# Master Thesis

# Consequences of the German 5G discourse for the development of the EU's strategic autonomy


Universiteit Leiden

**Student name:** Marta Isabel Vorwald de Vega

**E-mail address:** martavorwalddevega@yahoo.es

**Student number:** s2379996

**Master programme:** International Relations - Specialisation: Global Conflict in the Modern Era

**Word count:** 14.212 (including references but excluding the bibliography and appendices)

**Thesis supervisor:** Dr. Mohammadbagher Forough

**Second reader:** Dr. Lindsay O. Black

**Date of submission:** 3rd of July 2020

# Table of Contents

# Acronyms

**AfD:** Alternative für Deutschland (Alternative for Germany)

**BMWI:** Bundesministerium für Wirtschaft und Energie (German Ministry of Economy and Energy)

**BND:** Bundesnachrichtendienst (German Federal Intelligence Service)

**BnetzA:** Bundesnetzagentur (German Federal Network Agency)

**BSI:** Bundesamt für Sicherheit in der Informationstechnik (German Federal Office for Information Security)

**CDU/CSU:** Unionsparteien (Union parties) [Christlich Demokratische Union Deutschlands (Christian Democratic Union of Germany) and Christlich-Soziale Union in Bayern (Christian Social Union in Bavaria)]

**CFSP:** Common Foreign and Security Policy

**ESA:** European Strategic Autonomy

**EU:** European Union

**FDP:** Freie Demokratische Partei (Free Democratic Party)

**SPD:** Sozialdemokratische Partei Deutschlands (Social Democratic Party of Germany)

**SWP:** Stiftung Wissenschaft und Politik **(**German Institute for International and Security Affairs)

**TKG:** Telekommunikationsgesetz (German Telecommunications Act)

# 1. Introduction

Enabled by technology advances, the fourth industrial revolution represents a "new chapter in human development" (World Economic Forum 2020), in which emerging digital technologies are the new power resource in International Relations. Hence, an important foreign policy tool (see Spanish Ministry for Foreign Affairs and Cooperation 2020). The new fifth generation technology standard for cellular networks (5G) has the potential to change completely how we as individuals live but most importantly, revolutionise the whole functioning of industries and society at large (Webb 2018). How states approach the economic aspect (an important foreign policy tool) and the security implications of 5G, will determine its foreign and security policy power.

For the European Union (EU), 5G is "an integral determinant of strategic autonomy" (EPSC 2018). The concept of European Strategic Autonomy (ESA)[1] was first introduced in the EU's Global Strategy of 2016 (A global strategy for the European Union's foreign and security policy) and alludes to a stronger role of the EU in international politics, to consequently achieve more autonomy in its foreign and security policy. However, most scholars agree that ESA remains vague and ambiguous – depending on the legitimacy of the EU member states (Brustlein 2018; Franke and Varma 2018; Lippert et al. 2019). The EU's 5G toolbox[2] functions as a recommendation and the approach to 5G remains a national decision. Rather than looking at the EU's discourse on 5G, analysing the national discourse of a member state makes more sense. The German discourse is particularly important since Germany is one of the leading countries in the EU and the EU's foreign and security policy depends strongly on Germany's decisions (see Lehne 2012). In light of the mentioned academic, but also social relevance, this thesis will attempt to answer the following research question: *To what extent has the German discourse on 5G from 2018 until 2020 shaped the development[3] of the EU's strategic autonomy?*

This research study will firstly introduce the concept of ESA to try to find an answer to the main research question. Consequently, I will evaluate the effects of digital technologies and concretely 5G for the EU's security and economy (and thus for the development of ESA). In the following analysis chapter, the independent variables identified in the previous literature

[1] During this research study 'European Strategic Autonomy' refers more concretely to 'European Union Strategic Autonomy.'
[2] Cybersecurity of 5G networks EU Toolbox of risk-mitigating measures.
[3] 'Development of ESA' is understood as a) stronger ESA, b) weaker ESA or c) no change in ESA.

review (which explain the security and economic implications of 5G, that can shape the development of ESA into one of the three possible directions), will be explored through the German discourse. The methodology of Discursive Institutionalism (D.I.) will help in analysing the discourse. The first chapter of the analysis will be on the security threats related to 5G and the second on the economic aspects regarding 5G.

Thereby, the first and second sub-questions will read: *To what extent has the German discourse on 5G addressed security threats related to 5G and how has that approach shaped the development of ESA?*; and *To what extent has the German discourse on 5G addressed economic aspects related to 5G and how has that approach shaped the development of ESA?* Finally, the concluding chapter will present a summary of the findings, by assessing to what extent the German discourse on 5G has shaped the development of ESA into one of the three possible directions (answering the main research question and reverting to the scientific debate).

## 2. Conceptual Framework and Literature Review

Different definitions were given for the concept of ESA among the literature. As well, distinct explanations for the effects that digital technologies (and more concretely 5G) have for the development of ESA. Some scholars focus primarily on the security implications of digital technologies and 5G for the development of ESA. Others claim that economic issues have to be addressed with the same importance than security consequences.

### 2.1. The concept of European Strategic Autonomy (ESA)

ESA is part of the EU's foreign and security policy. It alludes towards a stronger role of the EU in international politics, in which it does not have to show "pure allegiance to the United States" (Lippert et al. 2019, 5) and can develop more self-sufficiency. The EU's self-reliance has been developing since the 1960s with the Common Trade Policy; the 70s with the European Political Cooperation, the Common Foreign and Security Policy (CFSP) and the Common Security and Defence Policy; and the Economic and Monetary Union in the 80s (Benneyworth 2011; Smith 2018, 609; Lippert et al. 2019, 5).

*EU Global Strategy of 2016*

It was not until 2016, nonetheless, that the concept of ESA was officially introduced in the EU Global Strategy. Due to increasing external threats and external and internal security becoming mutually more dependent, the EU's ambition would be to pursue strategic autonomy (European Union Global Strategy 2016, 4). Hence, becoming a "global security provider" (ibid., 3) and taking more responsibility for its security[4] by acting autonomously when necessary (ibid. 7, 19). Also, becoming more active instead of reactive by appearing credible and effective when taking action (Smith 2018, 613).

*European Strategic Autonomy: conceptual ambiguity*

The vague design of ESA's definition in the Global Strategy has been criticised by some scholars. These claim that important elements of ESA remain contentious, as there is no "clear definition or even an agreed understanding" (Brustlein 2018, 1-2) for the concept. Consequently, this has confused the member states and fuelled critique from the Trump administration, which has been sceptical towards European defence initiatives, claiming these

[4] Refers to being able "to deter, respond to, and protect ourselves against external threats" (European Union Global Strategy 2016, 19).

could undermine NATO (Franke and Varma 2018, 1; Lippert et al. 2019, 27). The current debate on ESA is to some extent a response to Trump's criticism and his overall "erratic foreign policy [and] critical perspective on multilateral cooperation in general" (Lippert et al. 2019, 27), new emerging threats and Brexit. The EU, however, commenced developing more self-reliance and independence when the Cold War ended, and the US started to disengage from Europe (CFSP etc.) (Lehne 2012, 8).

*Definition of ESA* by the German Institute for International and Security Affairs (SWP)

During this research paper, I employ a more extensive definition of ESA given by the German Institute for International and Security Affairs (SWP)[5]. According to the SWP, ESA is understood as:

> "[the] ability to set priorities and make decisions in matters of foreign policy and security, together with the institutional, political and material wherewithal to carry these through – in cooperation with third parties, or if need be alone. […including] the entire spectrum of foreign policy and security, and not just the dimension of defence." (Lippert et al. 2019, 1).

Like the concept of power, autonomy is also relative and can only be achieved in relation to others. Politically, it is considered more a "process rather than a condition" (ibid.), not an end itself but a means to promote and protect interests and values. Autonomy does not mean isolation, autarchy or rejection of alliances. This research study will build on this argument, comprehending strong ESA as the ability to enforce and modify international rules. Weak ESA will refer to unwillingly accepting the rules that others (e.g. the US) set, becoming subject to their strategic decisions (ibid., 5).

*The broader dimension of ESA: ESA in technology & economy*

The defence and more broadly the security realm, represent a central aspect of ESA. Nevertheless, ESA relates equally to foreign policy. The degree and capacity of ESA vary between policy fields. The concept of autonomy is not only used in relation to the US but also regarding other global, middle and emerging powers of the current multipolar world order (Lippert et al. 2019, 16).

In contrast to the security and especially the military dimension, in the economic one ["a significant source of foreign policy power" (Lippert et al. 2019, 23)], the EU and the US are much more balanced – despite recent US allegations of the "EU's trade surplus in goods with

[5] SWP is "Europe's largest think-tank in the field of international politics" (SWP 2020).

the US" (Lippert et al. 2019, 27). In the global economy (especially in terms of trade, competition and regulation), the EU is the biggest competitor, adversary and partner to global powers – this refers not only to the US but also to China (ibid., 23-24). In these aspects, the EU is perceived by China and the US as strategically autonomous. With the implementation of the General Data Protection Regulation (GDPR), the EU has demonstrated strategic leadership in data protection and regulation (Franke and Varma 2018, 14). In technological innovation terms (another source of foreign policy power), which together with economic performance is a precondition for ESA, the EU is the third major (together with North-East Asia and the US) producer of technical innovation and knowledge.

