Universiteit
Leiden
The Netherlands

Securitisation of the 5G rollout in Germany

An analysis of the extent to which the 5G rollout in Germany has been securitised

Name: Nicolas Schuierer

Student Number: s2946343

Thesis Supervisor: Dr. Jan Oster

Programme of Study: European Politics and Society (MA)

Word Count: 18 443

Date submitted: 19 July 2021

Abstract

The fifth generation of mobile communication networks (5G) has the capability to facilitate ground-breaking innovation as well as to contribute to a digital transformation of societies and economies alike. While this new network standard has game-changing potential, it has also brought about security concerns. Due to societies as well as industries being projected to develop a greater dependency on services facilitated by these networks, many countries have grown concerned by potential threats such as espionage or sabotage. This thesis analyses the case of the 5G rollout in Germany placed in a global as well as European context. Securitization Theory is used as a theoretical framework. Embedded in the context of cyber-security the study then tests whether the theory aids in explaining the rollout of the 5G network in Germany. By means of discourse analysis, speech acts from actors in the industry, the media as well as from political actors are examined. The study finds that the rollout of the 5G network in Germany was partially securitised. This study shows that, despite the lack of security incidents, securitisation nevertheless occurred.

Keywords

Securitization Theory, Cyber-Security, 5G rollout in Germany, Case Study, Discourse Analysis

Bibliographic reference

Chicago Manual of Style 17th edition

Declaration

I, Nicolas Schuierer, candidate for the MA Degree European Politics and Society, hereby declare that the present thesis is exclusively my own work, based on my research and only such external information as properly credited in notes and bibliography. I declare that no unidentified and illegitimate use was made of works of others, and no part of the thesis infringes on any person's or institution's copyright. I also declare that no part of this thesis has been submitted in this form to any other institution of higher education for an academic degree.

The Hague, 19 July 2021 Nicolas Schuierer

Table of contents

1. Introduction

1.1. Research outline

The fifth generation of mobile communication networks (5G) has been perceived to herald profound changes to societies and economies across the globe as it has the capability to facilitate ground-breaking innovation as well as to contribute to a digital transformation. These features have been widely recognised and have induced a global competition with the European Union (EU), United States of America (US) and China, amongst others, having assumed pioneering roles. While the potential has been a determinant factor for the rollout of 5G networks, the other side of the coin gives way to security concerns. With the increased capabilities of the new communication networks, societies as well as industries are set to develop a greater dependency on services facilitated by these networks and thereby become more susceptible to potential attacks and infiltrations. Consequently, a debate on security standards for network equipment vendors ensued and the trustworthiness of equipment vendors, especially Huawei Technologies, has been scrutinised. Different countries have polarised the issue to different degrees and have accordingly applied different regulatory approaches ranging from outright bans to installing hurdles for certain vendors. Within the EU, Germany was the last of the big EU economies to regulate the 5G sector. While the novel IT-Security Law 2.0 shied away from banning any specific network equipment vendor, it installed sweeping powers for the government to block the acquisition of untrustworthy vendors. While Germany took a middle way with this approach, it nevertheless expressed its security concerns with this legislation. Against this background, this thesis explores whether the Copenhagen School's Securitization Theory can be helpful in explaining how the 5G rollout in Germany took shape. The theory is based on the premise that security issues are not natural givens that manifest themselves but are constructed as social phenomena by securitising actors. When an issue is successfully securitised, it enables the actor to call for extraordinary measures that deal with the constructed threat by any means necessary. Applied to the case at hand, this raises the question whether security issues surrounding the rollout of the 5G network in Germany were constructed by securitising actors. This thesis approaches this issue with the help of Securitization Theory embedded in the context of cyber-security.

1.2. Research question

This thesis addresses the following research question:

To what extent has the rollout of the 5G network in Germany been securitised?

This thesis employs a theory testing type of research question. In practical terms, this means that the study aims at testing whether Securitization Theory in the context of cyber-security aids in explaining the rollout of the 5G network in Germany.

1.3. Rationale for case selection

Neither amongst the global leaders of the 5G rollout, nor specifically across the EU is there a uniform approach to the 5G rollout. While there is a certain agreed upon harmonisation, EU Member States have designed their individual approaches as well as timelines and have implemented them to their own extent. Thereby, 5G rollouts have taken on different shapes and progressed at varying speeds. That makes it difficult to research the topic uniformly across all EU Member States. Faced with this, the single case of Germany's 5G rollout was chosen as a unit of analysis for two reasons.

To begin with, the case of Germany is a well-suited instance for research within the EU due to the extend and shape of its rollout. According to the EU Commission's Digital Economy and Society Index 2020[1], Germany ranks eighth among Member States in the connectivity-dimension. Most notably within this dimension, Germany ranks first amongst EU Member States regarding 5G readiness[2]. This indicator is based on the amount of spectrum assigned in a Member State and ready for 5G use by the end of 2020[3]. While this indicator does not take into account how operators' take-up and implementation of the available spectrum has unfolded, it nevertheless shows that Germany has laid comprehensive foundations for a prolific 5G rollout. Thus, Germany's rollout has already progressed to a point where it has taken a shape that is substantial enough to serve as an object of study. Moreover, with such a consolidation, the baseline of the rollout will not change, which means that this research avoids the pitfall of aiming at a moving target. With this characteristic, Germany emerges as a

[1] The Index is made up of five dimensions: *connectivity* (demand and supply of fast and reliable broadband connections), *human capital* (internet user skills and advanced skills), *use of internet* (citizens' use of internet services and online transactions), *integration of digital technology* (business digitisation and e-commerce) and *digital public services* (e-Government)

[2] European Commission, 'Digital Economy and Society Index (DESI) 2020 - Germany', 5,6.

[3] European Commission, 'Digital Economy and Society Index (DESI) 2020 - Connectivity', 20.

representative case. Studying Germany's 5G rollout has to potential to capture the circumstances and conditions of a commonplace situation and to produce lessons learned that can be informative about the experiences of other institutions across the board[4].

Second, Germany is a suitable case as it finds itself in a situation that is an illustrative representation of the EU's position. The rollout of 5G infrastructure is a key site where the broader development of international power politics takes place. There is a shift away from a unipolar world with the US as the technology leader, to a bipolar world in which China plays a progressively dominant role in the development of information and communications technology (ICT)[5]. Indeed, China views supremacy in ICT as key in its aspirations to become a major global power[6]. The EU finds itself in the middle of this global competition. On the one hand, the EU is strongly entangled with China economically, as it is the EU's largest trade partner[7], and depends on China's pivotal position in the value chain for ICT, especially regarding hardware. On the other hand, the EU is accustomed to dependency on the US: technologically as the US dominates software development and especially politically as the US remains Europe's prime security guarantor[8]. For Germany the situation is strikingly similar. Among EU Member States, Germany has the strongest economic ties with China, it is the largest trading partner with the country[9]. Furthermore, the US is traditionally a close ally of Germany, and the countries share intelligence in an effort for mutual security. Thus, Germany finds itself walking the same fine line as the EU between US political pressure and Chinese economic dependency. The combination of these attributes is unparalleled within the EU and makes Germany stand out. The specific circumstances of the German rollout emerge as a unique case engendering a second rationale for examination[10].

1.4. Relevance of research

1.4.1. Societal relevance

The societal relevance of the research topic originates from the impact that the 5G network can have. Services utilising the 5G network have the capacity to permeate society as well as

[4] Bryman, *Social Research Methods*, 70.
[5] Kleinhans, 'Europe's 5G Challenge and Why There Is No Easy Way Out'.
[6] Inkster, 'The Huawei Affair and China's Technology Ambitions', 108.
[7] European Commission, 'Client and Supplier Countries of the EU27 in Merchandise Trade 2020'.
[8] Rühlig, Seaman, and Voelsen, '5G and the US–China Tech Rivalry – a Test for Europe's Future in the Digital Age', 1.
[9] Eurostat, 'China-EU - International Trade in Goods Statistics'.
[10] Yin, *Case Study Research : Design and Methods*, 47.

the economy and to bring profound changes to them. Ideally, users not only have access to information about facts, figures and usages of this new technology but also to the underlying reasons of how and why the technology took form in the specific shape that is now available to them. Political decisions played a decisive role in how the 5G rollout was designed. Knowing whether these decisions were influenced by securitisation is relevant to society. It allows creating awareness for whether the shape of the technology with which users interact in everyday life is the result of injected urgency and a political mobilisation. This can form the basis for an educated interaction with 5G services and is a valuable asset in digital literacy.

1.4.2. Scientific relevance

To begin with, there is a warranted claim for examining the rollout of the 5G network in Germany by means of a security oriented theoretical frame. Corresponding to other novel issues, the emergence of cyber-security has affected a high demand for actionable, problem-solving knowledge. Accordingly, the issue has found widespread relevance in the larger policy discourse. Yet, there has been limited systematic theoretical analysis of the topic from the perspective of security studies[11]. Applying a theoretical perspective thus helps to advance an understanding of the effects of cyber-security on politics, especially the influence on shaping threat perceptions, and thus provides insight into the topic which policy approaches are not capable of providing[12].

Taking a step further, the topic warrants an analysis by means of a theory stemming from the field of International Relations theory. Cyber-space carries a particular weight in the broader questions that International Relations scholars study. The discipline is by and large interested in patterns of collaboration and conflict between states and how these patterns connect with shifts in the allocation and character of power in the international system. Technology has become a site where power relations can be seen in operation and where the shaping as well as coordination of the behaviour of political and social actors happens[13]. While, at the outset, cyber-space was deliberately designed to be a system with minimal rules which had no central power and no censor, cyber-incidents as well as events outside the cyber-domain with influence on cyber-security politics acted as catalysers that influenced this design. By

[11] Balzacq and Cavelty, ‘A Theory of Actor-Network for Cyber-Security’, 178.

[12] Kello, ‘The Meaning of the Cyber Revolution: Perils to Theory and Statecraft’, 15.

[13] Dunn Cavelty and Wenger, ‘Cyber Security Meets Security Politics: Complex Technology, Fragmented Politics, and Networked Science’, 10.

effectuating a perception that cyber-space creates and perpetuates insecurity with potentially catastrophic consequences, some incidents gained sufficient social and political salience that they became security politically relevant, bringing states into the arena[14]. Since the issue of cyber-security gained in significance in state interactions, questions of a new type of power arose and how this power source would affect the existing power allocation in the system[15]. Hence, cyber-space is of immediate relevance to International Relations.

Lastly, it can be claimed that Securitization Theory is an apt theory to deploy in the case at hand. The theory is a frequently applied concept stemming from the field of security studies within International Relations theory. The significant basis of this theory is that it recognises speech acts as a powerful means in the pursuit of securitisation. Security is seen as a performative speech act placed in a social context within which the speaker and the audience interact. While traditional security studies perceive threats as given and measurable and presume that security policies are reactions to an objectively existing increase of risks and threats, this concept is rooted in the assumption that security issues can be constructed. It focuses on when and how actors utilise language to frame something as a security issue and what consequences this has for political agenda-setting. Cyber-space and its security are characterised by the unpredictability and high pace of future technological development as well as the dynamic flux of the capabilities of potential adversaries[16]. Thereby, the security of cyber-space tends to have an elusive and evasive nature. A theory grounded in constructivism is a flexible tool that is capable of catering to these characteristics and therefore a particularly suitable means for analysing this field[17].

1.5. Definition of relevant concepts

This section sets out some key concepts of the thesis in order to allow for a better understanding of the scope and concepts used throughout the text.

This thesis approaches the rollout of the 5G network in Germany as a matter of cyber-security. In this context, the "-cyber" prefix is attached to a number of terms. The prefix is derived from the word "cybernetics", which is the study of communication and control in living beings as

[14] Dunn Cavelty and Wenger, 11.

[15] Dunn Cavelty and Wenger, 12.

[16] Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*, 5.

[17] Dunn Cavelty, 8.

well as in machines[18]. Today the prefix has obtained the general meaning of "through the use of a computer" and its combination with other terms creates portmanteau words whose notion is thereby relocated in technical, systemic thinking[19].

Cyber-security is concerned with rendering cyber-space safe. Therefore, the following first account elaborates on cyber-space. Different views have emerged as to how the concept of cyber-space should be understood. These perspectives are pertinent as they form the basis for how security in this realm is conceptualised. On the one hand, cyber-space has been impactfully depicted by means of a place metaphor. This image supports the intuition that the interconnection of computers generates a sort of new place, a man-made domain[20]. Within this conceptualisation, cyber-space is defined as simultaneously occupying a material and virtual realm. It is an environment grounded in physical reality as it occurs within the framework of real geography consisting of servers, cables, satellites, computers, etc.[21]. At the same time, it is a virtual, nonphysical environment whose existence is a social construction shaped by the way in which institutions and users interact with it, talk about it and administer it[22]. On the other hand, the image of the ecosystem has been adduced to describe cyber-space as a set of network technologies as well as network technology customers[23]. Referring to the environment of global digital electronic telecommunications, cyber-space is thereby broader than the internet. It includes the entire spectrum of networked information and communication devices and systems[24]. Fusing them into a vast, interconnected and diverse blanket of electronic interchange creates a network ecosystem that is unparalleled[25]. Lastly, cyber-space has been conceptualised by a mixture of the two views displayed above. Here, cyber-space is seen as the people who participate in it, the information that is stored, transferred and transformed in it, the logical building blocks that make it up (i.e. the applications and software) and the physical foundations that support the logical elements[26].

[18] Choucri, *Cyberpolitics in International Relations*, 7.
[19] Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*, 16.
[20] Dunn Cavelty, 'From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse', 107.
[21] Dunn Cavelty, 'Cyber-Security', 155.
[22] Barnard-Wills and Ashenden, 'Securing Virtual Space: Cyber War, Cyber Terror, and Risk', 111.
[23] Dunn Cavelty, 'From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse', 108.
[24] Deibert, 'Cyber-Security', 172.
[25] Dunn Cavelty, 'Cyber-Security', 155.
[26] Clark, 'Characterizing Cyberspace: Past, Present and Future', 1.

This understanding allows to heed different characteristics across the different layers of the domain and to pay attention to multiple components that vary depending on the region and country[27].

As such, cyber-space has a variety of characteristics that stand out. It is organised transnationally and not through institutional structures of the state system. Furthermore, cyber-space's architecture is formed by a mix of public and private networks. Private sector actors from various countries operate large shares of the core infrastructural components of cyber-space. Thus, its governance is distributed and does not take place within a singular point of control. Instead, there are countless sites of cyber-space governance, each of which involves numerous stakeholders, including governments, businesses and civil society networks[28].

States, societies, individuals and businesses more and more rely on technologies, systems and data located in cyber-space. Cyber-space now permeates all facets of society, politics and economics to the point of being acknowledged as indispensable for civil society, the state and the private sector[29]. Subsequently, cyber-security is concerned with rendering this environment secure. A general account of security can be understood as safety, freedom from the unwanted effects of another's actions, the state of being protected from danger, injury, attack and other detriment and protection against threats of all kinds[30]. Applied to the cyber-realm, cyber-security refers to a set of activities and measures that intend to protect the physical architecture of cybers-space as well as the information, data or software contained in cyber-space from all possible risks[31]. The security of cyber-space appears as distributed. The architecture of cyber-space is mainly privately owned and operated. Yet, it is used by the public and private sectors alike. This interdependent nature creates an environment where emerging risks are shared and where managing that risk requires close cooperation between the public and the private sector. For the public sector, it is technically as well as economically impossible to design and safeguard the architecture to withstand all disruptions, intrusions or attacks. In order to manage the residual risk, the responsibility for creating security is put on the shoulders of non-state actors. Thereby, the traditionally sovereign act of making society

[27] Deibert, 'Trajectories for Future Cybersecurity Research', 533.
[28] Deibert and Rohozinski, 'Risking Security: Policies and Paradoxes of Cyberspace Security', 16.
[29] Deibert, 'Cyber-Security', 172.
[30] Nissenbaum, 'Where Computer Security Meets National Security', 64.
[31] Dunn Cavelty, 'Cyber-Security', 155.

secure has lost its exclusivity. Securing cyber-space requires engagement with the civilian and private actors of society. Thereby, security is moved into society. Responsibility becomes distributed and shared[32].

