45084385 (Accessed: 25 May 2023).

Williams, M.C. (2003) 'Words, Images, Enemies: Securitization and International Politics', *International Studies Quarterly*, 47(4), pp. 511–531. Available at: https://www.jstor.org/stable/3693634 (Accessed: 25 June 2023).

YLE News (2020) *Researcher: US aiming to influence Finland's ties with China*: YLE. Available at: https://yle.fi/a/3-11433957 (Accessed: 26 May 2023).