In the digital economy, the EU lies far behind the US and China. Especially in the information technology industry[6]. The EU does currently not play an important role in the "duopoly of power around digital technologies" (Leonard et al. 2019) between the US and China. Important industry examples include Artificial Intelligence, the 5G network and autonomous/robotics systems (ibid.). These deficiencies (compared to the US and China) on innovation and invention, could become a threat to the EU in the multipolar world order characterised by increasing geopolitical competition and the "growing geopolitisation of technology" (EPSC 2018). Technological capabilities and mostly emerging digital technologies, are necessary to reduce dependencies and to create global influence in the current world order.

### 2.2. Existing explanations: digital technology effects for the development of ESA

The previous explanations have demonstrated the big role that technical advances and innovation play in the field of digital technologies, for shaping the foreign policy of a country and for the overall development of ESA (see Spanish Ministry for Foreign Affairs and Cooperation 2020). According to the European Political Strategy Centre (EPSC)[7], these technologies are "an integral determinant of strategic autonomy" (EPSC 2018). The following section will explore more in-depth the specific effects of these technologies for ESA – the resulting potential benefits for the EU industry and economy but also the vulnerabilities and arising threats for the EU. Experts' opinions will also be presented, to identify concrete measures the EU should adopt to succeed economically and to reduce threats related to digital technologies – and consequently contribute to the development of ESA.

[6] Out of the 20 world-leading IT companies, half of them are Chinese and a half from the US (Leonard et al. 2019).
[7] The EPSC is the in-house think tank of the European Commission.

*Benefits & threats resulting from digital technologies for the EU industry & economy*

Digital technologies have the potential to become "productivity driver[s]" (Lee-Makiyama 2018) for the EU. For instance, for the case of blockchain technologies and Artificial Intelligence, EU start-ups that employed these technologies in 2018 attracted higher investment levels than their US or Chinese counterparts (see also Castro 2018). But again, compared to China and the US, in the EU, there are still few businesses that have adopted Artificial Intelligence or are in the process of adopting it. Because there is no EU Digital Single Market, the process is difficult for EU firms, as developing digital technologies is costly (in terms of research & development and software engineering). A non-fragmented EU market with standard rules would help those businesses grow more easily (Castro 2018; Leonard et al. 2019).

Between experts on 'strategic autonomy in the digital era,' there are discrepancies on whether foreign investment (and mostly Chinese investment in the EU) is good or bad for the development of ESA. Castro (2018) has argued that Chinese investment – coming principally from Chinese state-owned enterprises – has increased significantly in the last years and is mostly targeted at sectors which are very important to EU strategic interests (e.g. economic leadership). Part of China's innovation strategy would consist of buying foreign technology companies (many from the EU) to obtain technological know-how. At the same time, the country restricts EU investments in many Chinese sectors, treating EU and other foreign companies operating in China under different rules than Chinese ones. This "indigenous innovation strategy" (ibid.) would aim to undermine the EU's competitiveness so that China would "replace foreign technology leaders with Chinese owned ones" (ibid.). Makiyama (2018) has not seen a threat in the foreign investment itself. Investment would be necessary for the EU's economic competitiveness as well as foreign actors coming "through the front door rather than the back door" (ibid.). Market barriers like "too extense" (ibid.) EU regulation would pose a threat too for the EU's economic competitiveness – working as a hurdle to foreign investment.

Digital technology supply-chains are also a high risk for the EU's economic competitiveness as the production cycle of an end product in the EU might be distributed along with different manufacturers from diverse countries. The EU (public institutions and the private sector) relies on foreign software and hardware manufacturers for the development of critical infrastructure. If certain industries (important to the EU's economic prosperity) depend on foreign providers

for the development of vital infrastructure, the EU's economic development could become compromised (see Leonard et al. 2020).

*IT-security threats resulting from digital technologies*

Technological vulnerability is per se not dangerous for the EU's overall security until geopolitical tensions and interests are added (Kello 2018). These vulnerabilities could be misused by foreign actors (e.g. countries) to introduce malware into hardware or software components, for all kinds of pernicious purposes (e.g. military and economic espionage or to harm vital infrastructure) (ibid., Lee-Makiyama 2018).

*Enhancing economic and IT-security for the development of ESA*

To improve IT- and economic security – and contribute to the overall development of ESA – the EU should adopt certain measures concerning emerging digital technologies. The most important ones are the relationship to China, improving EU regulation and building up more resilience. Firstly, the EU should limit China in buying EU technology companies or at least ensure "fair treatment" (Castro 2018) of China towards EU businesses. Secondly, EU regulation should be more specific to be effective. Regulation should focus on "key cornerstones of the critical infrastructure where the regulation might provide added value" (Särekanno 2018). It should also provide clear criteria to condemn actions which, according to classical security policy, cannot be considered acts of war (Kello 2018). Thirdly, as acting independently in the global economy and supply-chain is not possible, the EU has to accept, that until there is no proper global cybersecurity policy, insecurity will not disappear (Kenyon 2018).

The approach to security policy should be different. Namely, assuming that adversaries probably already have access to EU critical infrastructure. The focus should be on how to minimise their "ability to inflict harm from within" (Kello 2018). Also, the EU should leave protectionism behind, concentrate on diversifying its technology providers and be more innovative to produce the technology, instead of only regulating it (Särekano 2018; Leonard et al. 2019). Collecting data and using it (like in the US), is essential for the development of the new data-driven technologies. Many of these digital technologies involve "cyber-physical systems" (Castro 2018), like smart cities or smart manufacturing. Due to the EU's engineering strengths, the EU could thrive in these terms if it would invest more in software capabilities.

For the following research study, I will explore the security and economic effects of the information technology industry (specifically those of the 5G communication technology), to then determine the overall impact that 5G has for ESA.

### 2.3. The geopolitical dimension of 5G: existing explanations of 5G effects for the development of ESA

As mobile data traffic increases globally, more efficient technology is needed. For the telecommunications market, the fifth generation of mobile networks is a "new wave of innovation" (Ericsson 2020) as it enhances faster and more data transfer capacity, massive machine connectivity and ultra-low latency (Iannacci 2017; Webb 2018). This generation of communication technology does not only serve consumers (like previous 1G, 2G, 3G and 4G did) by adding more capacity to networks which are becoming more congested but most importantly, diverse industries and society at large (Webb 2018; see Ericsson 2020). 5G has the potential to revolutionise the world by changing the way industries and businesses work. The most trending technologies (e.g. Artificial Intelligence, IoT, Virtual Reality and Augmented Reality) which rely on massive data throughput will benefit from 5G's enhancement of transmission capacity (Iannacci 2017; Ericsson 2020). As objects and environments are becoming more interconnected and adaptative, and these have to possess data transfer capabilities to be networked, the IoT technology[8] relies especially on 5G (Iannacci 2017). 5G's ultra-low latency characteristic is very important to critical IoT technology[9] which requires instantaneous, ultra-reliable and resilient connectivity.

Currently, 5G networks have already been rolled-out in many countries (being commercially available or having limited availability[10]). In other countries, the 5G network is being tested before being accessible to consumers (Murnane 2019). There are distinct companies which account as world leaders for 5G roll-outs and devices. Depending on key 5G products (like semiconductor components, equipment and software), some IT companies have more or less influence as suppliers in the global market[11].

[8] IoT fields of application: smart agriculture, smart factory, smart city/environment, smart home etc. (Iannacci 2017).
[9] Critical IoT technology is used for: remote medical surgery, traffic safety and control, wireless control of production processes, industrial manufacturing etc. (Ericsson 2020).
[10] Countries considered most advanced regarding their plans for 5G: US, China, Japan, South Korea, Singapore and Taiwan (European Parliament 2019, 13).
[11] Main supplier companies for 5G equipment: Ericsson, Samsung, Qualcomm, Nokia, Huawei, LG, ZTE, Intel and Sharp (Noble et al. 2019).

*Security threats related to 5G*

Although 5G is already available to many people on their phones, it will still take some years until it is fully implemented across industries. Soon, "being connected to the mobile network will almost be as critical as being connected to electricity" (Kleinhans 2019, 1). If a mobile network gets disrupted, this could be detrimental for many industries. Secure 5G networks are thereby essential.

The 5G roll-out debate in the EU has mostly focused on if to include Chinese 5G equipment vendors due to security concerns. The debate has been highly politicised as the US has accused Chinese companies (Huawei and ZTE) of not being trustworthy. The US House of Representatives Intelligence Committee has blamed especially Huawei, warning that it could install a "backdoor for government spying[12] purposes" (Kello 2018). The EU is concerned about making its future digitalised critical infrastructure dependent on Chinese technology – and vulnerable to possible cyber-attacks. These security concerns are not solely a result of the technical equipment, but moreover from geopolitics. Politics are the reason a foreign government might exploit access to a network for malicious purposes (Kleinhans 2019, 17). The EU finds itself in the middle of a global competition between China and the US regarding new technologies and especially 5G (Särekanno 2018). Although the European Commission views China as a "systemic rival" (2019), there is no collective foreign policy position in the EU regarding China, as governments have been following different approaches to 5G (Kleinhans 2019, 17; Lippert et al. 2019, 28). Romania, Estonia, Latvia and Poland have signed "memorandums of understanding with the US" (Kleinhans 2019, 17) to avoid Chinese 5G vendors. Germany, for instance, has been reluctant to do so.