1.6. Reading guide

The goal of this research is to examine whether securitisation occurred in the course of the rollout of the 5G network in Germany. To this end, Chapter 2 of this thesis presents a theoretical framework for an analysis as well as the framework's contextualisation within cyber-security and a review of pertinent literature. The ensuing Chapter 3 embeds this framework in a research design. Here, topics such as research design and operationalisation are covered. Chapter 4 proceeds to elaborate on the context of the studied case. The chapter provides an account of the quintessence of 5G networks and then proceeds to gradually zooms in from an international perspective to the national context of Germany's 5G rollout. Chapter 4 covers the analysis of the sampled data. It first outlines how the data is collected and exploited and focuses on analysing speech acts surrounding the rollout of the 5G network in Germany. Lastly, Chapter 5 presents a conclusion. In this chapter the research question will be answered.

2. Theoretical framework

The theoretical framework of this thesis encompasses the Copenhagen School's Securitization Theory as an independent variable to the dependent variable of the rollout of the 5G network in Germany. This theory caters to the deductive nature of the research and forms the analytical framework for the thesis. Before being put to the test, the theory must first be explained and its content, functioning and role have to be demonstrated. This chapter serves this purpose. It gives a general account of Securitization Theory, outlines how cyber-security fits into the theoretical framework and lastly reviews the existing literature on the Copenhagen School's Securitization Theory embedded in cyber-security.

[32] Dunn Cavelty, 161.

2.1. Securitization Theory

2.1.1. Introduction

The theory of securitisation is commonly associated with the Copenhagen School of security studies. The concept first entered the realm of International Relations theories after Ole Wæver outlined it in 1995, and in 1998 it was comprehensively elaborated by Buzan, de Wilde and Waever in their book *Security: A New Framework for Analysis*[33]. The term "Copenhagen School" was subsequently coined by a critique of the authors' works[34].

Securitisation can be defined as "*the discursive process through which an intersubjective understanding is constructed within a political community to treat something as an existential threat to a valued referent object, and to enable a call for urgent and exceptional measures to deal with the threat*"[35].

In this understanding, security is not perceived in reference to particular topics or phenomena but rather as certain logic and process. This process of securitisation can be visualised as a spectrum running from non-politicized through politicised to securitised. An issue is non-politicised when it is not a topic for state action and is not incorporated in public debate[36]. An issue becomes politicised when it is administered in the political system as part of public policy and therefore requires government decisions as well as resource allocation[37]. Lastly, an issue can be mapped at the securitised end of the spectrum when it is considered as an existential threat and thus allows responses which go beyond the state's standard political practices[38].

Central to the Copenhagen School's understanding of securitisation is the discursive process marking the starting point of a securitisation move. The discursive process takes place between a securitising actor and an audience by means of a discursive representation of a particular matter as an existential threat to a valued referent object.

This paraphrase contains a number of elements which are explored in the following.

[33] van Munster, 'Securitization'.
[34] Mcsweeney, 'Identity and Security: Buzan and the Copenhagen School', 81.
[35] Buzan and Wæver, *Regions and Powers : The Structure of International Security*, 491.
[36] Emmers, 'Securitization', 175.
[37] Buzan, Wæver, and Wilde, *Security : A New Framework for Analysis*, 23.
[38] Peoples and Vaughan-Williams, *Critical Security Studies : An Introduction*, 116.

2.1.2. Speech Acts

In order to flesh out the discursive representation the Copenhagen School draws upon Speech Act Theory, a particular branch of the theory of language. Speech Act Theory proposes the concept of performative utterances: often utterances are equivalent to actions; when we say particular phrases or words, we perform a certain action, we do things with words[39]. Thereby, performative utterances do not merely describe and mirror the world but have the potential to create reality[40]. They constitute the opposite of constitutive speech acts, which merely report states of affairs and are therefore subject to truth and falsity tests[41]. The utterance itself then is the act. Consequently, a speech act alone can transform an issue into a security question, irrespective of whether the matter factually represents an existential threat. A securitising actor can use language to articulate an issue in security terms with the goal of persuading a relevant audience of its immediate danger[42]. The meaning inherent in the word security is secondary to the act of saying security. Thus, by saying security securitisation begins[43].

With this focus on speech acts, The Copenhagen School distinctively differs from other conceptions of how to construct security. Within the academic debate, there exists a variety of different strands. The Paris School, a sociologically oriented approach, suggests paying attention to routine practices by means of which issues are defined as matters of security. Scholars in this field argue that security is embedded in bureaucratic practices of security practitioners. These professional managers of unease advance securitisation with the help of routine procedures that connect otherwise disparate issues and thereby contribute to a security continuum[44]. Furthermore, a range of scholars has suggested that visual representations can be essential for the construction of security. Images can be central to the establishment of dominant perceptions of security and threat[45]. Their immediacy, ambiguity and circulability can change the dynamics of securitisation by increasing both the extend of

[39] Peoples and Vaughan-Williams, 116.
[40] Stritzel, 'Towards a Theory of Securitization: Copenhagen and Beyond', 361.
[41] Balzacq, 'A Theory of Securitization : Origins, Core Assumptions, and Variants', 1.
[42] Emmers, 'Securitization', 176.
[43] Peoples and Vaughan-Williams, *Critical Security Studies : An Introduction*, 117.
[44] Bigo, 'Security and Immigration: Toward a Critique of the Governmentality of Unease', 63–92.
[45] McDonald, 'Securitization and the Construction of Security', 569.

actors that can partake in the construction of security as well as the types of audiences with which these actors interact[46].

With its linguistic approach, the Copenhagen School leans on speech acts for the construction of security issues. The critical political quality of speech acts of security is a break in the customary political rules of the game[47]. By expressing limits as well as bringing limits into being, this practice creates boundary conditions. Thereby speech acts rupture a given situation in a decision to create and bring about certain calculable consequences for others[48]. Thus, it is their decisional character that gives speech acts their importance.

2.1.3. Speech acts' content: threat to referent object

The speech act's content comprises an existential threat to a valued referent object.

Framing the concept of the threat as having to be existential shows that the very existence of the referent object is at stake. As the Copenhagen School argues that security is in essence about survival, an existential threat is on hand when the survival of a referent object is called into question[49].

The referent object then is the thing that is seen to be existentially threatened and that has a legitimate claim to survival[50]. In line with traditional security studies, the Copenhagen School views the state as a possible referent object. However, the School moves away from this exclusively narrow understanding and advocates for widening the definition of security beyond the focus on the military sector. Accordingly, it adopts a multi-sectoral approach and identifies four other general sectors of security: environmental, economic, societal and political security[51]. While compartmentalising security into these sectors can carry the risk of consolidation, this design should rather be viewed as a means for differentiating how processes of securitisation unfold in various empirical areas. Accordingly, sectors are rather lenses or discourses instead of objectively existing phenomena, and are defined by certain types of threats as well as by the correlative rhetorical structure of securitisation[52]. Thereby, the design is flexible and is open to other entities becoming referent objects.

[46] Hansen, 'Theorizing the Image for Security Studies: Visual Securitization and the Muhammad Cartoon Crisis', 51–74.

[47] Huysmans, 'What's in an Act? On Security Speech Acts and Little Security Nothings', 372.

[48] Huysmans, 373.

[49] Peoples and Vaughan-Williams, *Critical Security Studies : An Introduction*, 115.

[50] Buzan, Wæver, and Wilde, *Security : A New Framework for Analysis*, 36.

[51] Emmers, 'Securitization', 174.

[52] van Munster, 'Securitization'.

2.1.4. Enunciator: securitising actor

The speech act is uttered by a securitising actor. This position can be adopted by government elites as well as by non-state actors such as the media. Yet, as authority to a great extend lays with actors in powerful, privileged positions, the securitising actor often happens to be the government and its elites. In a democratic system, a government benefits from the legitimacy obtained through elections, supplying it with a significant advantage on the pursuit to convince an audience of the need for exceptional measures[53].

2.1.5. Felicity conditions

For performative speech acts to be effective, certain facilitating conditions have to be fulfilled. These are so-called felicity conditions, and the Copenhagen School sets them up threefold.

First, the speech act must follow the grammar of security. It must construct a plot that encompasses an existential threat, a point of no return and extraordinary measures to combat the threat representing a possible way out[54]. Second, the enunciator must hold a position of authority and social or political capital[55]. For the actor attempting to securitise a certain issue this is a necessary factor in order to convince an audience of the existence of an existential threat. The speaker's authority influences the relationship with the audience and, as a consequence, the likelihood of the audience accepting the claims made in a securitizing attempt[56]. Usually, the actors designated as security experts are taken to have the competence to speak authoritatively on what represents a security issue based on their qualifications, whereas non-experts are typically not taken to have the same capacity to speak security[57]. Third, speech acts referring to conditions or features of the alleged threats that facilitate or impede security have it easier to present an issue as an existential threat and thus increase its chances of success[58]. It is more likely that a securitising actor can evoke a security threat if there are certain objects to associate with that are commonly held to be threatening, such as tanks for example. These objects per se don't constitute a threat but they nevertheless

[53] Emmers, 'Securitization', 176.

[54] Buzan, Wæver, and Wilde, *Security : A New Framework for Analysis*, 33.

[55] Vuori, 'Illocutionary Logic and Strands of Securitization: Applying the Theory of Securitization to the Study of Non-Democratic Political Orders', 70.

[56] Stritzel, 'Towards a Theory of Securitization: Copenhagen and Beyond', 364.

[57] Peoples and Vaughan-Williams, *Critical Security Studies : An Introduction*, 118.

[58] Buzan, Wæver, and Wilde, *Security : A New Framework for Analysis*, 33.

can facilitate the construction of a threat through speech acts[59]. What's more, objects associated with the issue often times carry historical connotations of threat, harm and danger or have a history of hostile sentiments[60]. Consequently, referring to properties of external conditions can enhance the speech act's prospect of success.

2.1.6. Audience

Finally, there is the recipient of the securitising actor's presentation of a matter as a threat. While a speech act on its own can be productive of security as a form of linguistic representation that can position a particular issue as an existential threat, the Copenhagen School leans towards an intersubjective understanding of security where speech acts are defined as securitising moves that become securitisation through audience consent[61]. The Copenhagen School outlines the audience as "those the securitizing act attempts to convince to accept the exceptional procedures"[62]. The reason for describing the audience in such a way is that an issue is securitised solely if and when the audience accepts it as such[63]. Thereby, a certain threat is no longer merely assessed but its interpretation and representation are negotiated between the actor and the audience: while the actor can put forward a particular recognition and representation, it is the audience which decides over the proposal being accepted as common narrative[64]. In a discipline where the security attribute of an issue has predominantly been seen as immanent to their objective nature, arguing that security problems are established intersubjectively has been an important contribution by the Copenhagen School[65]. However, the outlined description reveals only little about the audience itself but rather restates its task in the securitisation process[66]. This factor has evoked the criticism that the Copenhagen School has left the concept of the audience underdeveloped[67]. Accordingly, criticism points out that in the School's formulation of Securitization Theory there is an inherent tension between subjectivity and intersubjectivity: on the one hand securitisation is conceptualised as a speech act event and thereby subjective, while on the

[59] Wæver, 'The EU as a Security Actor — Reflections from a Pessimistic Constructivist on Post-Sovereign Security Orders', 253.
[60] Peoples and Vaughan-Williams, *Critical Security Studies : An Introduction*, 118.
[61] McDonald, 'Securitization and the Construction of Security', 566.
[62] Buzan, Wæver, and Wilde, *Security : A New Framework for Analysis*, 41.
[63] Buzan, Wæver, and Wilde, 25.
[64] Stritzel, 'Towards a Theory of Securitization: Copenhagen and Beyond', 363.
[65] Balzacq, Léonard, and Ruzicka, '"Securitization" Revisited: Theory and Cases', 501.
[66] Côté, 'Agents without Agency: Assessing the Role of the Audience in Securitization Theory', 547.
[67] Williams, 'The Continuing Evolution of Securitization Theory', 213.

other hand it is the outcome of a negotiated interaction between the actor and the audience and thereby intersubjective[68]. This indecisiveness between describing the securitisation process as an intersubjective process while at the same time heavily focusing on the securitising actor's speech act and thereby attributing hardly any significance to the audience lies at the core of the critique. While critical voices thus postulate a more concise and differentiated outline of the audience, there is also awareness that specifically defining who the audience is risks decontextualising the audience as well as attributing an essential characteristic to it. This has the potential to limit the scope of the audience analysis and can have the effect of pigeon-holing Securitization Theory into certain conceptions of politics[69]. In order to resolve this situation different conceptualisations of the audience have been put forward. One suggestion defines the audience by its "ability to provide the securitizing actor with whatever s/he is seeking to accomplish with the securitization"[70]. Another position suggests considering the audience as an entity that "empowers the securitizing actor to act"[71]. Lastly, a further sentiment contends to define audience as "the individual(s) or group(s) that has the capability to authorize the view of the issue presented by the securitizing actor and legitimize the treatment of the issue through security practice"[72]. To sum up, different works attempt to resolve the definitional conundrum by introducing a capabilities definition of the audience.

This thesis acknowledges the expressed criticism as regards the tension that arises from the Copenhagen School's definition of the audience and the shortcomings to flesh out the characteristics of the audience. Nonetheless, this text will not explore an audience defined through a capabilities-trait but will apply the Copenhagen School's original approach. The reason for this is that this thesis attempts to test the original theory itself. Consequently, it will only be explored who the securitising actor attempts to convince and whether this audience was accepting.

[68] McDonald, 'Securitization and the Construction of Security', 573.

[69] Côté, 'Agents without Agency: Assessing the Role of the Audience in Securitization Theory', 548.

[70] Vuori, 'Illocutionary Logic and Strands of Securitization: Applying the Theory of Securitization to the Study of Non-Democratic Political Orders', 72.

[71] Balzacq, Léonard, and Ruzicka, '"Securitization" Revisited: Theory and Cases', 500.

[72] Côté, 'Agents without Agency: Assessing the Role of the Audience in Securitization Theory', 548.

2.1.7. Result of securitisation

With regard to the result of a successful securitising move the Copenhagen School maintains that the securitising actor is provided with the special right to call for urgent and exceptional measures to deal with the threat. Here, the School points out that the success of the process is not necessarily determined by the adoption of such actions. It suffices that the argued existential threat gains enough resonance for a platform to be made from which it is possible to justify the measures which otherwise would not have been possible[73]. This grammar of security is marked by a range of notable characterisations: the issue in questions is elevated to absolute priority, a need for new policies is voiced alongside with other political options becoming closed down, larger available budgetary resources are called for, public discussion is restricted and the circle of those endowed with decision-making is narrowed down[74]. The aspired measures then go beyond rules generally abided by and are situated outside the customary bounds of political procedures and practices: they specifically address a critical incident and can encompass powers and actions that are not legislated[75]. While the types of aspired measures depend on the specific context, they essentially attempt to transform existing patterns of practices.

2.1.8. Positioning Securitization Theory withing International Relations theory

The Copenhagen School's Securitization Theory occupies a distinctive position in the stream of International Relations theory. Essentially, it resides at the intersection of constructivism and realism[76]. At its base, the theory has a close affinity with social constructivism. It views security issues not as natural givens that manifest themselves but argues that they are created as social phenomena[77] which then in turn become institutionalised and are taken as real and as indisputable as the physical reality that can tangibly be experienced[78]. Thereby the theory aligns with social constructivism which is concerned with the formation of social realities: how certain issues are constructed not solely based on objective facts but take shape due to human interaction in a social world[79]. On the other hand, the theory pays heed to the idea of

[73] Buzan, Wæver, and Wilde, *Security : A New Framework for Analysis*, 25.
[74] Balzacq, Léonard, and Ruzicka, '"Securitization" Revisited: Theory and Cases', 518.
[75] Emmers, 'Securitization', 177.
[76] Balzacq, Léonard, and Ruzicka, '"Securitization" Revisited: Theory and Cases', 496.
[77] Huysmans, 'Defining Social Constructivism in Security Studies: The Normative Dilemma of Writing Security', 42.
[78] Vuori, 'Constructivism And Securitization Studies', 64.
[79] Fierke, 'Constructivism', 164–65.

existential threats and corresponding national survival. With this, it adheres to a notion of realism: it assumes that insecurity derives from the objectively threatening complexion of particular matters that call for the use of force in order to secure survival[80]. By placing the concept of securitisation in this framework, the theory carries forward a realist meaning of security[81]. To conclude, Securitization Theory can be seen as constructivist model with an incorporation of realism[82].

2.2. Securitisation of cyber-space

Having elaborated on the general structure of Securitization Theory, this part sets out how cyber-security fits within the theory's framework. For this, the subsequent sections showcase how the theory's constituent components can be fleshed out in the cyber-context.

2.2.1. Introduction

As outlined above, the Copenhagen School advocates for widening the scope of security issues beyond the state as main referent object. The originally proposed sectors aren't conclusive but examples of lenses through which types of threats can be distinguished. Therefore, this approach allows to incorporate other sectors whose dynamics cannot be reduced to one of the established sectors. The security of cyber-space embodies such characteristics and warrants to be considered as a standalone sector. It encompasses a distinct referent object as well as a wealth of securitising actors and threat constellations which allows to theorise cyber-security as a distinct sector. In order to flesh out this conjuncture, this thesis refers to the work of leading scholars in the field. Drawing on the works of Deibert[83], Hansen and Nissenbaum[84] and Dunn Cavelty[85], the following section sets out how cyber-security fits in with the Copenhagen School's Securitization Theory.

2.2.2. Referent object

Contemplating the scope of cyber-security, a constellation of various referent objects appears.

[80] Balzacq, Léonard, and Ruzicka, '"Securitization" Revisited: Theory and Cases', 496.

[81] Stritzel, 'Towards a Theory of Securitization: Copenhagen and Beyond', 360.

[82] Emmers, 'Securitization', 177.

[83] Deibert, 'Circuits of Power: Security in the Internet Environment', 115–42.

[84] Hansen and Nissenbaum, 'Digital Disaster, Cyber Security, and the Copenhagen School', 1155–1175.

[85] Dunn Cavelty, 'From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse', 105–122.

To begin with, cyber-space's character as critical infrastructure stands out as a referent object. Critical infrastructure is predominantly concerned with the role of things in society, their functioning and their resilience. Material objects appear for the provision of services and thereby contribute to social order as well as societal cohesion and are therefore considered as the core rationale for protection[86]. Infrastructure is the very foundation of society. Societies are grounded in infrastructure, and their functioning, continuity and viability are made possible by the protection of infrastructure[87]. Infrastructures are deemed critical based on their vital, crucial and essential role for the functioning of society and because their destruction or disruption harbours the potential for major crisis. Cornerstones of critical infrastructure include, among others, electricity, water and fuel supply, telecommunications, transportation, health and financial services[88]. Nowadays, these elements are exhaustively cybered: information infrastructures are facilitators between material objects and physical infrastructure. Bridged and intertwined by information pathways, the body of critical infrastructures is viewed as interdependent, interconnected and highly complex. Thereby, the image of modern critical infrastructure has become one in which the human and the technology become inextricably intertwined. Technology is not merely a tool that makes life liveable, it becomes constitutive of a specific image of society: a society that is inseparable from technologised critical infrastructure[89].

Another referent object can be business networks. Here, the maintenance of business continuity for an individual, corporate or local actor is affected[90]. As business structures have moved away from fixed locations towards multi-location flexibility, the underlying logic is to sustain and bolster a friction-free communications environment in which ideas, data, financial transactions can move freely and with as much speed as feasible across borders and around the world. This ensures that the functioning of global capital markets is upheld[91].

Moreover, computer networks appear as a referent object. At the core of this referent object are the goals of ensuring availability of systems, information and networks to users, safeguarding the integrity of networks and guaranteeing the confidentiality of information

[86] Aradau, 'Security That Matters: Critical Infrastructure and Objects of Protection', 492.
[87] Aradau, 500–501.
[88] Bendrath, 'The Cyberwar Debate: Perception and Politics in US Critical Infrastructure Protection', 81.
[89] Dunn Cavelty, 'From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse', 114.
[90] Dunn Cavelty, 'Cyber-Security', 155.
[91] Deibert and Rohozinski, 'Risking Security: Policies and Paradoxes of Cyberspace Security', 19.

and communication within the networks[92]. Here, the focus lies on ensuring a network that possesses as little software failures as possible as well as makes it as difficult as possible to penetrate from the outside[93].

Lastly, national security encompassed by military networks can be discerned as a referent object. Corresponding to the deeply entrenched paradigm of a state's national security, the concern for power and authority of the state apparatus takes precedence. Within this twofold concern, the former dimension relates to securing a state's power in cyber-space, whereby this dimension is seen as a potentially new medium of warfare or, more realistically, as a site of sporadic low-level electronic disruptions carried out by so-called rogue states, terrorists or other nonstate actors[94]. The latter dimension is concerned with the possible loss of state control over information flows within and out of the country. Overall, the goal is to secure state authority from vulnerability by ensuring state sovereignty outwardly as well government security inwardly[95].

Following Hansen's and Nissenbaum's assessment, this thesis holds that the cyber-security sector is composed of a constellation of these referent objects, rather than separate referent objects. Multiple discourses surrounding these referent objects exist. Yet, they are not isolated but they overlap. Perceiving them as fragmenting along the lines of distinct referent objects would downplay the way in which cyber-security discourse obtains its coherence from making connections between referent objects rather than at separate tracks. Tying these referent objects together allows to heed the existing interconnectedness[96].

2.2.3. Security threat

Corresponding to the referent objects outlined above, there is a variety of threats. The referent object critical infrastructure is threatened by disruption or destruction, the referent object business networks by espionage of cyber-criminals, the referent object computer

[92] Nissenbaum, 'Where Computer Security Meets National Security', 63.
[93] Hansen and Nissenbaum, 'Digital Disaster, Cyber Security, and the Copenhagen School', 1160.
[94] Deibert, 'Circuits of Power: Security in the Internet Environment', 122.
[95] Deibert, 'Trajectories for Future Cybersecurity Research', 535.
[96] Hansen and Nissenbaum, 'Digital Disaster, Cyber Security, and the Copenhagen School', 1163.

networks by malware and hackers and lastly the referent object national security is threatened by cyber-terrorism and cyber-espionage[97].

2.2.4. Securitising actor

Furthermore, the field of cyber-security has a various array of securitising actors who can engage in uttering speech acts. Actors can stem from the government, can be business actors, technical experts or the media[98].

2.2.5. Audience

The identity of a securitisation audience depends on the specific securitisation process in question. Given the variety of invoked referent object, the audience varies. The audience can be society, actors in the business sector or it can also be political actors[99].

2.2.6. Felicity conditions

Contemplating the felicity conditions surrounding the speech act, slight adjustments have to be made. While speech acts can engulf themselves in the grammar of security and can be enunciated by an authoritative figure, it is not possible for them to conjure up an association with what is commonly held to be threatening. Cyber securitizations have no similar history of founding incidents to base themselves on[100].

2.2.7. Conclusion

The foregoing text has set out the characteristics of Securitization Theory and has elaborated on how cyber-security can fit within this framework. These aspects will be taken up again and exploited in the case study sampling as well as the operationalisation.

[97] Dunn Cavelty, 'From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse', 109.

[98] Balzacq and Cavelty, 'A Theory of Actor-Network for Cyber-Security', 180; Nissenbaum, 'Where Computer Security Meets National Security', 67.

[99] Hansen and Nissenbaum, 'Digital Disaster, Cyber Security, and the Copenhagen School', 1165; Dunn Cavelty, 'From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse', 117.

[100] Hansen and Nissenbaum, 'Digital Disaster, Cyber Security, and the Copenhagen School', 1164.

2.3. Literature review and knowledge gap

Having set out Securitization Theory and cyber-security's incorporation, the following section gives an overview of the existing research within this sector.

2.3.1. Introduction

Past research on cyber-security has been rather fragmented. Different bodies of literature on the topic exist yet do not tend to form a cohesive area of research. While initially these bodies appeared to have not been informed by each other, they have moved towards certain overlaps and interconnectedness[101].

To begin with, literature on the emergence of information society sets out how it developed but says very little about security and, when it does, the emphasis mostly lies on the security of markets and firms rather than the security of societies and states[102].

In addition, there is a large body of specialist literature on information warfare and cyber-security. It is a field populated by technically educated military analysts and security experts whose traditional expert knowledge has been concerned with the hard facts and issues of conflict and military strategy[103]. Written work in this field tends to fall into either one of two categories. A number of contributions has applied an alarmist framing over sober analysis, alluding to disaster scenarios such as "electronic Pearl Harbour", "cyber 9/11" or "weapons of mass disruption"[104]. This was the case predominantly in the 1990s and early 2000s when the issue of cyber-security emerged. In response to that, more cautious contributions have come forth condemning the preceding phrasing as fear mongering and pointing to the practical difficulties of a serious cyber-attack[105]. Typically, these contributions come in the form of policy analyses, make little contact with the more general research and theory and seldomly involve the application or development of theory[106].

[101] Dunn Cavelty and Wenger, 'Cyber Security Meets Security Politics: Complex Technology, Fragmented Politics, and Networked Science', 17.

[102] Eriksson and Giacomello, 'The Information Revolution, Security, and International Relations: (IR) Relevant Theory?', 223.

[103] Eriksson, 'Cyberplagues, IT, and Security: Threat Politics in the Information Age', 217.

[104] Bendrath, Eriksson, and Giacomello, 'From "Cyberterrorism" to "Cyberwar", Back and Forth : How the United States Securitized Cyberspace', 58.

[105] Eriksson and Giacomello, 'Introduction: Closing the Gap between International Relations Theory and Studies of Digital-Age Security', 8.

[106] Eriksson and Giacomello, 'The Information Revolution, Security, and International Relations: (IR) Relevant Theory?', 227.

Lastly, there is the theoretically oriented field of security studies within International Relations theory. Its aim is to touch upon the influence of the information revolution for the common understanding of security in today's world as well as to elucidate variation in security relations and policies throughout the world.

In order to create a pertinent review, the following overview explores and sketches out existing research literature on the nexus of cyber-security and the Copenhagen School's Securitization Theory.

The security of cyber-space is a topic which did not attract the attention of early contributions on Securitization Theory. In fact, the founders of the theory implied its rather subordinate significance when reviewing computer hackers[107]. Nonetheless the recent past has seen an increment in the number of studies applying Securitization Theory to the issue of cyber-space. This increase springs from two correlative trends. To begin with, states', societies' and businesses' heightened reliance on cyber-space offered fertile grounds for a range of actors to generate novel securitising moves identifying a variety of threats[108]. Second, the end of the Cold War opened a window for security beyond the prevailing focus on conventional war and nuclear threats between states. This initiated a search for the new threats and risks to protect against[109].

2.3.2. Literature review

Eriksson explores why information technologies were securitised only in the late 1990s even though political decision makers had been aware of the vulnerability of computer systems since their inception[110]. In order to analyse information technologies as a source of national security threats he examines the case of IT security policy in Sweden. As a means for investigating how information technologies became part of the security agenda, he utilises the concept of framing and illustrates how it corresponds to the Copenhagen School's Securitization Theory. From this standpoint he sets out how successful framing resulted in placing IT security on the political agenda. In his study he furthermore shows how the framing of information technologies as a security issue simultaneously emerged from separate policy realms intertwining civilian viewpoints and threat defence policy. Even though Eriksson

[107] Buzan, Wæver, and Wilde, *Security : A New Framework for Analysis*, 25.

[108] Balzacq, Léonard, and Ruzicka, '"Securitization" Revisited: Theory and Cases', 515.

[109] Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*, 27.

[110] Eriksson, 'Cyberplagues, IT, and Security: Threat Politics in the Information Age', 211–22.

applies his study exclusively to the case of Sweden, he still showcases a bigger picture of how policies propagate internationally by means of imitation as the applied threat frames relevant to IT originated in the United States.

Bendrath, Eriksson and Giacomello examine the different developments in the securitisation of cyber-space in the United States during the early 1990s until the early 2000s[111]. For this, they adopt an approach which incorporates the Copenhagen School's Securitization Theory but goes beyond it by utilising the three factors of frame characteristics, frame actors and contextual conditions into their analysis. They find that, despite multiple securitising moves, the administration of President Clinton securitised the issue of cyber-security merely in rhetoric. Yet, this period also includes that a link between cyber-security and infrastructure was established. Beyond that, the US government implemented hardly any measures in practice. Subsequently, the authors show how the Bush administration oscillated between framing cyber-threats in terms of cyber-terrorism and in terms of interstate cyber-conflict and eventually settled on the latter. Despite this increased profile, exceptional measures in order to counter cyber-threats remained scarce. This prompts the authors to express criticism of Securitization Theory's focus on extraordinary measures and subsequently to postulate further development of a threat politics approach.

Dunn Cavelty provides another analysis of the US cyber-threat debate[112]. For this, she utilises the fundamentals of the Copenhagen School's Securitization Theory and expands them by adding insights from framing theory. Her study concentrates on setting out and explaining the disparity between the increasing rhetorical significance of cyber-threats on the security agenda and the absence of incidents that would warrant this elevated status. As the actual countermeasures in place build upon risk analysis and risk management, Dunn Cavelty reasons that the lack of exceptional policy measures in response to cyber-threats ought to be viewed as an example of failed securitisation. She argues that this is due to the responsibility for safeguarding critical infrastructure having been largely delegated to private actors. Against this backdrop, she develops a larger argument about a novel logic of security according to

[111] Bendrath, Eriksson, and Giacomello, 'From "Cyberterrorism" to "Cyberwar", Back and Forth : How the United States Securitized Cyberspace', 57–82.

[112] Dunn Cavelty, 'Cyber-Terror-Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate', 19–36.

which two previously separate conceptions of security conflate as technical security and safety and national security become one.

Nissenbaum also endorses the idea of conceptualising the security of cyber-space along the two notions of technical and national security[113]. Utilising the construct of the Copenhagen School's Securitization Theory, she develops a comparative evaluation of these two notions and sketches out the different political implications each of these notions bring about. On this basis, Nissenbaum stresses the normative essential to the decisions over how threats to cyber-space should be dealt with. In closing, she advocates for the notion of technical computer security over national security as this allows cyber-space to unfold its core purpose as a realm of public exchange.