Assessing if a vendor is trustworthy or not, according to verifiable and transparent criteria, is very subjective. A first step would be to evaluate the regulatory system of a company's country of origin by foreign policy, trade and intelligence community experts and to be able to hold a company accountable in case of wilful wrongdoing or malicious activities (ibid., 19; Lee-Makiyama 2019). Diversification is also essential for EU security. Since a diversified network is less vulnerable to attacks, diversifying in terms of 5G supplier companies is more effective than banning some suppliers from the EU market (see Kleinhans 2019). Diversification is as well important for economic security as it reduces possible dependencies.

[12] The Chinese National Intelligence Law enables the government to "require Chinese citizens, organizations and […] their equipment to collaborate with the Chinese national intelligence" (Lee-Makiyama 2018).

Apart from threat actors, insufficient security measures in the networks are also a threat to secure 5G networks. Making the networks more resilient is necessary to minimise threats coming from foreign actors. Common Criteria-based IT-security certification for sensitive mobile network equipment[13] is however not the correct approach since it merely evaluates the software quality of a vendor and neglects shortcomings on the operator's level (ibid., 8). According to Kleinhans (2019, 5), shortcomings in IT-security need to be addressed by the vendors, operators and governments. Thereupon, the security of a network depends on legislation, technical standards and how these are implemented by the vendors, how the operators configure the network equipment, the operator's continuous risk assessment and maintenance of the network. Additionally, as 5G networks are very complex, they need to be updated or repaired in case of malfunctions by the equipment vendors, which are often allowed remote access to the network. Another step towards more security would be to ensure privacy-preservation and secure maintenance of networks (ibid., 14).

*Industry & economy: possible benefits and threats*

Economic security is equally important to ESA. Thus, the industrial policy dimension of 5G cannot be neglected. It has to be addressed conjointly with IT-security and possible threats coming from foreign actors. In January 2020, the EU released the 5G toolbox[14]. The toolbox is a coordinated approach to safeguarding the security of 5G networks between all member states. It guides on how to deal with main threat actors and IT-vulnerabilities and emphasises the importance of "effective implementation of the Recommendation in order to avoid fragmentation in the Single Market" (NIS Cooperation Group 2020, 3). Fragmented national regulations should be avoided "since they create unnecessary costs for operators and vendors and do not incentivise new players to enter the market" (Kleinhans 2019, 10). High costs are associated with the installation of 5G. Mobile network operators have to acquire new radio spectrum (from the national regulator) and new equipment for the instalment (Webb 2018). However, 5G represents a business potential for the EU since operators could experience a 36% growth in revenues due to the digitalisation of industries, benefitting the EU's economic competitiveness and contributing to strong ESA (Ericsson 2020). Nokia and Ericsson, the two

[13] Most widely used and accepted framework that certifies the IT-security of products (Kleinhans 2019).

[14] The toolbox was released following the member states' national risk assessments (EU Coordinated Risk Assessment on Cybersecurity in 5G Networks) of their 5G network infrastructures and ENISA's (the European Union Agency for Cybersecurity) threat landscape mapping (NIS Cooperation Group 2020, 3). The coordinated risk assessment identified mitigation measures which could be applied at national and EU level. The toolbox functions as a framework which concretises common measures to be prioritised at the national and EU level (ibid., 4).

EU companies which produce 5G equipment, are the major suppliers of some of the 5G roll-out leading countries (US, Japan, South Korea). Including those companies for further implementation or modernisation of 5G in EU countries is essential for future EU economic competitiveness.

## 3. Research Design

The 5G toolbox remains a recommendation and is open for interpretation by the EU member states. How to approach the 5G dimension is a decision that each state can adopt individually (see Leonard et al. 2020). As the development of ESA also depends mostly on the contribution of the member states to it, it is particularly interesting to analyse the national 5G discourse of a member state, to then evaluate the extent to which this discourse shapes the development of ESA. The German 5G discourse can provide practical knowledge that might contribute to the theoretical debate of 'what constitutes ESA.' Firstly, as 5G has an economic and security dimension, it is an important tool for the EU's foreign and security policy that can shape the development of ESA. Secondly, Germany is considered one of the leading nations (if not the leading) in shaping EU foreign and security policy. The following research design will elaborate on this argument, justifying the German case-selection and presenting the methodology.

*Case-selection: The German discourse*

Decisions in EU foreign and security policy tend to be consensus-based and intergovernmental – hindering the process towards ESA (Franke et al. 2018, 10). Most scholars agree that for strong ESA, Germany and France (the two global actors in the EU after Brexit) have to adopt a leadership role and cooperate (see Lehne 2012; Franke et al. 2018; Lippert et al. 2019). Germany is considered by many member states "a (or the) leading nation"[15] (Lippert et al. 2019, 7). It is the largest economy and most inhabited country in the EU. Germany sends 96 members of Parliament to the European Parliament (constituted of 705 members) (Deutschland.de 2019). The country has further recently been adopting a leadership role not only in monetary and economic affairs but also in foreign and security policy. Germany has directly shaped three past crises (Ukraine conflict, Greek euro crisis and refugee crisis), underlining its "pivotal role" (Janning 2015) in the EU. According to a survey from 2015, it was already then perceived by "political elites across all EU member states [… ] "the most influential member state" (ibid.). Without Germany's decisive contribution, there can be no ESA (Lippert et al. 2019). At the same time, Germany considers the EU a very important foreign policy tool (see Lehne 2012). Germany also interacts with the US and China in bilateral inter-governmental meetings[16] on a much frequent basis than other member states (Lippert et

[15] Due to its high industrial profile, GDP and foreign trade ratio (Lippert et al. 2019).
[16] On many levels: economically, politically, technologically etc.

al 2019, 28). However, the Trump administration has been since the beginning critical regarding security matters (including 5G) towards the EU and Germany in particular (Franke and Varma 2018). In Germany, the ESA discourse has only gained momentum in response to US' criticism. As the US and China play an important role in the global 5G debate and the concept of ESA alludes partially to more autonomy from global powers, analysing the German discourse is especially interesting.

The limitations of this research study also need to be highlighted. A major one is a limited scope, allowing a comprehensive study of just one national discourse to determine how ESA is shaped. Examining more discourses of member states would not have been as effective. Limiting the richness of detail would have distracted from the in-depth analysis. Secondly, a full-blown analysis of all policy fields that shape ESA goes beyond the scope of this thesis.

*Conceptualisation and operationalisation*

The definition of the SWP (presented in the conceptual framework) will be used throughout the analysis to determine the three possibilities for the development of ESA. The maintenance of the status quo (no change) will be interpreted as no development of ESA – neither development towards stronger nor weaker ESA. Since 'autonomy' in ESA refers to autonomy in EU foreign and security policy, the policy fields 'security related to digital technologies' and 'economic performance' are representative for ESA. The former is a foreign policy resource, and the latter is part of the EU's overall security policy. As 5G has implications for security and economic policy, how these two policy fields are addressed by Germany (if conjointly or by focusing only on one field) will determine the development of ESA.

Following the presentation of the dependent variable 'ESA,' the independent variables (causal conditions) will be explained, taking into account two categories developed along with the literature review. These two categories explain the relationship between ESA and the most relevant consequences of 5G, which can shape the development of ESA into one of the three possible directions. Consequently, the variables chosen for each category (*1. security implications of 5G, 2. economic impact of 5G*) will be operationalised. Due to scope limitations, not all 5G independent variables which can shape the development of ESA will be considered. The most relevant ones (deducted from the literature review) which will be operationalised are the following ones: *1. a) relationships to foreign threat actors, b) IT-security of networks, 2. c) EU regulation and d) innovation in EU market*.

To measure the development of ESA regarding *variable a)*, the following aspects are representative of development towards stronger ESA: a cooperative relationship towards foreign threat-actors, through an assessment of the regulatory system of the threat-actor by experts; the diversification of suppliers of digital technology components; limited foreign investment by threat-actors in EU technology companies, or ensuring fair treatment of EU companies operating in the country of origin of the threat-actor and companies hold accountable in case of malicious activities. For development towards weaker ESA, the following aspects are representative: banning foreign companies from the EU market, non-diversification, allowing uncontrolled investment and non-action in case of malicious activities.

Regarding *variable b)*, the following aspects are representative of stronger ESA: more investment in the security of EU networks and more secure maintenance of networks with privacy-preserving measures, to reduce threats of foreign suppliers with remote access. For weaker ESA: no investment and no security maintenance of networks.

For *variable c)*, the following aspects are representative of development towards stronger ESA: non-fragmented EU regulation. For weaker ESA, the following aspects are representative: fragmented regulation, which reduces the EU's economic competitiveness and Common Criteria-based IT-security certification for sensitive mobile network equipment (only evaluates software quality of vendor and neglects shortcomings on operator's level).

Finally, for *variable d)*, the following aspects are representative of stronger ESA: more investment in EU IT-companies and further EU businesses and industries employing 5G technology. For weaker ESA: no investment and no employment of 5G in businesses and industries.

Before proceeding with the methodology, it is essential to emphasise again that all four independent variables are crucial to determine the development of ESA. Not including all of them into the analysis would make the assessment of ESA incoherent since all four are the most relevant consequences of 5G that can shape the development of ESA. In the analytical part, I will expand on this argument by explaining the immediate relationship between the variables.

*Methodology: Discursive Institutionalism*

To answer the main research question, I will analyse the German 5G discourse. According to one's analytical approach to IR discourse analysis (D.A.), one can perceive the social structure as constituting discourses or agents' discourses as constituting the social structure. Foucault (1969), Gramsci and Habermas (1971) include the agent into the analysis (quoted in Carta et al. 2014, 4-5). These scholars of constructivist ontology do not perceive politics solely as a "phenomenon of the superstructure" (Habermas 1971, 101 quoted in Carta et al. 2014, 4). In their eyes, society exerts power and social transformation through communicative action. According to Habermas (1984), discourse is considered intersubjective and interactive (quoted in Carta et al. 2014, 2). Furthermore, the interpretative constructivist epistemology understands agents as constructing social reality. Agents interact discursively within a given structure and simultaneously reconstruct their preferences through their interaction within that structural context (Carta et al 2014, 7).

Discursive Institutionalism (D.I.) is a specific type of D.A. of constructivist ontology. D.I. understands discourse as being constitutive of (instead of constituted by) the social world. According to Schmidt (2008), discourses not only represent ideas (what is said) but also the discursive interactions (who said what to whom, where, how, when and why). D.I. is therefore also about agency (who said what to whom) and not only about structure (what is said, where and how) – institutions influence "agents [… and are] influenced by them" (Carta et al. 2014, 314).

In D.I., the analysis has to be conducted on three distinct levels. Firstly on the generality level of ideas and their content, secondly on the interactive processes through which those ideas are exchanged and thirdly on the institutional context in which those ideas and discourses are taking place (Schmidt 2008, 3). Due to scope conditions, for the following research study, the first level will not be contemplated. As the variables that could shape the development of ESA have already been identified, the following analysis will focus on identifying how these ideas are exchanged within the German institutional context. The first sub-question will analyse how the ideas about 'relationship to foreign threat actors' and 'IT-security of networks' are addressed in the coordinative discourse (discourse among policy actors) and the communicative discourse (discourse between political actors and the public) (see ibid., 8-10).

The second sub-question will assess how 'EU regulation' and 'innovation in EU market' are addressed again in both discourses.

Studying the German discourse through D.I. is especially appropriate since the German governing activity is distributed among many different authorities. This institutional characteristic makes the coordinative discourse more elaborate than the communicative (in Germany). Negotiations among many actors take place at the coordinative level, and these negotiations are then communicated in vague terms to the German public to not jeopardise compromises made in private among policy actors (ibid., 10). Therefore, the coordinative discourse will be studied in much more detail than the communicative one. I will still look at the communicative discourse since the development of ESA requires "high external and internal political legitimacy [and] internal legitimacy is strongly dependent on the governments and the citizens of the EU member states" (Lippert et al 2019, 14). The government corresponds to the coordinative discourse and the citizens to the communicative. For determining the development of ESA, it is necessary to include the whole German society (coordinative and communicative) into the 5G discourse. D.I. suits very well to analyse the relevant levels of discourses.

However, only the coordinative discourse can tangibly shape the development of ESA by influencing the decision-making process. The communicative discourse is a "mass process of public persuasion [that] engender[s] debate" (Schmidt 2008, 8). It focuses on how ideas from the coordinative discourse are debated, helping to understand the political climate and public opinion. Yet, regarding 5G in Germany, it only responds to governmental decisions and cannot shape the decision-making process. For that reason and due to the previous justifications, the latter discourse will be evaluated in significantly more detail than the former. Almost the complete analysis for each independent variable will be on sources from the coordinative discourse. Communicative-level data will be merely included for the representativeness of the German society and the internal legitimacy of ESA.

According to Schmidt (2008), for the coordinative discourse, the chosen data will be drawn mainly from official statements of policy documents or interventions of parliamentarians, network operators in Germany and experts. For the communicative discourse, the sources that I will employ are German newspaper articles. The analysis will encompass the period from the end of 2018 until the beginning of 2020 (when the 5G debate started to gain momentum in

Germany). I will prioritise on the most recent data as that data will provide a more comprehensive picture of the current discourse.

## 4. Analysis: How have security threats and economic aspects related to 5G been addressed in the German discourse?

The consequent section will be devoted to evaluating how the independent variables[17] are approached in the German 5G discourse to then determine the development of ESA. Each independent variable has been interpreted independently to lose no overview and structure in the analysis. *Variable b) (IT-security of networks)* and *variable d) (innovation in EU market)* will apply as well to the security of German networks and innovation in the German market since the latter ones contribute immediately to the former ones.

When searching for data, more independent variables were identified that could have been included into one of the two categories (*1. security implications of 5G, 2. economic impact of 5G implications*)[18] developed along with the literature review. Apart from the four independent variables, the predominant reoccurring theme in the German 5G discourse was 'resulting health risks of 5G.' The theme was specially raised by the opposition and through the petitions committee[19]. Although the theme should not be neglected in terms of representativeness of the overall 5G debate in Germany, for the following analysis I will not elaborate on it since it cannot contribute to the development of ESA into one of the three possible directions. The same applies to other topics which are exclusively domestic and are thereby not interesting for further analysis. These include, for instance, the German 5G frequency auction and all the related parliamentary debates or conversations with representatives of mobile network operators performing in Germany.

Due to scope conditions, only the most recent and representative sources have been selected (for the discourse analysis) from the wide amount of data that I found. With representative sources, I refer to the ones that allude clearly to one of the four independent variables. Not all national strategies and publications, policy and press documents, passed legislation, parliamentary debates or measures taken by the German government related to digital technologies and 5G, will be included in the analysis. After interpreting the data, I will ideally be able to identify a pattern of prevalent themes within the two mentioned categories. This pattern and how the two categories are addressed in the German 5G debate (if conjointly or

[17] Independent variables that can shape the development of ESA: 1. *a) relationships to foreign threat actors* and *b) IT-security of networks*, 2. *c) EU regulation* and *d) innovation in EU market*.
[18] These two categories compile the principal consequences of 5G, which can shape the development of ESA.
[19] The petitions committee represents the German population. It allows citizens to send letters of request or complaint to the Bundestag (German federal parliament).

not) will ultimately elucidate on the process of the development of ESA. To recall, for each independent variable, almost the complete analysis will be on sources from the coordinative discourse.

Before proceeding with the analysis, I will give a brief overview of the political context surrounding the German 5G debate. The present Bundestag (German federal parliament) is constituted by six political groups. On the one hand, the incumbent coalition government (since the 24th of September 2017) is comprised of the conservative CDU/CSU group (Union parties)[20] and the social-democrat SPD group. On the other hand, the opposition consists of the following political groups: The Left, The Greens, the liberal FDP and the right-wing AfD[21].

As a result of the radio frequencies auction, the designated mobile network operators responsible for the 5G roll-out in Germany are Deutsche Telekom, Vodafone and Telefonica Deutschland. The nationwide roll-out will yet take years to be completed. Besides, the 4G roll-out has not been fully implemented across the whole country (Süddeutsche Zeitung 2020 c). Some rural areas are especially negatively affected, having poor reception and sometimes no signal at all.

The consecutive section will be devoted to finding out what Germany's approach towards 5G has been. Has Germany been prioritising the importance of the economic dimension of 5G or rather the security dimension? Perhaps, has it been addressing both dimensions equally? The German discourse is very important for the concept of ESA since German economic and security decisions will ultimately have implications for the whole EU. If Germany demonstrates the ability to enforcing and modifying international rules and in addressing the four independent variables altogether and adequately, it could contribute to strengthening ESA. The country could subsequently weaken ESA too, if it unwillingly accepts the rules of others by being subject to their strategic decisions and if it does not address the four independent variables as a whole and correctly (see Lippert et al. 2019, 5).

Germany itself does not perceive ESA as a "realistic goal" (Franke and Varma 2018) or an end itself" (Lippert et al. 2019) but rather a "means to protect and promote values and interests"

[20] The union parties are a political alliance of the Christian Democratic Union of Germany (CDU) and the Christian Social Union in Bavaria (CSU).
[21] Political groups in the German Bundestag: The Left (Die Linke), SPD (Sozialdemokratische Partei Deutschlands), The Greens (Bündnis 90/Die Grünen), FDP (Freie Demokratische Partei) and AfD (Alternative für Deutschland).

(ibid.). Throughout this research study, ESA is understood as a process instead of an "absolute condition" (ibid.). Germany has emphasised "leading through consensus" (Janning and Möller 2016) instead of as a hegemon. Accordingly, during this research study, Germany's influence on the EU discourse is interpreted as steps taken by Germany into a direction that could shape ESA but not as tangible mechanisms through which Germany exerts influence on the EU 5G discourse.