Yet, in a subsequent contribution Hansen and Nissenbaum indicate that political debates increasingly move towards the national security notion and the particular solutions accompanying such an understanding of security[114]. They set out that security in cyber-space is distinguished by a complex configuration of public-private responsibility and governmental authority. Placing cyber-security within the framework of the Copenhagen School's Securitization Theory, they highlight that cyber-security stand out from other sectors in the way in which it connects the referent objects of the network and the individual to national security. Furthermore, they delineate three specific security modalities related to cyber-security: hypersecuritisation (exaggeration incorporating extreme dependence on the future and the magnitude of the threats claimed), everyday security practices (linking elements of doomsday scenario with familiar experiences of threat as well as securing the individual's accordance in safeguarding network security) and technification (experts with technical knowledge have a privileged role and the authority to speak about the unknown). In closing, Hansen and Nissenbaum use the case-study of attacks on Estonian private and public digital structures in 2007 and illustrate how Securitization Theory can bring conceptual clarity to a subject area that often finds itself either reduced to simplifications or entangled in feeling overpowered with the incapability to engage critically with the issues.

[113] Nissenbaum, 'Where Computer Security Meets National Security', 61–73.
[114] Hansen and Nissenbaum, 'Digital Disaster, Cyber Security, and the Copenhagen School', 1155–1175.

Lawson critically examines cyber-doom scenarios as a key tactic for calling attention to prospective cyber-threats[115]. He adduces insights from research in the history of technology, military history as well as disaster sociology in order to examine essential assumptions and assertions upon which these scenarios rely. For this analysis he utilises the framing concept which Dunn Cavelty developed as an extension of the Copenhagen School's Securitization Theory. Lawson finds that cyber-doom scenarios are a manifestation of longstanding anxieties within Western societies, that narratives of infrastructural and consequential civilisational collapse are unrealistic and motivate the implementation of counterproductive policies. In closing, he provides insight into approaches that potentially help critical security scholars with alternating the framing of cyber-threats so that cyber-security policies are based on more realistic understandings of what is possible.

Lacy and Prince take up Hansen's and Nissenbaum's remarks on hypersecuritisation and technification and suggest that the speed of these modalities as well as the resulting need for interdisciplinary competence require a re-examination of the dynamics that shape relevant ideas and policy[116]. They identify three positions within the debate on cyber-security: the cyber catastrophist, the digital realist and the techno-optimist. Lacy and Prince demonstrate that the controversy amongst these positions has aided in clarifying the issues at stake. Yet, they don't give preference but suggest remaining open to the options revealed in each position. Thereby, it ought to become possible to perceive how actors that shape cyber-space conduct themselves in the debate and live up to their responsibility for assessing the security of cyber-space adequately. Lastly, they advocate for discarding the traditional geopolitical view of digital dangers emerging from the non-West. As the sources of threats become de-territorialised, Lacy and Prince make the case for globalising the perspective on threats to cyber-space.

Vuori takes up Lacy's and Prince's discussion on responsibility as well as de-territorialising and stresses the importance of focussing on the implications they have on political orders[117]. He highlights that the interrelation of technologized securitisation with core values of political

[115] Lawson, 'Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats', 86–103.
[116] Lacy and Prince, 'Securitization and the Global Politics of Cybersecurity', 100–115.
[117] Vuori, 'The Politics of Securitized Technology', 116–17.

orders and their vision of the political must be examined further. This has the potential to help unpack the oftentimes diffuse interweaving of practices in cyber-securitisation.

2.3.3. Gap in the literature

This literature review showcases that securitisation of cyber-space is a merely moderately researched field in academia. Within this empirical issue, case studies focusing on different countries, such as Sweden, Estonia and the US, have been undertaken. Yet, the case of Germany's cyber-security has not been a subject of Securitization Theory research. To this adds that also the topic of the 5G rollout in Germany has not experienced a security-oriented theoretical debate. Hence, there is a gap in the literature which this thesis attempts to fill.

3. Methodology

This chapter outlines the research design and how the tested theory within this design is operationalised for the subsequent analysis.

3.1. Research design

3.1.1. Case study

The research design of this thesis is a holistic single case study. This means that it comprises a single unit of analysis which is intensely studied within the given context[118]. The focus is on a single instance of a social phenomenon and the research aims at providing an in-depth elucidation of it. Within this design, the case is an object of interest in its own right[119]. With these characteristics, the case study research design emerges as the primary research strategy in securitisation literature[120] and also constitutes a profitable approach for an analysis of the research question at hand. Accordingly, this thesis treats the rollout of the 5G network in Germany as the single unit of analysis and studies it in the context of the speech acts surrounding it.

3.1.2. Sampling

This thesis employs purposive sampling. Consequently, the selection is made based on the framework so that the most productive samples are at hand to answer the research

[118] Yin, *Case Study Research : Design and Methods*, 46.

[119] Bryman, *Social Research Methods*, 69.

[120] Balzacq, 'Enquiries into Methods: A New Framework for Securitization Analysis', 32.

question[121]. This type of sampling is applied because random sampling would not be expedient. There is a plethora of speech acts surrounding the case at hand, yet many of them fall out of the scope of this research. In this situation, purposive sampling asserts itself. In order to set up a solid sample, a number of characteristics needs to be accounted for. The sample ought to be sizeable enough so that a larger size would be unlikely to yield a different result and simultaneously be ample enough so that a broad enough viewpoint is facilitated. Hence, this thesis employs sampling based on the characteristics determined by the topic of the 5G rollout being analysed as a matter of cyber-security: the securitising actor (as listed in 2.2.4.), content of the speech act (contextualising the 5G rollout in Germany as a threat to one of the referent objects expanded upon in 2.2.2. and 2.2.3.), timeframe of the speech act (between 2018 and 2020 as this was the crucial timeframe for the rollout of the 5G network in Germany) and availability of the speech act in written text form (for reasons of feasibility).

3.1.3. Discourse analysis

For the case study at hand, this thesis adopts a discourse analysis.

While the analysis of discourse, due to its being present in many disciplines, carries various meanings, a general account could be understood as the analysis of linguistic action, be it written, oral, or visual communication, verbal or nonverbal, performed by social actors in a particular setting determined by social rules, norms, and convention[122]. In this sense, discourses are not solely a medium of communication but vehicles of meaning; they can bring ideas, objects and practices into the world. Yet, this meaning is rarely self-evident but has to be charted by analysis. Against this background, it is the aim of discourse analysis to establish the meaning of these linguistic actions. As outlined above, Securitization Theory aims to capture how a topic becomes a security issue. Given this premise, the adopted technique needs to be tailored to the undertaking of uncovering the practices and structures which engendered the threat image whose effects the analysis wants to explicate. The Copenhagen School of Securitization Theory explicitly takes recourse to a discursive approach to account for processes of securitisation and focuses on spoken and written utterances. Applying this social linguistic approach within discourse analysis brings about the objective to examine the constructive aspects of texts, to understand not only the discursive dynamics of individual

[121] Coyne, 'Sampling in Qualitative Research. Purposeful and Theoretical Sampling', 624.

[122] Wodak, 'Dilemmas of Discourse (Analysis)', 597.

decisions but also the discursive foundations of the social reality in which those decisions are located. Thereby, the social linguistic approach helps to scrutinise the creation of specific phenomena such as identities, decisions, or norms[123].

While these characteristics help in distinguishing the Copenhagen School's approach to analysing securitisation from other approaches, they furthermore and more importantly determine the scope of a discourse analysis to be carried out. The scope of a discourse analysis under the premises of the Copenhagen School is whether securitisation has occurred or not and how it has taken shape[124]. The approach does not focus on revealing why certain securitising moves succeeded and its scope does not encompass the implications of a matter being securitised, which measures are drawn up in response to a successful securitisation or which procedures are consequently employed in the pursuit of security[125].

3.1.4. Limits of research design

Any given research design has a different setup, yet quality should be safeguarded. The research design at hand encompasses a single case study. This causes the study's result to not be representative of all speech acts in all contexts. Speech acts of a different set of actors in other countries than Germany are not represented by the utilised design. This issue of external validity is a catch, which a single case study design entails. External validity refers to the question of whether the results of a study can be generalised beyond the specific research context[126]. This thesis appreciates this pitfall and undertakes to accommodate this aspect by considering speech acts of multiple relevant actors from a wide range of sectors.

Furthermore, the employed research design uses discourse analysis as a sole research method. This can prompt the question whether a potentially established causal relationship yields a conclusion that holds water. In this context, the issue of internal validity is concerned[127]. Triangulation of methods is an often-used possibility to increase internal validity. This approach entails using more than one method in the study of a social phenomenon. It allows to verify findings and enhance validity[128]. Yet, in the case at hand, such an approach would not be expedient. The Copenhagen School's Securitization Theory is based

[123] Balzacq, 'Enquiries into Methods: A New Framework for Securitization Analysis', 39–40.

[124] Balzacq, Léonard, and Ruzicka, '"Securitization" Revisited: Theory and Cases', 519.

[125] Zajko, 'Canada's Cyber Security and the Changing Threat Landscape', 147.

[126] Bryman, *Social Research Methods*, 47.

[127] Yin, *Case Study Research : Design and Methods*, 40.

[128] Bryman, *Social Research Methods*, 392.

on speech acts. Discourse analysis is the most apt approach to researching this constellation. Other approaches would not cater to the scope of the research question to the same extent and yield applicable results. Furthermore, in order to minimise interpretation bias, this thesis establishes an ample context and elaboration of underlying power relations in which the speech acts occur.

3.2. Operationalisation

In order to assess whether speech acts brought about a securitisation of the rollout of the 5G network in Germany, securitisation must be made measurable. Hence, an operationalisation is needed.

As stated and explained above, securitisation can be understood as *"the discursive process through which an intersubjective understanding is constructed within a political community to treat something as an existential threat to a valued referent object, and to enable a call for urgent and exceptional measures to deal with the threat"*[129].

Drawing from the above explanations relating to this definition, this section deduces a number of conditions which have to be met in order for an issue to be deemed securitised.

First, a speech act has to be uttered by a securitising actor. Second, the speech act has to allude to a threat to a valued referent object. Third, the threat is portrayed as so existential that it requires urgent and exceptional measures to alleviate it. Fourth, the call for measures has gained public assent to a degree that a platform is made from which it is possible to justify aspired measures or even that measures are implemented.

Due to the application of purposive sampling, only speech acts uttered by key securitising actors in the field of Germany's 5G rollout will be selected. Hence, the first indicator will be fulfilled in any case and thus can be removed from the list of conditions.

For the second indicator the analysis will draw on the above remarks on threats and referent objects within the cyber-context.

With regard to the last indicator, this thesis acknowledges that measuring the degree of audience assent can be difficult. Therefore, if indications are sparse, this research takes recourse to a preponderance of views in the larger social or national context[130].

[129] Buzan and Wæver, *Regions and Powers : The Structure of International Security*, 491.

[130] Nissenbaum, 'Where Computer Security Meets National Security', 67.

Consequently, the following three conditions are determinative for measuring whether an issue was securitised:

1) The speech act has to allude to a threat to a valued referent object.
2) The threat is portrayed as so existential that it requires urgent and exceptional measures to alleviate it.
3) The call for measures has gained assent from an audience to a degree that a platform is made from which it is possible to justify aspired measures or even that measures are implemented.

4. The case of the 5G rollout in Germany

This chapter present the case study of the rollout of the 5G network in Germany. It supplies ample context and goes into details relevant for the assessment of the rollout. An introduction is followed by the provision of the topic's international context, a section on security concerns and lastly a comprehensive account of the 5G network rollout in Germany.

4.1. Introduction – substance, form and shape of the rollout of the 5G network

5G commonly stands for the fifth generation of mobile communication networks. It is an end-to-end ecosystem that meets the demands of an increasingly connected and mobile society as well as industry. Surpassing the capabilities of the four preceding generations, 5G is expected to handle higher traffic density and higher data rates, provide ultra-low latency and greater liability as well as enable connectivity for more devices per area and ensure a lower energy usage[131]. With this, the 5G network is the first generation of mobile networks that enables the most pioneering technologies, such as massive Internet of Things networks, artificial intelligence, virtual reality as well as augmented reality[132]. By design the network addresses a vast range of needs of a multitude of sectors. For individual consumers and society at large 5G offers unlimited mobile broadband experience and provides massive connectivity[133]. 5G can be a pivotal enabler for services in sectors such as education, healthcare, smart cities and entertainment. Furthermore, 5G has an enormous potential for industries. It is capable of providing critical machine communications with instant action and

[131] Osseiran et al., ‘Introduction’, 10.
[132] IEEE, ‘IEEE 5G and Beyond Technology Roadmap White Paper’, 9.
[133] 5G PPP Architecture Working Group, ‘View on 5G Architecture - Consolidated Version’, 25.

ultra-high reliability[134]. Thereby it facilitates pivotal features for sectors in the industry, such as industrial automation in manufacturing, intelligent control in smart grids as well as intelligent navigation and transportation in the automotive sector. To this extend, 5G differs significantly from the previous generations of mobile communication networks. While they were designed purely as a mobile communication technology, 5G does not simply transmit communication anymore. Rather, it has the potential to be, next to the power grid, the central and empowering infrastructure for large parts of the economy[135]. Bringing profound changes to societies and economies across the globe, 5G networks appear as critical infrastructure. They are the essential new technology which will facilitate innovation as well as contribute to the digital transformation. Furthermore, they play a substantial role for competing in the global market. 5G has the potential to spark a generational leap for industries and services and can be a springboard for established as well as emerging major players[136].

Contemplating the technical level, a few observations are made in the following. In principle, all mobile communications frequencies are suitable for the provision of 5G services. There is no “5G-frequency”, but it solely depends on the utilised technological equipment[137]. Yet, 5G networks will not be rolled out on randomly available frequencies. Rather, the rollout is harmonised and comes in the form of a three-pronged approach. 5G will be transmitted on a mix of three different bands, so-called pioneer bands, in order to serve different use cases. A low band, ranging from 600 to 700 MHz, is assigned to provide wide-ranging, universal coverage and expand reliable connectivity for e.g., smart grids. A mid band, ranging from 2 GHz to 6 GHz (mainly 3.4 - 3.8 GHz) is allocated to provide amplified urban mobile data speeds and thereby facilitate e.g., smart cities. Lastly, a high band, ranging mainly between 24 - 30 GHz, is assigned to service close-range coverage and expand hotspot data speeds for e.g., smart factories, train stations or stadiums[138]. While frequencies are the means for broadcasting mobile coverage, it is up to the telecommunications equipment to provide the enhanced performance, which marks 5G’s signature characteristics. A mix of different key technologies enables this. Among them are “network slicing”, which allows to serve multiple

[134] 5G PPP Architecture Working Group, 25.
[135] Kleinhans, ‘5G vs. National Security, A European Perspective’, 3.
[136] Duchâtel and Godement, ‘Europe and 5G: The Huawei Case’, 4.
[137] Wissenschaftliche Dienste des Deutschen Bundestages, ‘Sachstand: Aufbau Der 4G-/LTE- Und 5G-Mobilfunknetze in Ausgewählten Ländern’, 15.
[138] Horwitz, ‘The Definitive Guide to 5G Low, Mid, and High Band Speeds’; Stantchev, ‘Spectrum for 5G: EU-Level Developments’.

use cases simultaneously, “network virtualisation” for greater flexibility and remote network management, “heterogeneous networks”, which allows to integrate and exploit current and past technologies, as well as “Multiple Input Multiple Output (MIMO)” improving spatial efficiency, and “Beamforming” controlling and reducing interference[139].