The most relevant stakeholders that have been selected for the German 5G coordinative discourse are the parliamentarians of the German Bundestag (from the coalition government and the opposition). Equally important to the coordinative discourse are the experts that participate in it. The expert's discourse will be documented as part of discussions in the German Bundestag, for instance, in the form of public expert discussions in a specific ministry or committee. Within experts, I include representatives of mobile network operators (Telekom Deutschland, Vodafone and Telefonica Deutschland); the main 5G technology providers (Ericsson, Nokia and Huawei) and think tanks (Stiftung Neue Verantwortung and Mercator Institute for China Studies). Some parliamentary debates, governmental responses to motions by the opposition, meetings or discussions, are used several times. From those documents, some contain useful information for the assessment of more than one independent variable. Most data found corresponded to independent *variable a)*.

For the communicative analysis, I will employ recent articles from two important German newspapers, namely 'Frankfurter Allgemeine Zeitung' and 'Süddeutsche Zeitung.' More stakeholders could have been included in the analysis of the communicative discourse. Due to scope conditions, I will nonetheless only use articles which allude to the independent variables, and that include statements of political leaders or experts. German journalists are the most far-reaching and influential stakeholders in the communicative discourse since the opposition often relies on their articles by quoting some of them in their motions. 5G is a discussion topic that remains mostly part of closed coordinative debates, due to its technical, and foreign and security policy dimension. Thus, the media is more representative for the communicative discourse than the "general public of citizens and voters" (Schmidt 2008, 9). The media can, in this case, exert more influence than German citizens on the coordinative discourse – and consequently contribute to the internal legitimacy of ESA. When recompiling the data corresponding to the communicative discourse, the majority of articles found alluded to independent *variable a) (relationship to foreign threat actors)*. For some variables, only a few

sources were found (for some none). Thereby, *variables c) (EU regulation)* and *d) (innovation in EU market)* were identified in a much lower proportion. For *variable b) (IT-security of networks)* no article was found. Given the previous explanations, independent *variable a)* is a fair starting point for the analysis.

Finally, it is essential to remember that sources corresponding to the communicative discourse are only included in the analysis to represent the whole German society and discourse. The media (the main stakeholder of the communicative discourse) cannot influence the decision-making process regarding 5G and ESA as much as the German parliament (including the government, opposition and experts participating in it) and especially the German government. Thus, for the final evaluation of the development of ESA, only the data corresponding to the coordinative level will be employed.

### 4.1. Security threats related to 5G

*a) Relationship to foreign threat actors*

Regarding the specific aspects of *variable a)* that can shape the development of ESA into one of the three directions, only half of them were mentioned, namely 'cooperative relationship,' 'diversification' and 'banning foreign companies from the EU market.' The fact that the other remaining aspects[22] were not named and that from the mentioned ones, two of the three apply to development towards stronger ESA, makes the assessment of ESA more complicated. There are more factors which need to be explored to have a comprehensive understanding of *variable a)* that can then help determine the development of ESA.

Firstly, the opposition presented itself very critical towards the government. It accused the coalition government of not being coherent in its course-of-action statements regarding Huawei and national security. The critique referred to governmental representatives having expressed contradicting opinions on how to deal with suppliers considered not trustworthy. Reference was made specifically to chancellor Merkel, the president of the Federal Intelligence Service (Bundesnachrichtendienst – BND) and other representatives of German security services. In a

[22] For example, for stronger ESA: limit foreign investment by threat-actors in EU technology companies or ensure fair treatment of EU companies operating in the country of origin of the threat-actor and hold companies accountable in case of malicious activities.

governmental response to a motion[23] by the FDP, Merkel and Gerhard Schindler (president of the BND) were quoted.

According to Merkel, conversations would have to take place with the Chinese government, about Huawei not handing data over to the state. However, when working in Germany, the Chinese state would not be able to access all data of all Chinese products (Governmental response to FDP motion 2019). In German newspaper articles, chancellor Merkel was quoted various times speaking out against special treatment for Huawei (and Chinese companies) and having advocated for the non-exclusion of Huawei from the outset and general security requirements for suppliers (Frankfurter Allgemeine 2020; Süddeutsche Zeitung 2020 f, a). The media framed the government's rejection of a total blockade of Huawei, as a German fear that China would boycott German companies if Huawei was explicitly banned (Süddeutsche Zeitung 2020 b). According to the press, the Chinese leadership would have even threatened to take economic sanctions against the German industry. General security requirements should thus send a message to China (an important trading partner of Germany) that the procedure would only be a normal technical examination instead of a vote of no confidence against the country (Süddeutsche Zeitung 2020 g).

According to Schindler, the president of the BND, whoever provided the technology would also be able to intercept communications. Installing security systems would not make the risk disappear. Due to the fear of back doors, he pronounced himself for the exclusion of Huawei from the German 5G roll-out (Governmental response to FDP motion 2019). During a meeting of the Digital Agenda Committee (2019), a representative of the Federal Foreign Office also framed the 5G topic a matter of national security. Although the representative did not pronounce himself in favour of excluding Huawei, he did consider the company a not trustworthy partner based on past security-related incidents. He emphasised that Germany could not be working with companies which cooperated with a national secret service.

The critique towards the government did also concern the government's approach itself towards foreign threat actors. Criticism came in this aspect especially from the AfD group, although to a smaller extent also from The Left group. Parliamentarians from these two groups

[23] A governmental reply to a motion includes firstly, a summary of the demands made in the motion and secondly, answers to the questions posed in the motion.

framed Huawei a major threat to 5G security in Germany, to which the government had no convincing response strategy.

The AfD further referred to other countries having banned Huawei for their 5G roll-out for national security reasons and demanded proof of state-independence for network equipment suppliers (AfD motion 2019; parliamentary debate 2019). The German press highlighted the political dispute around the question of whether the government could exclude Chinese suppliers without evidence of malicious activities by the suppliers' side. Mentioned were numerous attempts by the US of persuading the German government to dispense from Chinese technology in their 5G roll-out. A lot would depend on the German decision since as Britain had not succumbed to the US's pressure, the Trump administration would fear that more European governments would not follow its course (Frankfurter Allgemeine 2020; Süddeutsche Zeitung 2020 f, a).

The AfD political group suggested prioritising companies with their headquarters in democratic European countries, which would thus be subject to control by European institutions (AfD motion 2019; parliamentary debate 2019). It also enquired if the government could rule out the possibility of foreign intelligence services carrying out surveillance activities after the 5G roll-out. Moreover, the group demanded from the government to take all regulatory measures possible to ensure that network equipment of dubious integrity would not be considered. According to the AfD, this would apply if the security of critical infrastructures, the economic competitiveness of Germany and Germany's technological sovereignty were at risk (AfD minor interpellation 2019; parliamentary debate 2019).

Lastly, though not as critical towards Huawei as the rest of the opposition, the FDP group wanted to know to what extent Chinese companies were already involved in projects and infrastructure of German federal ministries and authorities. To this motion, the government replied by stating that making information on technical skills and equipment available to an unrestricted group of people at home and abroad, could be disadvantageous for the security of the Federal Republic of Germany and would thus remain classified (Governmental response to FDP motion 2020).

As seen, some representatives of the government and members of the opposition expressed their willingness to ban foreign companies. This aspect does not contribute to the development

of stronger ESA. However, the chancellor, representatives of the Ministry of Economy and Energy (Bundesministerium für Wirtschaft und Energie – BMWI), and written responses of the government to motions of the opposition demonstrated a much more cooperative approach. In the relationship towards foreign threat actors, they assessed the regulatory system of the dangerous actor and insisted on the diversification of suppliers – aspects that contribute to stronger ESA. In a governmental response to a motion by the AfD (2019 a), the government assured not having any information on a specific security incident involving telecommunications hardware from Huawei and being aware of the legislation and administrative practices in China (Governmental response to AfD motion 2019). A representative of the BMWI further stated that excluding specific providers would not contribute to the immediate security of the networks and pointed the necessity of ensuring diversification in terms of network operators and manufacturers (Digital Agenda Committee meeting 2019). Besides, the government assured having been in conversations since 2018 regarding the German 5G roll-out, with the following companies: Cisco, Ericsson, Nokia and Huawei (Governmental response to FDP motion 2019).

Lastly, the experts that participated in the 5G discourse also have to be included since they possessed a high level of influence in the ultimate decision-making process of the government and the opinion of the whole Bundestag. They contributed with their opinions in the deliberation of ministries and committees by mostly opposing the exclusion of individual providers. Mikko Huotari, from the Mercator Institute for China Studies, characterised Huawei as a company with nontransparent ownership structures, that would not be expected to be bound by law due to the lack of the rule of law and separation of powers in China. Huotari and a representative of the Institute Montaigne considered that although the risks with Huawei were difficult to calculate, exclusion should not be the solution. A Chinese attack on data from 5G networks could as well take place when using technical components that were not manufactured in China. From the Federal Association of the German Industry, the argument was that the exclusion of individual providers would affect the German industry negatively, which needed efficient networks in the present and not in a few years. A representative of Deutsche Telekom stressed that 5G would not completely replace the previous generations but rather build on them. Since Huawei had been deployed by German network operators for the previous generations, changing Huawei technology for new technology would take decades until being fully implemented. Also, countries wanting to become leaders in the 5G market, could not get past Huawei technology.