4.2. International context

A widespread recognition of the fifth generation of mobile communication networks as a gamer-changer has brought about competition for global digital leadership. Accordingly, 5G networks are being rolled out across the globe with the European Union (EU), United States of America (US), China, Japan and South Korea being considered leading regions in terms of 5G readiness[140]. The EU initially tackled 5G when the European Commission introduced the 5G Action Plan in September 2016. As a strategic initiative to make 5G a reality for all citizens and businesses across the EU, the plan set out a roadmap for public and private investments in 5G infrastructure in the EU and aimed at boosting EU efforts for the deployment of 5G infrastructures and services across the EU’s Digital Single Market by 2020[141]. Subsequently, this plan has ensured a timely commercial launch of 5G by having earmarked at least one major city in every EU Member State by the end of 2020 and has prepared the ground for having smooth 5G network coverage in all urban areas as well as major terrestrial transport paths by 2025[142]. Furthermore, the European Commission presented its vision for a digitalised economy and society in the 2030 Digital Compass Communication “The European way for the Digital Decade”. In this proposal, 5G is a key element for reaching secure and performant sustainable digital infrastructures, one of the vision’s four cardinal points[143]. The US introduced its “National Strategy To Secure 5G” in March 2020. The strategy sets out a private sector-led domestic rollout of 5G and details how the United States aims at leading global development, deployment and management of reliable and secure infrastructure[144]. Subsequently, the Federal Communications Commission auctioned off large parts of the spectrum for 5G between early 2019 and 2020, and the four main providers have launched 5G commercial services. Similarly, 5G deployment is strongly backed by the government in

[139] European 5G Observatory, ‘What Is 5G?’
[140] European 5G Observatory, ‘5G Observatory Quarterly Report 11 - Up to March 2021’, 114.
[141] European Commission, ‘5G Action Plan | Shaping Europe’s Digital Future’.
[142] European 5G Observatory, ‘5G Observatory Quarterly Report 11 - Up to March 2021’, 7.
[143] European 5G Observatory, 14–15.
[144] The White House, ‘National Strategy to Secure 5G’.

China. Establishing a 5G network ranks among the strategic priorities for the entire country. In a 2017 report the Chinese government set the objective of becoming one of the global leaders of 5G. To this effect, the Ministry of Industry and Information Technology issued 5G license to four major providers mid 2019, which subsequently launched their 5G services at the end of 2019[145]. In South Korea, the government and the public-private partnership defined the 5G mobile strategy as early as 2014. In a joint effort to save money and time, South Korean carriers agreed mid 2018 to establish a single 5G network. 5G services were then jointly launched by three mobile network operators in April 2019. Japan, too, presented its roadmap for 5G in 2014. Following extensive tests, Japanese operators launched their commercial 5G services between March and September 2020[146].

4.3. Security concerns and reactions

Alongside the potential of the fifth generation of mobile communication networks, control and security of the network's technology as well as of the data managed by the networks are key elements. While threats concerning network integrity and communication security are nothing novel, the issue has obtained particular significance with the advent of 5G networks[147]. As societies and industries shape up to be increasingly dependent on the new services, network infiltrations and attacks have profound implications: not only personal communication can be disrupted but also parts of the industry as well as critical services for society. Thus, network security will be all the more significant[148]. Consequently, the issue of network security surrounding the 5G rollout has become highly polarised and network equipment vendors are under particular scrutiny.

In this connection, the main focus has been on Chinese mobile network equipment vendor Huawei Technologies. Some of the technological equipment indispensable for 5G networks are offered worldwide almost exclusively by three companies: Nokia, Ericsson and Huawei Technologies[149]. Huawei claims the leadership for producing at scale and cost all the elements of a 5G network, while the other two competitors trail behind in their offer[150]. However, there

[145] European 5G Observatory, '5G Observatory Quarterly Report 11 - Up to March 2021', 115–17.
[146] European 5G Observatory, 117.
[147] Messas et al., '5G in Europe: Time to Change Gear!', 5.
[148] Kleinhans, '5G vs. National Security, A European Perspective', 3.
[149] Voelsen, '5G, Huawei Und Die Sicherheit Unserer Kommunikationsnetze', 1.
[150] Kaska, Beckvard, and Minárik, 'Huawei, 5G and China as a Security Threat', 7.

is fear that Huawei's technological equipment might pose a security risk. On the one hand, there is controversy about the company's obligations towards Chinese law. Under Chinese National Intelligence Law, the Chinese government can require Chinese citizens, organisations and their equipment to cooperate with the Chinese national intelligence[151]. Consequently, Huawei can be required by law to gather data on behalf of its government whenever it is requested to do so[152]. While all vendors of network technology integrate backdoors into their products so that remote maintenance is possible, the concern in the case of Huawei is whether it will be used for espionage or sabotage[153]. On the other hand, there is the company's own struggle with establishing trustworthiness for itself. There is a number of cases of intellectual property theft and at a minimum collusion for espionage throughout the company's past. Furthermore, there are cases where Huawei seems to have serious software engineering and cyber security troubles. Lastly, its opaque corporate governance structure makes it virtually impossible to conceive ownership structures, management hierarchies or ties to the CCP[154].

This constellation has raised concerns of trustworthiness. The ensuing debate on threat potential stemming from the equipment has been heavily driven by a US perspective and agenda. By virtue of a national security order the US effectively banned Huawei from their national communication networks in May 2019. In an effort to make their weight felt, the US followed up by calling on European states to consider potential security risks. In a December 2019 op-ed the US Secretary of State urged the European states to abstain from employing Huawei's 5G technology[155].

The EU Commission took a similar line. After having published a report on EU coordinated risk assessment of 5G networks security in October 2019[156], the Commission followed up with presenting a toolbox with risk mitigating measures related to the rollout of 5G in January 2020. While abstaining from singling out Huawei, the toolbox identified state-backed actors as the most serious as well as the most likely threat actors to target 5G networks[157]. Yet, with the EU's approach to security in cyberspace continuing to be fragmented[158], there is no EU regulation nor directive facilitating a uniform approach to the issue. Accordingly, EU Member

[151] Lee-Makiyama, 'Strategic Autonomy in the Digital Age', 12.
[152] Legarda, 'China Global Security Tracker'.
[153] Voelsen, '5G, Huawei Und Die Sicherheit Unserer Kommunikationsnetze', 3.
[154] Kleinhans, 'Whom to Trust in a 5G World? Policy Recommendations for Europe's 5G Challenge', 15.
[155] Pompeo, 'Europe Must Put Security First with 5G'.
[156] European Commission, 'Report on EU Coordinated Risk Assessment of 5G'.
[157] NIS Cooperation Group, 'Cybersecurity of 5G Networks - EU Toolbox of Risk Mitigating Measures', 45.
[158] Carrapico and Barrinha, 'The EU as a Coherent (Cyber)Security Actor?', 1264.

States have been applying different approaches. While there are still a few Member States' governments that have been hesitant to pass laws which would keep Huawei at bay, a majority of governments has either banned Huawei or installed sweeping powers to block the acquisition of Huawei equipment[159].

This overview has demonstrated that despite the new technology's considerable potential there are impactful influences surrounding the rollout preventing a smooth rollout and bringing about various reactions.

4.4. 5G network rollout in Germany

This section explores the status quo of the 5G rollout in Germany and how it came about. It takes account of the political and strategic efforts, the allocation of spectrum and availability of 5G services as well as the technological context and the concomitant security issues.

4.4.1. National political context of the 5G rollout

The German Federal Government launched a first comprehensive 5G policy in autumn 2016. The "5G Initiative for Germany" represented an early-stage framework for action. It outlined the government's goal to position Germany as a lead market for 5G applications and to support the rapid and successful deployment of 5G networks as well as the development of 5G applications[160]. Having subsequently engaged in a dialogue with the industry and research, the Government introduced the "5G Strategy for Germany" in July 2017. The scheme foresaw the conditions for the rollout were to be created by 2020 at the latest and outlined the Government's aspiration to have 5G connectivity by 2025. Furthermore, the document gave a detailed account of the 5G technologies available by 2020 as well as the frequency spectrum to be used and exemplified strategic developments of the digital transformation facilitated by 5G. In closing the strategy outlined the aspiration of making Germany a lead market for 5G applications and showcased five fields of action to support this objective. In September 2019, the Government updated the national mobile strategy. The newly introduced "Mobilfunkstrategie" comprised a five-point plan to accelerate the planning, approval and rollout of 4G and 5G networks and presented ways and means to minimise white spots in 4G

[159] Noyan, 'EU Countries Keep Different Approaches to Huawei on 5G Rollout'.

[160] Bundesministerium für Verkehr und digitale Infrastruktur, '5G - Initiative Für Deutschland', 3.

and consequently in 5G networks. 1.1 billion EUR were earmarked for achieving this goal. With the COVID-19 pandemic, the 5G rollout experienced a delay. Subsequently, the German Government included its 5G endeavours in the plan to counter the economic crisis caused by the pandemic. Accordingly, the 2020 stimulus package allocated a total of 7 billion EUR to 5G.

4.4.2. Allocation and availability of the 5G network

In an effort to lay the groundwork for implementing the government's policy on the 5G rollout in Germany, the Federal Network Agency (Bundesnetzagentur) undertook the necessary allocation of frequencies. The Agency is Germany's regulatory office for electricity, gas, telecommunications, post and railway markets. In telecommunications it has the authority over, amongst others, the administration and management of the frequency spectrum. Accordingly, it falls into the Agency's realm of responsibility to ensure that frequencies are made available in line with demand for the introduction of the fifth generation of mobile communications and the expansion of digital infrastructures. To that effect, the Agency was and is concerned with making the 5G networks' three pioneer bands available.

In June 2015 the Agency concluded the auction of frequencies in the low band, including the 700 MHz band. Three German mobile operators, Telefónica Deutschland GmbH & Co. OHG, Telekom Deutschland GmbH and Vodafone GmbH participated successfully and were allocated frequency blocks[161]. However, the 700 MHz band was not immediately ready for use but was freed up and made available for mobile broadband use only in successive steps[162]. It became fully available from mid 2019 onwards[163]. Since then, mobile operators have noticeably increased the pace of 5G expansion in this spectrum.

In July 2016 the Agency initiated a first substantial endeavour for making the mid-band available. Publishing its "Frequency Compass", the Agency identified areas requiring regulatory action on spectrum for 5G and provided an orientation on the heterogeneous interests in the mobile network sector[164]. In December of the same year the Agency followed up on this by publishing "Points of Orientation" for spectrum provision. The document provided an overview of the individual frequency bands along with initial thoughts on

[161] Bundesnetzagentur, 'Mobiles Breitband-Projekt 2016'.

[162] This was due to the concession of a lengthy switchover-period from the first generation of Digital Video Broadcasting - Terrestrial (DVB-T), which occupied the 700 MHz band, to the second generation (DVB-T2). This phasing out only had to be concluded by June 2019.

[163] Bundesnetzagentur, 'Informationen Zu Dem Zeitplan Der Räumung Des 700-MHz-Bandes'.

[164] Bundesnetzagentur, 'Frequenz-Kompass', 1.

prospective frequency assignment and invited mobile operators, new entrants, regional providers, service providers as well as virtual network operators to present their interest and views on potential usage[165]. On the basis of the submitted statements the Agency initiated an assessment of demands for nationwide allocations in the 2 GHz and 3.6 GHz band[166]. After it produced a preliminary draft for a competitive tendering procedure in January 2018, the Agency determined that more frequencies were in demand than were available. Therefore, in May 2018, it decided to auction off frequencies from the 2 GHz band as well as frequencies from the 3.6 GHz band. The auction took place between March and June 2019 and yielded a distribution of the available frequency blocks among the four mobile operators Drillisch Netz AG, Telefónica Germany GmbH & Co. OHG, Telekom Deutschland GmbH and Vodafone GmbH[167]. While the 2GHz band is assigned to be available for servicing 3G networks until the end of 2021, it is up to the mobile operator when they will phase out support for 3G coverage and use the then available band for 5G coverage. The 3.6 GHz band was ready for use after the auction was concluded[168].

Furthermore, frequencies in the 3,7-3,8 GHz band were made available with preference for the operation of 5G services in regional and local wireless networks. Having published administrative rules governing the allocation of frequencies in the 3,7-3,8 GHz band in November 2019, interested parties have since been able to submit applications. Eligible applications are evaluated on their spectrum usage concept as well as their specialist knowledge, financial capacity and reliability[169].

After having published preliminary considerations for future usage of the high band in September 2018, the agency composed a draft for future frameworks for 5G applications in the 24,25 - 27,5 GHz band (26 GHz band) in December 2019. A year later, the agency set up administrative rules according to which spectrum in the 26 GHz band for 5G services will be assigned upon application. Within this procedure, allocations will be made on a technology-neutral and service-neutral basis with the goal of enabling the implementation of retail telecommunications services and applications such as infrastructure links and the Internet of

[165] Bundesnetzagentur, 'Orientierungspunkte Zur Bereitstellung von Frequenzen Für Den Ausbau Digitaler Infrastrukturen', 1.

[166] Bundesnetzagentur, 'Eckpunkte Für Den Ausbau Digitaler Infrastrukturen Und Bedarfsermittlung Für Bundesweite Zuteilungen in Den Bereichen 2 GHz Und 3,6 GHz', 1.

[167] Bundesnetzagentur, 'Frequenzauktion 2019'.

[168] Metztger and Laser, '5G in Deutschland: Stand des Netzausbaus im Überblick'.

[169] Bundesnetzagentur, 'Administrative Rules for Spectrum Assignments for Local Spectrum Usages in the 3700-3800 MHz Band', 4.

Things. Preference will be given to the operation of 5G services in regional and local wireless networks. Furthermore, spectrum is assigned on the basis of applicants' spectrum usage concepts, in which applicants must provide a feasible account of their spectrum requirements based on the planned spectrum usage[170].

Availability of 5G services ensued following the spectrum allocation by the Bundesnetzagentur. Commercial launch of 5G services in Germany began mid 2019. In July that year, Vodafone was first to start its 5G network in Germany. The company has since deployed the 700 MHz band to provide coverage in rural areas. For the 2GHz band Vodafone decided to phase out support for 3G coverage at the end of June 2021 and now uses the band to provide 5G in densely populated cities. The 3.6 GHz band is being rolled out in high traffic areas such as train stations and stadiums. The company provides 5G coverage to more than 20 million customers and is set to reach 30 million by the end of 2021[171]. Telekom followed later the same year and switched on its 5G network in September 2019. The company makes comprehensive use of spectrum in the mid band for providing 5G coverage. It also phased out support for 3G coverage on the 2 GHz band at the end of June 2021 and now employs this band for providing 5G coverage in less densely populated areas. It furthermore uses the 3.6 GHz band for coverage in large cities. With this, Telekom provides 5G service to 66 million customers[172]. As third mobile network operator, Telefónica introduced 5G services in October 2020. It uses the 700 MHz band for coverage in rural areas and the 3.6 GHz band for urban areas. Telefónica is still growing its coverage and aims at covering more than 30% of the population by the end of 2021[173]. Drillisch has not yet rolled out 5G services.