The media focused on how completely excluding Huawei would be very expensive, since Vodafone and Deutsche Telekom had installed Huawei technology already in their 4G networks. The articles moreover highlighted that in the 4G networks, technology from Nokia and Ericsson was also installed. These companies were characterised as competitors of Huawei (Süddeutsche Zeitung 2020 b, e). Combining various suppliers was also recommended by a representative of the European School of Management and Technology in Berlin. To conclude, the representative of Huawei in Germany denied some allegations made by the other experts, claiming that Huawei would only sell equipment and not operate the networks, nor own them. The representative denied that the new Chinese intelligence law would require Huawei to collect data from its customers in China or abroad (Foreign Affairs Committee 2019 a; Foreign Affairs Committee 2019).

Due to a sometimes not coherent governmental discourse and because some important information remained part of closed debates, the opposition was very critical towards the government. "[C]oherence [in a] discourse can add to its strength" (Schmidt 2008, 10) and the government's discourse lacked coherence. I interpret the classified information and the vagueness in responding to some motions as a leverage tool from the government to have more room for manoeuvre regarding how to deal with foreign threat actors, but also, to be less vulnerable to critique and demands by the opposition. Furthermore, as "vagueness helps in particular in the context of international diplomacy" (ibid.,9), Germany's caution in positioning itself against a Chinese company like Huawei can be interpreted as the German government not wanting to directly confront the Chinese leadership.

German newspaper articles were fixed on Huawei rather than on the general evaluation of possible foreign threat actors for the 5G roll-out in Germany. Instead of addressing foreign threat actors generally (based on an analysis of the regulatory system of the home country of the actor), the media focused on justifying why the government had not banned Huawei from the outset. The government and the chancellor were presented as strategically autonomous actors in the transatlantic relationship. However, in the relationship to China, they appeared – according to the media's opinion – much weaker in their decision-making autonomy. It seems as if the chancellor decided to impose general security requirements for suppliers instead of banning Huawei, not based on its own will, but rather because China represented a bigger threat than the US. Regarding 'diversification of suppliers' the media again focused on Huawei. It

compared the company to other suppliers instead of explaining why the diversification of suppliers is important for the general security of the 5G network. Diversification is essential to avoid dependencies on a sole supplier and consequent negative ramifications for economic security and IT-security.

To summarise, within the opposition, the stance of the AfD and The Left on how to deal with foreign threat actors is representative of development towards weaker ESA. Due to the listed reasons, the media's discourse also weakened the development of ESA. On the contrary, the government's and experts' position is representative of development towards stronger ESA. Since the government is the ultimate decision-maker, the government's position is more influential than the opposition's and the media's. In the long-term, however, a very critical opposition and press could become problematic for decisive decision-making by the government. Moreover, no reference was made to foreign investment, fair treatment and accountability[24] – equally important aspects to the development of ESA. Regarding *variable a) (relationship to foreign threat actors)* it is fair to say, that the development of ESA was neither weakened nor strengthened. The status quo was maintained and the development of ESA did not change.

b) *IT-security of networks*

Apart from the 'relationship to foreign threat actors,' the 'IT-security of networks' is just as important to evaluate the security implications of 5G. These two independent variables are the two most relevant security consequences of 5G *(category 1)*, which can shape the development of ESA into one of the three possible directions. *Variable b) (IT-security of networks)* immediately builds upon *variable a) (relationship to foreign threat actors)*, and both variables are mutually dependent. For instance, if for *variable a)* all aspects that measure the development towards stronger ESA are given but then for *variable b)* the aspects given do not contribute to stronger ESA, the security of 5G could become compromised. On the one hand, having a cooperative relationship to the threat actor would alone not suffice since the security of 5G depends equally on a secure network. On the other hand, investing in a secure network would not be enough since if the relationship to the foreign threat actor is not cooperative, the threat actor could eventually find a way to disrupt the network.

[24] Foreign investment by threat-actors in EU technology companies, fair treatment of EU companies operating in the country of origin of the threat-actor and companies hold accountable in case of malicious activities (last two aspects refer to development towards stronger ESA). For the last two aspects, non-action would refer to development towards weaker ESA.

Regarding 'IT- security of networks' the opposition was less critical towards the government than within the context of *independent variable a)*. Still, some criticisms were expressed during a parliamentary debate in February 2019. During this debate, all political groups were discontent with the government's digital policy and reproached the government of neglecting the IT-security of the German 5G networks. The FDP, The Left and The Greens demanded to separate the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik - BSI) from the Federal Ministry of the Interior. The FDP even insisted on establishing a digital ministry. In response to such claims, a representative of a government party reminded the opposition of the IT-security law 2.0, which would be brought before parliament in 2019 and would make a decisive contribution to improving IT-infrastructure (Das Parlament 2019).

In meetings of the Foreign Affairs Committee, experts expressed the need for improving the security in the German 5G roll-out. During a consultation of the Foreign Affairs Committee (2019), Martin Schallbruch, from the European School of Management and Technology in Berlin, highlighted the considerable role that security acquired in the fifth generation. He described 5G as more software-based than the previous generations and hence more decentralised and complex. Since this could result in a larger potential area of attack, 5G would be more dependent than the previous generations on the identification of security gaps and permanent software updates. In a public expert discussion of the Foreign Affairs Committee (2019 a) earlier that year, Jan-Peter Kleinhans, from the SNV (Stiftung Neue Verantwortung) – a think-tank at the intersection of technology and society – pointed to the need of minimising risks already during network planning and configuration. In the literature review, aspects were identified that characterise the security of a network. Accordingly, 5G network security depends on legislation, technical standards, how these standards are implemented by vendors, how network equipment is configured by operators and more secure maintenance of networks with privacy-preserving measures.

I will proceed with assessing how these aspects (that can shape the development of ESA) are addressed by the government. For this purpose, I will analyse governmental responses to motions of the FDP and AfD, and the statements of a representative of the BMWI in a meeting of the Bundestag Committee Digital Agenda. To begin, in a governmental response to a motion of the AfD (2018 b), the government assured that the security of 5G networks was playing a

significant role within the context of the international standardisation process for mobile telecommunications. According to Kleinhans (2019), the development of trustworthy and secure standards would be the responsibility of governments, vendors and operators "as part of their work in 3GPP, the global standardization body for mobile equipment" (6). After those standards were defined, networks would have to comply with them (ibid., 5).

Technical standards alone do not contribute to the overall IT security of 5G. Thus, the government stated that operators and service providers were legally obliged to take certain technical and organisational preventive measures to ensure the security of telecommunications networks (like the creation of security concepts and the appointment of security officers) (Governmental response to FDP motion 2019). These security concepts would have to be submitted to the Federal Network Agency (Bundesnetzagentur – BnetzA) to be reviewed by it. This agency would also be able to order an inspection of network operators by a qualified independent body (Governmental response to AfD motion (2018 b). Additionally, according to a new approach by the BNetzA and the BSI from the 7th of March 2019, security requirements would apply not only to 5G networks but also to existing network technology (from previous generations on which 5G is set up). Security requirements should especially be concretised for operators with increased risk potential. Compliance with all these requirements would be legally mandatory (Governmental response to FDP motion 2019). Moreover, it would be the operator's obligation to prove that those security conditions had been fulfilled (Digital Agenda Committee 2019). Operators would also be forced by law [(by the German Telecommunications Act – Telekommunikationsgesetz (TKG)] to take appropriate technical measures to safeguard the confidentiality of telecommunications and to prevent interferences, especially to be protected against unauthorised access (Governmental response to AfD motion (2018 b). Lastly, the government assured that the German 5G strategy would also contain additional information on protecting 5G infrastructure against IT attacks (Governmental response to AfD motion 2018 b).

Despite the criticism coming from the opposition, the previous findings and especially the government's statements demonstrate the government's ambition in contributing to IT-security of the German 5G network. The government is aiming to make the networks more resilient to minimise possible threats coming from foreign threat actors. Although tangible results will rather be observed in the future, the statements indicate the path that the government wants to

take. Thus, after assessing the aspects regarding *variable b)* that can shape the development of ESA, I state that the development has been strengthened.

How technical standards are implemented is the vendor's responsibility (Kleinhans 2019, 6). Germany cannot influence completely the vendor regarding how to implement the standards. As previously seen, it can, however, decide about its relationship to foreign threat actors and improve the resilience of its 5G network. In addition, it can regulate the technology originating from foreign threat actors by setting security standards or innovating within its market. The next part of the analysis will be devoted to the German approach to regulation.

### 4.2. Economic aspects related to 5G

*c) EU regulation*

After exploring independent *variables a)* and *b)* of category 1 *(security implications of 5G)*, I will look at category 2 (*economic impact of 5G*). ESA applies to autonomy in EU foreign and security policy. 'Security related to digital technologies' and 'economic performance' are two policy fields representative of EU foreign and security policy. As 5G has implications for security but also for economic policy, both fields have to be addressed conjointly to measure the development of ESA. For example, for development towards stronger ESA, a correct approach to both 5G security and 5G economic implications is equally important. Furthermore, *variable c)* is again linked to *variables a)* and *b)*. Non-fragmented regulation – an aspect of *variable c)* that strengthens the development of ESA – also affects the 'relationship to foreign threat actors' and 'IT-security of networks.' It can improve efficiency when setting common standards at EU level about how to approach the relationship and IT-security.