Furthermore, 5G services in regional and local wireless networks have also expanded incrementally. Up to this point, the Bundesnetzagentur granted almost a total of 140 allocations of frequencies within the 3,7-3,8 GHz band and the 24,25 - 27,5 GHz band for regional and local 5G networks. Allocation holders come from a wide range of industries[174].

[170] Bundesnetzagentur, 'Administrative Rules for Spectrum Assignments for Local Broadband Spectrum Usages in the 24.25-27.5 GHz Band', 5, 8.

[171] Vodafone, 'Bye, Bye 3G – Willkommen Highspeed-Internet'; European 5G Observatory, '5G Observatory Quarterly Report 11 - Up to March 2021', 25.

[172] Dahmen, 'Diese 5G Frequenzen Nutzt Die Telekom in Deutschland'.

[173] Streicher, '5G Für 30 Prozent Der Bevölkerung 2021 - 5G-Standalone in Vorbereitung'.

[174] The Agency treats information on frequency allocations as trade secrets and only publishes names of allocation holders upon their consent. Thus, a definite number and account of holders is elusive.

4.4.3. Technological context and concomitant security issue

With the spectrum having been made available, apt technological equipment needs to be employed in order to provide the enhanced performance of 5G. There is a competition among telecommunications equipment vendors to produce at scale and cost the necessary technology for building national 5G networks. While there is a range of suppliers, Huawei, Nokia and Ericsson are market leaders. Their equipment prevails among mobile operators and they also supply a vast range of enterprise customers with their technology. Reflecting the global market distribution, Huawei also spearheads this race in Germany, while other vendors, most notable Nokia and Ericsson, lag behind. However, as outlined above, Huawei's products inhere concerns of trustworthiness. As in many other countries, this also brought about a debate in Germany on whether or not to use technology manufactured by Huawei. Even though there has not been a substantiated security incident in Germany that traces back to Huawei, Huawei's technological equipment was a much-debated topic that created a stir for months. In March 2019 Germany made a first tentative approach to regulating this sector. In a set of draft requirements for telecommunications security, Germany outlined the adoption of a middle way: no telecommunications equipment vendor was to be banned but critical components may only be obtained from vendors that have given adequate assurances of their trustworthiness and that abide by national security regulations. Thereby, Germany refrained from an open ban but kept the door open for an indirect one[175]. While the German government debated the issue and published amendments to the draft in course of the two years that followed, the fundamental non-ban approach remained unchanged. Eventually, in May 2021, Germany became the last of the big EU economies to regulate the 5G sector. Germany introduced the IT-Security Law 2.0. It was the second legislative act in the field and amended the previous IT-Security of Law of 2015 which itself was the very first consolidation of prior efforts to improve critical infrastructure security[176]. With regard to the protection of critical infrastructure, the novel IT-Security Law 2.0 foresees a two-stage assessment mechanism. An initial technical evaluation is followed by a security analysis. For this second step the law requires telecommunication vendors seeking access to Germany's 5G network to declare that its components cannot be used for sabotage or espionage and requires telecoms operators to inform the government of their intend to sign contracts with this vendor.

[175] Skierka, 'Germany Takes the Middle Way on Huawei—for Now'.
[176] Schallbruch and Skierka, *Cybersecurity in Germany*, 22.

Subsequently, the company enters a period of between two and four months during which the deal is checked against national security criteria and the envisaged 5G components are revied to match security policy goals of Germany, the EU and NATO. The assessment of the interior ministry is given priority amongst those of other ministries[177]. To this extend, the law supplies the German government with the capacity to veto the procurement from untrustworthy suppliers. Following the EU Commission's 5G toolbox, the new legislation does not single out Huawei. Yet, companies which are under the control of authoritarian states can be deemed to be untrustworthy[178].

4.4.4. Conclusion

The different fields of political aspirations, providing spectrum-availability for implementing these endeavours and regulating concomitant technological risks are important parts for analysing the context. They build the cornerstones of the 5G rollout in Germany. Yet, amidst them they create a tension. So far, the rollout has been considerable, and the benefits have become noticeable. Yet, an incident due to untrustworthy technology has yet to occur.

5. Analysis

This chapter presents the overall approach to the analysis as well as the analysis of the researched data. It first sets out how the data was collected and how the data was exploited. Subsequently, an analysis of the speech acts is presented and, following the discursive nature of the Copenhagen School's Securitization Theory, the audience acceptance as well as consequential results are illustrated.

5.1. Approach to the analysis

5.1.1. Data collection

As previously stated, the cyber-security sector is composed of a constellation of various referent objects which leads to the cyber-security discourse having a wide array of actors who can engage in uttering speech acts. Corresponding to the referent objects outlined above, data was collected from actors from the business sector, the media as well as the political sector.

[177] Cerulus, 'Germany Falls in Line with EU on Huawei'; Thomas, 'What Germany's New Cyber Security Law Means for Huawei, Europe, and NATO'.
[178] Noyan, 'EU Countries Keep Different Approaches to Huawei on 5G Rollout'.

From the business sector, the three major German mobile operators Vodafone Germany, Deutsche Telekom and Telefónica Germany are chosen. Amongst the range of companies providing 5G services, these operators have the most extensive share: they have the largest number of clients as well as the most extensively developed coverage network. With the largest stakes within the business sector, these operators have considerable interests in the rollout of the 5G network in Germany and were involved in the process of the rollout from early on. Accordingly, all three companies formulated their approach and how they envisage the rollout to take shape. This study consults these strategical documents. Deutsche Telekom published an eight-point plan on the 5G rollout, Vodafone Germany made available a white paper on 5G and Telefónica Germany had the company's chief technology innovation office interviewed by a telecommunication magazine on the company's 5G rollout strategy.

Data from the media sector is collected as it is a central provider of information. Due to 5G's economical, technological as well as foreign and security policy dimension, discussions on the topic tend to take place in closed debates. With its access to such information, the media wields significant influence on the topic. Publications from the outlets Zeit Online, Süddeutsche Zeitung, Frankfurter Allgemeine Zeitung are chosen. Selection is made on the publications' relevance on to the substance of the topic. A compilation of these outlets gives a well-founded overview of the media output.

Eventually, data from actors in the political sector is taken into account because they have a pivotal position in the regulatory dimension of the 5G rollout and thereby have an impactful influence on the eventual configuration of the 5G network. Hence, speech acts from all political parties represented in the German Parliament were collected.

5.1.2. Data exploitation

The collected data is exploited by means of coding. Each source of data is coded individually in order to develop a detailed understanding and ensure close contact with the content, context and perspective. The data is coded against the operationalisation-framework. The insights generated in doing so are then used to evaluate the significance and impact of the coded material as well as to assess potential interrelations. Ultimately, these insights form the basis for interpreting the findings and for measuring whether an issue was securitised.

5.2. Speech act analysis

This section examines the collected speech acts. It first elaborates on speech acts from actors from the business sector, then from the media and lastly from the political sector.

5.2.1. Speech acts from the business sector

Deutsche Telekom's strategic eight-point plan touched upon a range of issue which relate to referent objects that are relevant in the cyber-security context. It elaborated on issues that concern the 5G network as critical infrastructure, that outline its significance in business networks as well as computer networks. However, the eight-point plan did not allude to threats imminent to these referent objects. The issue of security was not incorporated in this strategic outlook. Rather, it approached the addressed referent objects from a service-driven perspective. For a start, the focus was on ensuring availability. Within this category, topic such as the provision of comprehensive nationwide coverage, the expansion of coverage in metropolitan areas as well as the accommodating to the needs of specialised infrastructures prevailed. Furthermore, the category of expanding the company's own operational performance stood out. It encompassed topics such as financial investment, the expansion of cell towers and the improved data transmission rate. Lastly, the eight-point plan focused on facilitating cooperation with the public and private sector as well as other network operators in order to exploit the unique features of 5G and thereby cater to specific needs and use cases. Against this background, no speech act could be discerned to conjure up a threat imminent to a relevant referent object.

Vodafone Germany's white paper on 5G took a very similar line. Here as well, the rollout of the 5G network was set within a context that touches upon the referent objects critical infrastructure, business networks and computer networks. Yet, the white paper did not allude to any threats to these referent objects. Rather, the focus was on the potential of the 5G network and how Vodafone can be of help for unfolding these capabilities. The emphasis ranged from expanding capacities in order to cope with demands that now stem from more than just mobile users to ensuring coverage reliability. Beyond that, there was a detailed focus on use cases within the business sector. Within this category, topics such as new productivity benefits, boosted innovation and streamlining value chains stood out. A threat imminent to a relevant referent object was not addressed.

The strategy for Telefónica Germany presented itself quite similar to the others mentioned above. Again, issues related to in the cyber-security referent objects such as critical infrastructure, business networks and computer networks. Yet, no threat to these referent objects was presented. Once more, the service-perspective protrudes. One fundamental focus was on solidifying coverage so that comprehensive coverage is guaranteed. Another category that stood out was the regard for technological developments as this determines the effectiveness of 5G services. Lastly, the strategy focused strongly on user-needs: it emphasised measures so that consumers have an enhanced user experience and so that specific business needs are catered to within rapid delivery periods.

Summing up the data collected from the business sector, this study holds that no speech acts were uttered that alluded to threats to valued referent objects. Therefore, already the first indicator of the operationalisation-framework was not given.

5.2.2. Speech acts from the media

The findings of the data from the media are presented not fragmenting along the lines of each news outlet but in a collective summary because they produced a homogenous picture.

This section proceeds as follows: each respective referent object is touched upon individually and it is demonstrated which issues were depicted to threaten them as well as how this threat is portrayed as existential. After each referent object is assessed individually, a joint conclusion gives an account of the call for measures. This approach is chosen because referent objects were discussed differently, yet the called upon measures shared commonalities across the board.

To begin with, it can be noted that, while the data contains a wealth of pertinent speech acts, none of them touch upon the referent object of business networks. Rather, the referent object of critical infrastructure and especially the referent object of national security as well as computer networks are prevailing subjects of the speech acts.

Critical infrastructure was portrayed to be threatened by eventuality of a “kill switch”, a possibility to turn off network equipment remotely and thereby cause disruption or even destruction of infrastructure as the very foundation of society. This threat was highlighted as existential against the backdrop of potentially dramatic consequences: the breakdown of modern life as well as society turning blind and disoriented.

The referent object of national security was not dealt with in regard to its first component of state power in cyber-space but it was dealt with in regard to its second component of state control over information flows within and out of the country. The issue of espionage, the stealing of national intelligence, was portrayed to threaten this dimension of the referent object. With several allusions, this threat was depicted as existential: the total surrender of sovereignty was invoked as well as the impacting and undermining of the German state as this situation would leave the door wide open for foreign governments to gain insight into any aspired intelligence.

Lastly, with regard to computer networks, speech acts addressed both components of the referent object. The first component of ensuring availability of systems, information and networks to users was portrayed to be threatened essentially by malware. As per its design, network equipment technology required regular and frequent maintenance. As mobile networks have become extremely complex, the mobile operators no longer carry out maintenance themselves but let the original vendor assume this responsibility. Under these circumstances, vendors, who cooperate with foreign intelligence services, have ample leeway to install backdoors which can serve as technical gateway for malware. This threat was depicted as existential due to a number of reasons. First, malware facilitates entry points through which hackers can spread out and exploit a wealth of data and commit manipulation as well as sabotage. Furthermore, this causes high unpredictability of risk and ultimately has the potential of detrimental consequences because 5G brings about a comprehensive interconnection of services, which then can all be affected. Lastly, another reason for the existential nature of the threat is that network availability could become controlled by foreign players. Turning to the referent object's second component of network integrity, speech acts alluded to the threat of surveillance of information and communication that is ultimately confidential. This threat was portrayed as existential because even the most thorough verification cannot guarantee reliability. Again, a high unpredictability of risk and the potential for detrimental consequences stood out.

In consequence of threats being depicted as existential, the speech acts contained a range of postulated exceptional measures. The most widespread called upon measure was the integrated approach of banking on diversification of equipment vendors, expanding deployment of European vendors and limiting access to essential network-domains for equipment vendors fraught with risk. Furthermore, an outright ban of high-risk vendors from the 5G network was repeatedly postulated. Taking it a step further, a sporadically called upon measure was to strip the 5G network of existing equipment by high-risk vendors as well as to impose high fines in cases of installed backdoors.

Summing up the data collected from the media sector, this research finds that speech acts alluded to threats to the referent objects critical infrastructure, national security and computer networks. Moreover, these threats were portrayed as so existential that they required urgent and exceptional measures to alleviate them.

5.2.3. Speech acts from the political sector

The findings in this section are presented in the same manner as in the preceding chapter. Each referent object is touched upon individually and it is outlined which issues were depicted to threaten them as well as how this threat is portrayed as existential. Following this, a joint conclusion gives an account of the call for measures.

To begin with, the analysis finds that speech acts addressed the referent object of business networks. It was portrayed to be threatened by the possibility that the 5G network can have undetected interfaces that allow intercepting corporate information. The existential nature of this threat results from the importance of 5G for the future competitiveness of Germany as a business location.

Furthermore, speech acts referred to critical infrastructure in its form as the very foundation of society. Depictions of threats to this referent object included the potential installing of a "kill switch" and especially less noticeable scenarios of tampering such as slowing down, redirecting, or altering information flows. Thereby, fundamental services can be brought to a standstill. This threat was portrayed as existential. 5G has the potential to become the digital neural system of society and bring about an unparalleled interconnectedness. Consequentially, if the threat materialised, the consequences could be cascading and detrimental.

The referent object of national security was dealt with in regard to its second component of state control over information flows within and out of the country. Potential infiltration and resulting espionage were depicted as threats. They were seen as existential nature due to the state's loss of sovereignty over these information flows and the potential resulting exposition to constraint.

Lastly, computer networks were again prevailing subjects of the speech acts. The referent object's first component of ensuring availability of systems, information and networks to users was depicted to be threatened by malware, which can be planted through backdoors and facilitate sabotage. With regards to referent object's second component of network integrity, speech acts highlighted the threat of surveillance of information and communication that is ultimately confidential. The threats were portrayed as existential because their materialising could bring about a far-reaching risk.

Turning to the called upon measures, the analysis found a range of suggestions. Also among actors in the political sector, an integrated approach was favoured. This consisted primarily of avoiding a monoculture of equipment vendors but banking on diversification with, first, preference to European vendors and, second, the exclusion of non-trustworthy vendors. Additionally, diversification of utilised software was postulated so that open-source software would service central components of networks. Lastly, a comprehensive regulatory mechanism was called for. This demand comprised the development of an up-to-date and dynamic criteria- and security-catalogue which includes not only technical, but also legal and other security-relevant aspects in order to assess network equipment vendors. This political assessment was demanded to be made by politically legitimized decision-makers.

Summing up the analysis of data from the political sector, this research finds that speech acts alluded to threats to all four referent objects. Moreover, these threats were portrayed as so existential that they required urgent and exceptional measures to alleviate them.

5.3. Audience acceptance

Having carved out the portrayal of threats to valued referent objects as well as the concomitant exceptional measures to alleviate them, this last section of the analysis examines whether these calls for measures gained assent from an audience. The identity of the securitisation audience is dependent on the context of the particular securitisation process in question[179]. With the case at hand, political actors as well as actors from the business sector

[179] Côté, 'Agents without Agency: Assessing the Role of the Audience in Securitization Theory', 546.

stand out as audience. The existence of assent is assessed on the basis of preponderance of views amongst this audience.