For *variable c)*, how the German government deals with regulation (fragmented or not) and what its approach is to Common Criteria-based IT-security certification (certification of critical core components), will determine the development of ESA into one of the three possible directions. For stronger ESA for instance, fragmented national regulation should be prevented since it could result in unnecessary costs for vendors – but also for operators – and hinder the entrance of new players into the German and EU market (Kleinhans 2019, 10). Common Criteria-based IT-security certification only evaluates the vendor's software quality and is expensive as it is a "one-time assessment that quickly loses validity" (ibid., 8) with each software update. It also creates market entrance barriers and can only contribute to stronger ESA when being part of a broader strategy.

To begin, the government highlighted its role in meeting the highest security standards for hardware and software by mentioning additional security requirements for operators and vendors (Digital Agenda Committee 2019). In a public expert discussion of the Foreign Affairs Committee, a representative of the Federal Association of the German Industry insisted on uniform European safety standards and clear and transparent guidelines in the 5G roll-out (Foreign Affairs Committee 2019 a). During that discussion, it was only the representative of the German Industry who raised the topic of non-fragmented regulation. Again, this highlights the importance that non-fragmentation (in this case regarding 5G) has for the German and EU economy. Through a governmental response to an FDP motion (2019), the government assured that it was engaged in intensive exchanges with other EU member states on network security issues, particularly for the future 5G network. In another governmental response to an AfD motion (2019), the government cited three EU directives that would provide harmonisation guidelines at EU level and affirmed that they had been converted into national legislation. Part of the TKG would even derive from EU guidelines. Also, the TKG would soon be adapted according to new EU harmonisation guidelines. The BNetzA would work together with ENISA (the European Union Agency for Cybersecurity) and other EU member states to ensure a harmonised application of those guidelines. Newspaper articles concentrated mostly on propositions made by the Union parties. These included again, ensuring high-security standards for the 5G roll-out, uniform security standards at European level and enhancing European capacity to act (Süddeutsche Zeitung 2020 f).

After previously identifying measures taken by the government to ensure IT-security on the operator's level *(variable b)*, I will now look at how Germany regulates the vendor's technology before installing it in its networks. According to a very recent media article, the government had agreed recently on security requirements for the 5G roll-out in Germany. Thereby, under the new IT-security law 2.0, critical core components would have to be certified either by the BSI or by the authority of another EU country. Also, suppliers from all countries would have to provide proof of trustworthiness (Frankfurter Allgemeine 2020). The media further alluded to the strong critique from the parliament's side for the long time taken by the government in drafting the IT-security law 2.0 (Süddeutsche Zeitung 2020). By adjusting the TKG under the new IT-security law 2.0, the government intended that critical core components used in critical infrastructures would only be allowed to be bought from trusted suppliers and manufacturers (Governmental response to AfD motion 2019 a). The definition of what

constitutes security-relevant components (critical core components) would be agreed soon by the BNetzA and the BSI. These components could only be used after an acceptance test at the time of delivery and would be subjected to regular safety tests (Governmental response to FDP motion 2019). Thus, critical core components should only be accepted after certification by the BSI (Digital Agenda Committee 2019). Furthermore, general network components deployed in 5G infrastructures (but also in 2G, 3G and 4G) were also being certified according to the Common Criteria-based IT-security certification (Governmental response to AfD motion 2019).

As previously seen, defining what exactly constitutes trustworthiness, is a difficult task. Evaluating the regulatory system of a company's country of origin seemed to be the first step into defining trust (Kleinhans 2019, 19; Lee-Makiyama 2019). The BMWI went a step further, stating that Germany considered trustworthy suppliers those complying with national security, confidentiality and data protection regulations (Digital Agenda Committee 2019). Proof of trustworthiness would have to be provided as part of the certification process, following the requirements of the BSI (Governmental response to AfD motion 2019 a). The proof would also have to include a declaration by the supplier in the sense of a "no spy clause," accompanied by measures (which would still have to be determined) to ensure the best possible verification of trust.

To conclude, the government's non-fragmentation initiatives regarding 5G (adjustment of the TKG according to EU guidelines and cooperation of BNetzA with EU institutions) have contributed to strengthening ESA. Regarding certification, the German government has approached Common Criteria-based IT-security certification as part of a broader strategy. It has invested in the IT security of its networks by also setting security requirements for operators *(variable b)*. Therefore, the German approach to Common Criteria-based IT-security certification has also contributed to making ESA stronger. Also, the government has been successful in defining critical core components for the 5G network to then minimise risks at such points. Since regulation should be more specific to be effective and focus on "key cornerstones of the critical infrastructure where the regulation might provide added value" (Särekanno 2018), in terms of certification, I can also affirm that the German discourse has contributed to strengthening ESA.

d) *Innovation in EU market*

Lastly, *variable d)* builds again upon *variables a)*, *b)* and *c)*. Regarding 5G it would make no sense to exclusively address the 'relationship to foreign threat actors,' 'IT-security of networks' and 'EU regulation,' without considering the 'innovation in EU market.' To comprehensively determine the development of ESA, it is necessary to as well look, at possibilities of implementing 5G across businesses and industries, and investment options in EU IT-companies. 5G and digital technologies generally represent a business potential for the EU, and since economic competitiveness is a foreign policy tool, *variable d)* can also shape the development of ESA (Ericsson 2020).

To measure the development of ESA regarding *variable d)*, the following aspects are representative of development towards, for instance, stronger ESA: more EU businesses and industries employing 5G technology and more investment in EU IT-companies. Regarding the two mentioned aspects, the opposition was again very critical towards the government, presenting many motions demanding more ambitious action from the government's side. The minister of state assured during a parliamentary debate (2018), that Germany wanted to become a 5G market-leading country and that rural areas would not be forgotten in the roll-out. The opposition, however, criticised the government for a non-existing 5G strategy, poor network coverage in Germany and a not ambitious digitisation strategy. An ambitious strategy would include, for instance, making the energy system smarter, controlling mobility more intelligently or introducing new business models in rural areas.

To start, in terms of network coverage, the government made clear that conforming to a decision by the BNetzA from November 2018, by the end of 2022, 98 % of German households would be supplied with 5G (Governmental response to FDP motion 2019). As previously seen, a strong 4G network serves as the basis for the 5G network expansion since the base stations of the fifth generation will be built initially on the fourth generation networks (Governmental response to AfD motion 2019). Within the mobile communications strategy, the government has planned to supply with reception 99.95 % of households and 97.5 % of German territory until 2024. Within the strategy, the government has also intended to end with the remaining dead zones. Special focus should be put on the rural areas through promoting, for instance, the use of modern technologies in agriculture and forestry by making 5G frequencies available for local networks at very low fees (Governmental response to FDP minor interpellation 2019; Federal Government 2019).

Regarding the employment of 5G in the German industry, the government informed about six 5G applications fields that were being developed in cooperation with research institutions. These included, among other fields of application: the implementation of 5G in the manufacturing industry; improving effectiveness and efficiency in rural health care through 5G technology; the development and testing of 5G applications in the areas of Industry 4.0, agriculture and viticulture, smart city and campus mobility; and research in the future fields of teleoperated, automated and cooperative flying, driving and construction (Governmental response to AfD minor interpellation 2019). In addition, during an interview, the president of the Fraunhofer Society (a German research organization) expressed the need for developing a technology-oriented industrial policy to increase the competitiveness and resilience of the economy in Germany and Europe. He also stressed the importance of data sovereignty. The goal would not be to become self-sufficient but to ensure sovereign freedom of decision in crises. According to the expert, innovation had never been more important than today (Frankfurter Allgemeine 2020 a).

The government laid out the plan for 5G network coverage in German households and demonstrated how industries were already employing 5G technology. However, no reference was made in the German discourse from the government's or opposition's side to businesses utilising 5G technology. For that reason, for the aspect of 'businesses and industries employing 5G technology,' the development of ESA has not been changed.

In terms of investment in EU IT-companies, the opposition again expected more action from the government. During a parliamentary debate (2019), the government was urged to strengthen European and national sovereignty in the field of information and communication technology in the future, with funding measures (or assistance or support measures). The opposition asked what possibilities the government saw in becoming an EU leader in manufacturing hardware and software components of critical infrastructure. Also, what possibilities it saw in establishing production capacities of non-European hardware and software manufacturers in Germany, to ensure a self-sufficient EU supply (Governmental response to an AfD motion 2019).

The government stated that national subsidies for enterprises were not given or only in a very limited extent due to the fully harmonised state aid rules at EU level. However, in the

framework of 'Important Projects of Common European Interest,' adopted by the Commission, subsidies could be granted. Those subsidies would be intended so that support could be given in particular to large projects that could significantly increase European economic growth, employment and competitiveness. The media further reported on the successful merge of T-mobile (the subsidiary group of Deutsche Telekom in the US) and Sprint. The president of Telekom announced that T-mobile wanted to become the number one in the US and that it was good for Germany when a German company managed to take a leading role in a key industry like high-tech, in the US (Süddeutsche Zeitung 2020 d).