For political actors the focus falls on the members of the German Parliament (Bundestag) and the German Federal Council (Bundesrat). With their voting behaviour during the legislative procedure for the novel IT-Security Law 2.0, they can be seen to have given their assent to the call for measures. After the government's draft law was discussed in the Parliament in three reading sessions, the Parliament's committee on internal affairs amended the draft to include stricter measures. Most notably the amendment added a political component for the assessment of network equipment vendors: next to the technical assessment to be made by the Federal Office for Information Security, the amendment assigned final authority to the Federal Ministry of Interior to prohibit the use of a critical component on a case-by-case basis if there is "probable impairment of public safety and order"[180]. The majority of members of Parliament voted in favour of this amended draft law. Subsequently, members of the German Federal Council had the opportunity to raise objections. Even though the Council's committee on internal affairs recommended calling on a conciliation committee to amend the draft, the members of the Council decided against it. With the absence of an objection, the Council approved the draft law. With these decision, members of the Parliament and the Council substantially decided on the IT-Security Law 2.0; the remaining required steps for the law to enter into force were almost exclusively of a formal nature. This new law strengthened means to safeguard fundamental infrastructure and to prevent the risk of loss of state control over information flows within and out of the country. The outlined voting behaviour indicates that political actors accepted the portrayed threat to the referent object "critical infrastructure" and "national security".

Actors from the business sector can be seen to have accepted the call for measures to alleviate the threat by their change in direction when it comes to network equipment vendors. Between 2019 and 2021 all three major German mobile operators have decided to build their core network without equipment from Huawei Technologies. In contrast to the access network, which only consists of transmitting and receiving antennas, the core network processes all applications and all data transferred within the network. It is the most central and security-relevant part of a mobile network[181]. The exclusion of Huawei equipment from

[180] Deutscher Bundestag, 'Gesetz Zur Erhöhung Der IT-Sicherheit Mit Koalitionsmehrheit Beschlossen'.
[181] Handelsblatt, 'Kein Huawei: Netzbetreiber Setzen Beim 5G-Kernnetz Auf Ericsson'.

this domain indicates that the actors in the business sector accepted the portrayed threat to integrity and confidentiality of information and communication within networks. Therefore, it can be noted that these actors accepted a threat to the referent object “computer networks”.

6. Conclusion

This final section turns to answering the question to what extent the rollout of the 5G network in Germany has been securitised. Drawing on the conducted analysis, this thesis finds that the rollout has been partially securitised. Speech acts touched upon the array of the four referent objects: business networks, critical infrastructure, national security and computer networks. With regard to the first referent object, the analysis finds that speech acts referred to business networks but only scarcely included references to circumstances that would existentially threaten the maintenance of business continuity. Subsequently, no acceptance of the threat could be found amongst a potential audience. Hence, a securitisation of business networks did not occur.

Critical infrastructure was touched upon, and speech acts alluded to a circumstance which would threaten the provision of services and consequently social order and the functioning of society. Furthermore, the threat was depicted as existential, and measures were called upon to alleviate the threat. Also, the analysis found that there was audience acceptance geared towards infrastructure to be threatened in its role as the very foundation of society. Thus, the referent object of critical infrastructure was securitised.

For the latter two referent objects the analysis finds similar result. National security and computer networks were addressed heavily. Even though no substantive threats had materialised in the run-up to as well as since the beginning of the rollout, these two referent objects nevertheless were portrayed to be threatened to an existential degree. Building on this portrayal, extraordinary measures were called for. As outlined above, these calls were met with audience assent so much so that even measures were implemented. These measures corresponded to the characters of the grammar of security: larger budgetary resources are made available to deal with the threat and the circle of those endowed with decision-making is narrowed down[182]. Summing up, the referent objects of national security as well as computer networks were successfully securitised.

It can therefore be concluded that testing the Copenhagen School's Securitization Theory in the case at hand yields the result that the rollout of the 5G network in Germany experienced a partial securitisation. This means that urgency was injected into the rollout and that the topic was the target of mobilisation. Momentum was created to a point where there was enough resonance to justify the adoption of urgent and exceptional measures.

This insight helps to explain a facet of how the rollout of the 5G network in Germany took shape.

[182] The authority to assess the political trustworthiness of an equipment vendor is imparted on a committee made up of representatives of the Federal Ministry of the Interior, the Federal Ministry for Economic Affairs, the Federal Foreign Office and the Federal Chancellery; final precedence is given to the Ministry of the Interior.

Bibliography

5G PPP Architecture Working Group. 'View on 5G Architecture - Consolidated Version', February 2020. https://5g-ppp.eu/wp-content/uploads/2020/02/5G-PPP-5G-Architecture-White-Paper_final.pdf.

Aradau, Claudia. 'Security That Matters: Critical Infrastructure and Objects of Protection'. *Security Dialogue* 41, no. 5 (2010): 491–514. https://doi.org/10.1177/0967010610382687.

Balzacq, Thierry. 'A Theory of Securitization : Origins, Core Assumptions, and Variants'. In *Securitization Theory : How Security Problems Emerge and Dissolve*, edited by Thierry Balzacq. PRIO New Security Studies. Milton Park, Abingdon, Oxon: Routledge, 2011.

———. 'Enquiries into Methods: A New Framework for Securitization Analysis'. In *Securitization Theory : How Security Problems Emerge and Dissolve*, edited by Thierry Balzacq. PRIO New Security Studies. Milton Park, Abingdon, Oxon: Routledge, 2011.

Balzacq, Thierry, and Myriam Dunn Cavelty. 'A Theory of Actor-Network for Cyber-Security'. *European Journal of International Security* 1, no. 2 (2016): 176–98. https://doi.org/10.1017/eis.2016.8.

Balzacq, Thierry, Sarah Léonard, and Jan Ruzicka. '"Securitization" Revisited: Theory and Cases'. *International Relations* 30, no. 4 (5 August 2015): 494–531. https://doi.org/10.1177/0047117815596590.

Barnard-Wills, David, and Debi Ashenden. 'Securing Virtual Space: Cyber War, Cyber Terror, and Risk'. *Space and Culture* 15, no. 2 (2012): 110–23. https://doi.org/10.1177/1206331211430016.

Bendrath, Ralf. 'The Cyberwar Debate: Perception and Politics in US Critical Infrastructure Protection'. *Information & Security: An International Journal* 7 (2001): 80–103.

Bendrath, Ralf, Johan Eriksson, and Giampiero Giacomello. ‘From “Cyberterrorism” to “Cyberwar”, Back and Forth : How the United States Securitized Cyberspace’. In *International Relations and Security in the Digital Age*, edited by Johan Eriksson and Giampiero Giacomello, 57–82. Routledge Advances in International Relations and Global Politics. Taylor & Francis, 2007.

Bigo, Didier. ‘Security and Immigration: Toward a Critique of the Governmentality of Unease’. *Alternatives* 27, no. 1_suppl (1 February 2002): 63–92. https://doi.org/10.1177/03043754020270S105.

Bryman, Alan. *Social Research Methods*. 4th edition. Oxford: Oxford University Press, 2012.

Bundesministerium für Verkehr und digitale Infrastruktur. ‘5G - Initiative Für Deutschland’, 27 September 2016. https://www.bmvi.de/SharedDocs/DE/Anlage/DG/Digitales/bmvi-initiative-5-schritte-zu-5g.pdf?__blob=publicationFile.

Bundesnetzagentur. ‘Administrative Rules for Spectrum Assignments for Local Broadband Spectrum Usages in the 24.25-27.5 GHz Band’, 17 December 2020. https://www.bundesnetzagentur.de/SharedDocs/Downloads/EN/Areas/Telecommunications/Companies/TelecomRegulation/FrequencyManagement/FrequencyAssignment/LocalBroadband26GHz.pdf;jsessionid=94FFC5B5A097A2084F67AE3DB4745B2D?__blob=publicationFile&v=1.

———. ‘Administrative Rules for Spectrum Assignments for Local Spectrum Usages in the 3700-3800 MHz Band’, 19 November 2019. https://www.bundesnetzagentur.de/SharedDocs/Downloads/EN/Areas/Telecommunications/Companies/TelecomRegulation/FrequencyManagement/FrequencyAssignment/LocalBroadband3,7GHz.pdf;jsessionid=4C53498EEBCBB1F4C33C84879DC5CF3A?__blob=publicationFile&v=1.

———. ‘Eckpunkte Für Den Ausbau Digitaler Infrastrukturen Und Bedarfsermittlung Für Bundesweite Zuteilungen in Den Bereichen 2 GHz Und 3,6 GHz’, July 2017. https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Frequenzen/OffentlicheNetze/Mobilfunk/EckpunkteBedarfsermittlung.pdf;jsessionid=62097692321170596BEF4DCE0A3D3F90?__blob=publicationFile&v=2.

———. ‘Frequenzauktion 2019’, https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Breitband/MobilesBreitband/Frequenzauktion/2019/Auktion2019.html.

———. ‘Frequenz-Kompass’, July 2016. https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Frequenzen/OffentlicheNetze/Mobilfunk/DrahtloserNetzzugang/Mobilfunk2020/Kompasspapier.pdf?__blob=publicationFile&v=1.

———. ‘Informationen Zu Dem Zeitplan Der Räumung Des 700-MHz-Bandes’, June 2018. https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Frequenzen/OffentlicheNetze/Mobilfunk/700MHz.pdf?__blob=publicationFile&v=3.

———. ‘Mobiles Breitband-Projekt 2016’, https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Breitband/MobilesBreitband/Frequenzauktion/Z_Auktion2016.html?nn=268128.

———. ‘Orientierungspunkte Zur Bereitstellung von Frequenzen Für Den Ausbau Digitaler Infrastrukturen’, December 2016. https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Frequenzen/OffentlicheNetze/Mobilfunk/DrahtloserNetzzugang/Mobilfunk2020/Orientierungpunkte.pdf;jsessionid=B40D784366DD6AE082748003C7D8EBC1?__blob=publicationFile&v=1.

Buzan, Barry, and Ole Wæver. *Regions and Powers : The Structure of International Security*. Cambridge Studies in International Relations. Cambridge: Cambridge University Press, 2003.

Buzan, Barry, Ole Wæver, and Jaap de Wilde. *Security : A New Framework for Analysis*

Carrapico, Helena, and André Barrinha. ‘The EU as a Coherent (Cyber)Security Actor?’ *Journal of Common Market Studies* 55, no. 6 (2017): 1254–72. https://doi.org/10.1111/jcms.12575.

Cerulus, Laurens. ‘Germany Falls in Line with EU on Huawei’. POLITICO, 23 April 2021. https://www.politico.eu/article/germany-europe-huawei-5g-data-privacy-cybersecurity/.

Choucri, Nazli. *Cyberpolitics in International Relations*. Cambridge, Massachusetts : MIT Press, 2012.

Clark, David. ‘Characterizing Cyberspace: Past, Present and Future’. *MIT Computer Science and Artificial Intelligence Laboratory*, 12 March 2010. https://ecir.mit.edu/sites/default/files/documents/%5BClark%5D%20Characterizing%20Cyberspace-%20Past%2C%20Present%20and%20Future.pdf.

Côté, Adam. ‘Agents without Agency: Assessing the Role of the Audience in Securitization Theory’. *Security Dialogue* 47, no. 6 (24 October 2016): 541–58. https://doi.org/10.1177/0967010616672150.

Coyne, Imelda T. ‘Sampling in Qualitative Research. Purposeful and Theoretical Sampling’. *Journal of Advanced Nursing* 26, no. 3 (1997): 623–30. https://doi.org/10.1046/j.1365-2648.1997.t01-25-00999.x.

Dahmen, Leonard. ‘Diese 5G Frequenzen Nutzt Die Telekom in Deutschland’, https://www.telekom.com/de/konzern/details/5g-frequenzen-alles-was-du-wissen-musst-622924.

Deibert, Ronald. ‘Circuits of Power: Security in the Internet Environment’. In *Information Technologies and Global Politics : The Changing Scope of Power and Governance*, edited by James N. Rosenau and J. P. Singh. SUNY Series in Global Politics. Albany, NY: SUNY Press, 2002.

———. ‘Cyber-Security’. In *Routledge Handbook of Security Studies*, edited by Myriam Dunn Cavelty and Thierry Balzacq, Second edition. Handbook of Security Studies. London, 2017.

———. ‘Trajectories for Future Cybersecurity Research’. In *The Oxford Handbook of International Security*, edited by Alexandra Gheciu and William Curti Wohlforth. International Security. Oxford : Oxford University Press, 2018.

Deibert, Ronald J, and Rafal Rohozinski. ‘Risking Security: Policies and Paradoxes of Cyberspace Security’. *International Political Sociology* 4, no. 1 (2010): 15–32. https://doi.org/10.1111/j.1749-5687.2009.00088.x.

Deutscher Bundestag. ‘Gesetz Zur Erhöhung Der IT-Sicherheit Mit Koalitionsmehrheit Beschlossen’. Deutscher Bundestag, https://www.bundestag.de/dokumente/textarchiv/2021/kw04-de-sicherheit-informationstechnik-817418.

Duchâtel, Mathieu, and François Godement. ‘Europe and 5G: The Huawei Case’. Institut Montaigne, June 2019. https://www.institutmontaigne.org/ressources/pdfs/publications/europe-and-5g-huawei-case-part-2-cover.pdf.

Dunn Cavelty, Myriam. ‘Cyber-Security’. In *The Routledge Handbook of New Security Studies*, edited by J. Peter Burgess. Routledge Handbooks. London: Routledge, 2010.

———. *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*, 2008.

———. ‘Cyber-Terror-Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate’. *Journal of Information Technology & Politics* 4, no. 1 (2008): 19–36. https://doi.org/10.1300/J516v04n01_03.

———. ‘From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse’. *International Studies Review* 15, no. 1 (2013): 105–22. https://doi.org/10.1111/misr.12023.

Dunn Cavelty, Myriam, and Andreas Wenger. ‘Cyber Security Meets Security Politics: Complex Technology, Fragmented Politics, and Networked Science’. *Contemporary Security Policy* 41, no. 1 (2020): 5–32. https://doi.org/10.1080/13523260.2019.1678855.

Emmers, Ralf. ‘Securitization’. In *Contemporary Security Studies*, edited by Alan Collins, Fifth edition. Oxford: Oxford University Press.

Eriksson, Johan. ‘Cyberplagues, IT, and Security: Threat Politics in the Information Age’. *Journal of Contingencies and Crisis Management* 9, no. 4 (2001): 200–210. https://doi.org/10.1111/1468-5973.00171.

Eriksson, Johan, and Giampiero Giacomello. 'Introduction: Closing the Gap between International Relations Theory and Studies of Digital-Age Security'. In *International Relations and Security in the Digital Age*, edited by J. Eriksson and G. Giacomello, 1–28. Routledge Advances in International Relations and Global Politics. Taylor & Francis, 2007.

———. 'The Information Revolution, Security, and International Relations: (IR) Relevant Theory?' *International Political Science Review* 27, no. 3 (2006): 221–44. https://doi.org/10.1177/0192512106064462.

European 5G Observatory. '5G Observatory Quarterly Report 11 - Up to March 2021', April 2021. http://5gobservatory.eu/wp-content/uploads/2021/04/90013-5G-Observatory-Quarterly-report-11-2.pdf.

———. 'What Is 5G?', https://5gobservatory.eu/about/what-is-5g/.

European Commission. '5G Action Plan | Shaping Europe's Digital Future', https://digital-strategy.ec.europa.eu/en/policies/5g-action-plan.

———. 'Client and Supplier Countries of the EU27 in Merchandise Trade 2020', 12 April 2021. https://trade.ec.europa.eu/doclib/docs/2006/september/tradoc_122530.pdf.

———. 'Digital Economy and Society Index (DESI) 2020 - Connectivity', 2020. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=67079.

———. 'Digital Economy and Society Index (DESI) 2020 - Germany', 2020. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=66916.

———. 'Report on EU Coordinated Risk Assessment of 5G'. Text, 9 October 2019. https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6049.

Eurostat. 'China-EU - International Trade in Goods Statistics', March 2021. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=China-EU_-_international_trade_in_goods_statistics.

Fierke, Karin Marie. 'Constructivism'. In *International Relations Theories : Discipline and Diversity*, edited by Timothy Dunne, Milja Kurki, and Steve Smith, Fifth edition. Oxford : Oxford University Press, 2021.

Handelsblatt. ‘Kein Huawei: Netzbetreiber Setzen Beim 5G-Kernnetz Auf Ericsson’, https://www.handelsblatt.com/technik/it-internet/datenuebertragung-kein-huawei-netzbetreiber-setzen-beim-5g-kernnetz-auf-ericsson/27295242.html.

Hansen, Lene. ‘Theorizing the Image for Security Studies: Visual Securitization and the Muhammad Cartoon Crisis’. *European Journal of International Relations* 17, no. 1 (19 January 2011): 51–74. https://doi.org/10.1177/1354066110388593.

Hansen, Lene, and Helen Nissenbaum. ‘Digital Disaster, Cyber Security, and the Copenhagen School’. *International Studies Quarterly* 53, no. 4 (2009): 1155–75. https://doi.org/10.1111/j.1468-2478.2009.00572.x.

Horwitz, Jeremy. ‘The Definitive Guide to 5G Low, Mid, and High Band Speeds’. *VentureBeat* (blog), 10 December 2019. https://venturebeat.com/2019/12/10/the-definitive-guide-to-5g-low-mid-and-high-band-speeds/.

Huysmans, Jef. ‘Defining Social Constructivism in Security Studies: The Normative Dilemma of Writing Security’. *Alternatives* 27, no. 1_suppl (1 February 2002): 41–62. https://doi.org/10.1177/03043754020270S104.

———. ‘What’s in an Act? On Security Speech Acts and Little Security Nothings’. *Security Dialogue* 42, no. 4–5 (1 August 2011): 371–83. https://doi.org/10.1177/0967010611418713.

IEEE. ‘IEEE 5G and Beyond Technology Roadmap White Paper’, October 2017. https://futurenetworks.ieee.org/images/files/pdf/ieee-5g-roadmap-white-paper.pdf.

Inkster, Nigel. ‘The Huawei Affair and China’s Technology Ambitions’. *Survival* 61, no. 1 (2 January 2019): 105–11. https://doi.org/10.1080/00396338.2019.1568041.

Kaska, Kadri, Henrik Beckvard, and Tomáš Minárik. ‘Huawei, 5G and China as a Security Threat’. NATO Cooperative Cyber Defence Centre of Excellence, 2019. https://ccdcoe.org/uploads/2019/03/CCDCOE-Huawei-2019-03-28-FINAL.pdf.

Kello, Lucas. ‘The Meaning of the Cyber Revolution: Perils to Theory and Statecraft’. *International Security* 38, no. 2 (2013): 7–40. https://doi.org/10.1162/ISEC_a_00138.

Kleinhans, Jan-Peter. ‘5G vs. National Security, A European Perspective’. Stiftung Neue Verantwortung, February 2019. https://www.stiftung-nv.de/sites/default/files/5g_vs._national_security.pdf.

———. 'Europe's 5G Challenge and Why There Is No Easy Way Out'. TechNode, 25 June 2019. https://technode.com/2019/06/25/europes-5g-challenge-and-why-there-is-no-easy-way-out/.

———. 'Whom to Trust in a 5G World? Policy Recommendations for Europe's 5G Challenge'. Stiftung Neue Verantwortung, 12 May 2019. https://www.stiftung-nv.de/sites/default/files/whom_to_trust_in_a_5g_world.pdf.

Lacy, Mark, and Daniel Prince. 'Securitization and the Global Politics of Cybersecurity'. *Global Discourse* 8, no. 1 (2 January 2018): 100–115. https://doi.org/10.1080/23269995.2017.1415082.

Lawson, Sean. 'Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats'. *Journal of Information Technology & Politics* 10, no. 1 (2013): 86–103. https://doi.org/10.1080/19331681.2012.759059.

Lee-Makiyama, Hosuk. 'Strategic Autonomy in the Digital Age'. European Commission, Berlaymont building, 200 rue de la Loi: European Political Strategy Centre, 17 December 2018. https://ec.europa.eu/assets/epsc/files/hearing/epsc_transcript_hearing-on-strategic-autonomy.pdf.

Legarda, Helena. 'China Global Security Tracker'. International Institute for Strategic Studies, 13 February 2019. https://www.iiss.org/blogs/research-paper/2019/02/china-global-security-tracker.

McDonald, Matt. 'Securitization and the Construction of Security'. *European Journal of International Relations* 14, no. 4 (1 December 2008): 563–87. https://doi.org/10.1177/1354066108097553.

Mcsweeney, Bill. 'Identity and Security: Buzan and the Copenhagen School'. *Review of International Studies* 22, no. 1 (1996): 81–93. https://doi.org/10.1017/S0260210500118467.

Messas, Achour, Julien Huvé, David Luponis, and Laurent Inard. '5G in Europe: Time to Change Gear!' Institut Montaigne, May 2019. https://www.institutmontaigne.org/ressources/pdfs/publications/5g-europe-time-change-gear-part-1-note.pdf.

Metztger, Tim, and Marcel Laser. ‘5G in Deutschland: Stand des Netzausbaus im Überblick’. Netzwelt, https://www.netzwelt.de/5g/168913-5g-deutschland-stand-netzausbaus-ueberblick.html.

Munster, Rens van. ‘Securitization’. In *International Relations*. Oxford: Oxford University Press, 2012. https://doi.org/10.1093/obo/9780199743292-0091.

NIS Cooperation Group. ‘Cybersecurity of 5G Networks - EU Toolbox of Risk Mitigating Measures’, January 2020. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64468.

Nissenbaum, Helen. ‘Where Computer Security Meets National Security’. *Ethics and Information Technology* 7, no. 2 (1 June 2005): 61–73. https://doi.org/10.1007/s10676-005-4582-3.

Noyan, Oliver. ‘EU Countries Keep Different Approaches to Huawei on 5G Rollout’, 19 May 2021. https://www.euractiv.com/section/digital/news/eu-countries-keep-different-approaches-to-huawei-on-5g-rollout/.

Osseiran, Afif, Jose F. Monserrat, Patrick Marsch, and Olav Queseth. ‘Introduction’. In *5G Mobile and Wireless Communications Technology*, edited by Afif Osseiran, Jose F. Monserrat, and Patrick Marsch. Cambridge University Press, 2016.

Peoples, Columba, and Nick Vaughan-Williams. *Critical Security Studies : An Introduction*. 3rd edition. Abingdon, Oxon, 2021.

Pompeo, Michael R. ‘Europe Must Put Security First with 5G’. POLITICO, 1 December 2019. https://www.politico.eu/article/europe-must-put-security-first-with-5g-mike-pompeo-eu-us-china/.

Rühlig, Tim, John Seaman, and Daniel Voelsen. ‘5G and the US–China Tech Rivalry – a Test for Europe’s Future in the Digital Age’. Stiftung Neue Verantwortung, 29 June 2019. https://www.swp-berlin.org/publications/products/comments/2019C29_job_EtAl.pdf.

Schallbruch, Martin, and Isabel Skierka. *Cybersecurity in Germany*. Springer Briefs in Cybersecurity. Cham, Switzerland: Springer, 2018.

Skierka, Isabel. ‘Germany Takes the Middle Way on Huawei—for Now’. The Strategist, 13 March 2019. https://www.aspistrategist.org.au/germany-takes-the-middle-way-on-huawei-for-now/.

Stantchev, Branimir. ‘Spectrum for 5G: EU-Level Developments’. Presented at the ITU Forum: Towards 5G Enabled Gigabit Society, Athens, 12/10 2018. https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Events/2018/5G%20Greece/Session%205%20Stantchev-Athens_12102018.pdf.

Streicher, Florian. ‘5G Für 30 Prozent Der Bevölkerung 2021 - 5G-Standalone in Vorbereitung’, 29 March 2021. https://www.telefonica.de/news/corporate/2021/03/5g-fuer-30-prozent-der-bevoelkerung-2021-5g-standalone-in-vorbereitung-telefonica-deutschland-o2-startet-5g-ausbauturbo.html.

Stritzel, Holger. ‘Towards a Theory of Securitization: Copenhagen and Beyond’. *European Journal of International Relations* 13, no. 3 (1 September 2007): 357–83. https://doi.org/10.1177/1354066107080128.

The White House. ‘National Strategy to Secure 5G’, March 2020. https://trumpwhitehouse.archives.gov/wp-content/uploads/2020/03/National-Strategy-5G-Final.pdf.

Thomas, Beryl. ‘What Germany’s New Cyber Security Law Means for Huawei, Europe, and NATO’. *European Council on Foreign Relations* (blog), 5 February 2021. https://ecfr.eu/article/what-germanys-new-cyber-security-law-means-for-huawei-europe-and-nato/.

Vodafone. ‘Bye, Bye 3G – Willkommen Highspeed-Internet’, https://www.vodafone.de/business/hilfe-support/abschaltung-3g-netz.html.

Voelsen, Daniel. ‘5G, Huawei Und Die Sicherheit Unserer Kommunikationsnetze’. Stiftung Wissenschaft und Politik, The German Institute for International and Security Affairs, February 2019. https://www.swp-berlin.org/publications/products/aktuell/2019A05_job.pdf.

Vuori, Juha A. ‘Constructivism And Securitization Studies’. In *Routledge Handbook of Security Studies*, edited by Myriam Dunn Cavelty and Thierry Balzacq, Second edition. Routledge Handbooks, 2017.

———. ‘Illocutionary Logic and Strands of Securitization: Applying the Theory of Securitization to the Study of Non-Democratic Political Orders’. *European Journal of International Relations* 14, no. 1 (1 March 2008): 65–99. https://doi.org/10.1177/1354066107087767.

———. ‘The Politics of Securitized Technology’. *Global Discourse* 8, no. 1 (2 January 2018): 116–17. https://doi.org/10.1080/23269995.2017.1410370.

Wæver, Ole. ‘The EU as a Security Actor — Reflections from a Pessimistic Constructivist on Post-Sovereign Security Orders’. In *International Relations Theory and the Politics of European Integration : Power, Security and Community*, edited by Morten Kelstrup and Michael Williams. London: Routledge, 2000.

Williams, Michael C. ‘The Continuing Evolution of Securitization Theory’. In *Securitization Theory : How Security Problems Emerge and Dissolve*, edited by Thierry Balzacq. PRIO New Security Studies. Milton Park, Abingdon, Oxon: Routledge, 2011.

Wissenschaftliche Dienste des Deutschen Bundestages. ‘Sachstand: Aufbau Der 4G-/LTE- Und 5G-Mobilfunknetze in Ausgewählten Ländern’, 19 October 201AD. https://www.bundestag.de/resource/blob/579494/f0cef6f4390a67b6f4262350f0548f08/wd-5-121-18-pdf-data.pdf.

Wodak, Ruth. ‘Dilemmas of Discourse (Analysis)’. Edited by Jan Blommaert, James Paul Gee, Sara Mills, Jan Renkema, and Henry G. Widdowson. *Language in Society* 35, no. 4 (2006): 595–611.

Yin, Robert Kuo-zuir. *Case Study Research : Design and Methods*. 4th ed. Los Angeles, CA: Sage, 2009.

Zajko, Mike. ‘Canada’s Cyber Security and the Changing Threat Landscape’. *Critical Studies on Security* 3, no. 2 (2015): 147–61. https://doi.org/10.1080/21624887.2015.1071165.

Bibliography for Analysis

Business sector:

5G network for our country: Deutsche Telekom's 8-point plan for network expansion. Available at: https://www.telekom.com/de/konzern/details/5g-netz-fuer-unser-land-545416

5G whitepaper | The new network generation. Available at: https://www.vodafone.de/media/downloads/pdf/5G_Whitepaper.pdf

Telefónica's chief technology officer Mallik Rao explains in an interview the strategy behind O2's 5G rollout and why 5G is not just 5G. Available at: https://www.connect.de/ratgeber/telefonica-o2-5g-netz-ausbau-deutschland-3201169.html

Media:

5G expansion with Huawei: Germany exposes itself to massive risks. Available at: https://www.faz.net/aktuell/politik/inland/warum-der-bundestag-den-5g-ausbau-mit-huawei-korrigieren-muss-16445541.html

5G mobile communications standard : Death switch in the network? Available at: https://www.faz.net/aktuell/politik/inland/5g-mobilfunkstandard-die-gefahren-fuer-hersteller-und-konsumenten-16140042.html

5G network : The drafts are already in the drawer. Available at: https://www.faz.net/aktuell/politik/5g-netz-die-entwuerfe-liegen-schon-in-der-schublade-16549592.html

Chinese technology is a security risk. Available at: https://www.sueddeutsche.de/wirtschaft/5g-ausbau-china-sicherheit-huawei-1.4699493

Mobile communications - fear of the Chinese. Available at: https://www.sueddeutsche.de/politik/mobilfunk-furcht-vor-den-chinesen-1.4798725

Why Huawei is so divisive in politics. Available at: https://www.sueddeutsche.de/wirtschaft/huawei-5g-netzausbau-deutschland-1.4776270

5G network: Control is better. Available at: https://www.zeit.de/politik/ausland/2018-12/5g-netz-mobilfunk-huawei-deutschland-china-telekom-sicherheit

5G expansion - German government wants to exclude manufacturers from 5G expansion if necessary. Available at: https://www.zeit.de/digital/internet/2020-11/it-sicherheit-gesetz-g5-netz-ausbau-huawei

Network expansion: Huawei should stay outside. Available at: https://www.zeit.de/wirtschaft/2020-01/huawei-netzausbau-5g-sicherheit-risiken-internet

Political actors:

AfD – motion within the legislative procedure for the IT Security Law 2.0, "IT Security Law 2.0 - Creating Planning and Legal Certainty for Network Operators". Available at: https://dserver.bundestag.de/btd/19/262/1926226.pdf

CDU/CSU – position paper, "Securing Germany's digital sovereignty - Setting standards for secure 5G networks". Available at: https://www.cducsu.de/sites/default/files/2020-02/Positionspapier%205G-Netzaufbau-100220.pdf

FDP – motion in the Parliament, transferred to the committee for internal affairs, "Smart Germany – Cyber-security of 5G networks". Available at: https://dserver.bundestag.de/btd/19/140/1914046.pdf

SPD – position paper "A digitally sovereign Europe with secure 5G networks". Available at: https://www.spdfraktion.de/system/files/documents/positionspapier-ein-digital-souveraenes-europa-mit-sicheren-5g-netzen-20191217.pdf

The Greens – motion in the Parliament, transferred to the committee for internal affairs, "Measures to ensure the integrity of digital infrastructures, devices and components - For greater digital sovereignty for Germany and Europe". Available at: https://dserver.bundestag.de/btd/19/160/1916049.pdf

The Left – position paper "Mobile communications". Available at: https://www.linksfraktion.de/themen/a-z/detailansicht/mobilfunk/