The FDP further presented a motion[25] (FDP denied motion 2019) that proposed sending innovation ambassadors to the centres of tech industries like Silicon Valley, so that Germany could catch up with the world leaders in digitisation. According to the motion, diplomacy between states and information technology companies was deemed necessary, as technology companies could be more influential than nation-states in the era of the fourth industrial revolution. Thus, states would have to be attentive to the latest technological developments and engage in dialogue with leading IT companies. Germany, however, would often lack innovations and investors in the field of technological development which could dangerously result in Germany falling behind.

Regarding the aspect of 'investment in IT-companies,' the government presented some measures that could contribute to more investment in German and EU IT-companies. The government also made clear the difficulty of accessing subsidies. The FDP motion could have strengthened the development of ESA. The motion was, nonetheless, denied. The media again highlighted the importance of innovation for the German and EU market. It also expressed the significance of investing in an EU IT-company like Deutsche Telekom. Nevertheless, no allusion was made to German or EU businesses and industries employing 5G. Hence, the development of ESA has remained the same, since the analysis has shown that more could be done to strengthen German and EU sovereignty in IT terms.

The German approach to the four independent variables has for v*ariables a) (relationship to foreign threat actors)* and *d) (innovation in EU market)* not changed the development of ESA and for *variables b) (IT-security of networks) and c) (EU regulation)* strengthened it. The

[25] Although the motion was denied in the end, it is representative of the aspect of investment in IT companies.

security and economic dimension have been addressed more or less equally and conjointly. Albeit most data found corresponded to *variable a)*, and *b)* and *c)* have been addressed more comprehensively, no variable has been completely neglected. Besides, the German discourse has demonstrated that Germany does not unwillingly accept the rules set by others – in terms of how to deal with the security and economic dimension of 5G – and is not subject to their strategic decisions.

As stated in the research design, strong German leadership within the EU is necessary for strengthening the development of ESA. The analysis has demonstrated that Germany has approached the 5G topic correctly – in a way that contributes to strengthening ESA. Germany can now be seen as a role model by other EU countries regarding 5G. Ultimately, results will be seen soon when other EU countries act. Strong ESA depends on the appropriate approach of all EU countries to 5G. Although Germany is only one of them, it has demonstrated leadership within the EU. Germany's approach to 5G has accordingly to experts' opinions, set the right path towards strengthening the process of ESA.

## 5. Conclusion

ESA alludes to more autonomy in the EU's foreign and security policy and depends on the legitimacy of the member states. 5G is an integral determinant of strategic autonomy, having implications for security and economic policy (a foreign policy tool). How well the economic and security implications of 5G are approached, determines the foreign and security policy power of the EU. Because the EU 5G toolbox functions as a recommendation for the member states, I believed that examining the national discourse of a member state would be innovative and contribute more to the scientific debate of 'what constitutes ESA', than studying the EU 5G discourse. I chose the German discourse to study the implications of 5G for ESA because of Germany's strong ability to shape the making of EU foreign and security policy.

The question that this research study has attempted to answer is to what extent has the German discourse on 5G (from 2018 until 2020) shaped the development of the EU's strategic autonomy. The results of the discourse analysis show that the approach to independent *variables a) (relationship to foreign threat actors)* and *d) (innovation in EU market)*, did not provoke any change for the development. Regarding *variables b) (IT-security of networks)* and *c) (EU regulation)*, the development was strengthened. In addition, both categories (*1. security implications of 5G, 2. economic impact of 5G*)[26] were addressed conjointly. No variable or category was given more importance than the rest – consequently contributing to the strengthening of ESA. Besides, although the media has portrayed Germany as depending on China, the stance of the German government of not giving in to the threats of the US has demonstrated that Germany can enforce and modify international rules. In that sense, the German 5G discourse has strengthened the development of ESA. Given these explanations, I can state that the overall process of the development of ESA has been slightly strengthened.

Finally, it is important to clarify that some independent variables might have been mentioned in sources that were not selected for the analysis. In case that those variables were overlooked unintentionally, those exceptions should not have affected the representativeness of the whole analysis. An interesting piece of further research would be to analyse all the national member state discourses on 5G or at least that of those countries leading in the 5G roll-out. Analysing all policy fields that shape ESA could also provide a broader understanding of ESA.

[26] *variables a)* and *b)* belong to *category 1 (security implications of 5G)* and *variables c)* and *d)* to *category 2 (economic impact of 5G)*.

## Bibliography


Benneyworth, I. (2011) *Does the European Union have a strategic culture?*. E-International Relations.

Brustlein, C. (2018) *European Strategic Autonomy: Balancing Ambition and Responsibility*. Paris: Éditoriaux de L'Ifri, Ifri.

Carta, C. and Morin, J. (2014) *EU Foreign Policy through the Lens of Discourse Analysis Making Sense of Diversity*. Globalisation, Europe, Multilateralism Series. Farnham: Ashgate Publishing.

Castro, D. (2018) *Strategic Autonomy in the Digital Age (High-Level Hearing)*. Brussels: European Political Strategy Centre. Available at: https://wayback.archive-it.org/12090/20191129073205/https://ec.europa.eu/epsc/events/strategic-autonomy-digital-age_en. (Accessed: 03.2020).

Deutschland.de (2019) *Ten facts about Germany in Europe*. Available at: https://www.deutschland.de/en/topic/politics/germanys-role-in-the-eu-ten-facts-and-figures. (Accessed: 05.2020).

Ericsson (2020) *What is 5G?*. Available at: https://www.ericsson.com/en/5g/what-is-5g. (Accessed: 02.2020).

European Commission (2019) *EU-China – A strategic outlook*. Available at: https://ec.europa.eu/commission/sites/beta-political/files/communication-eu-china-a-strategic-outlook.pdf. (Accessed: 04.2020).

European Parliament (2019) *5G Deployment: State of Play in Europe, USA and Asia*. Available at: https://www.europarl.europa.eu/RegData/etudes/IDAN/2019/631060/IPOL_IDA(2019)631060_EN.pdf. (Accessed: 04.2020).

EPSC (European Political Strategy Centre) (2018) *Strategic Autonomy in the Digital Age (High-Level Hearing)*. Available at: https://wayback.archive-it.org/12090/20191129073205/https://ec.europa.eu/epsc/events/strategic-autonomy-digital-age_en. (Accessed: 03.2020).

European Union Global Strategy. (2016) *Shared Vision, Common Action: A Stronger Europe – A Global Strategy for the European Union's Foreign And Security Policy*. European Union.

Franke, U. and Varma, T. (2018) *Independence Play: Europe's Pursuit of Strategic Autonomy*. Berlin: European Council on Foreign Relations.

Iannacci, J. (2017) "*Chapter 3: The future 5th generation (5G) of mobile networks: Challenges and opportunities of an impelling scenario"* in *RF-MEMS Technology for High-Performance Passives: The challenge of 5G mobile applications*. Release 4. IOP (Series).

Janning, J. (2015) *What does Germany think about its role in Germany?*. Berlin: European Council on Foreign Relations. Available at:

https://www.ecfr.eu/article/commentary_what_does_germany_think_about_its_role_in_europe5006. Accessed: 05.2020).

Janning, J. and Möller, A. (2016) *Leading from the centre: Germany's role in Europe*. Berlin: European Council on Foreign Relations.

Kello, L. (2018) *Strategic Autonomy in the Digital Age (High-Level Hearing)*. Brussels: European Political Strategy Centre. Available at: https://wayback.archive-it.org/12090/20191129073205/https://ec.europa.eu/epsc/events/strategic-autonomy-digital-age_en. (Accessed: 03.2020).

Kenyon, B. (2018) *Strategic Autonomy in the Digital Age (High-Level Hearing)*. Brussels: European Political Strategy Centre. Available at: https://wayback.archive-it.org/12090/20191129073205/https://ec.europa.eu/epsc/events/strategic-autonomy-digital-age_en. (Accessed: 03.2020).

Kleinhans, J. (2019) *Whom to trust in a 5G world? Policy recommendations for Europe's 5G challenge*. Berlin: The Stiftung Neue Verantwortung (SNV).

Lee-Makiyama, H. (2018) *Strategic Autonomy in the Digital Age (High-Level Hearing)*. Brussels: European Political Strategy Centre. Available at: https://wayback.archive-it.org/12090/20191129073205/https://ec.europa.eu/epsc/events/strategic-autonomy-digital-age_en. (Accessed: 03.2020).

Lee-Makiyama, H. (2019) *5G: What we talk about when we talk about trust – the EU risk assessment process*. Brussels: European Centre for International Political Economy (ECIPE). Available at: https://ecipe.org/blog/5g-eu-risk-assessment-process/. (Accessed: 04.2020).

Lehne, S. (2012) *The big three in EU Foreign Policy.* Washington: Carnegie Endowment for International Peace.

Leonard, M. and Iilves, T. (2019) *Can Europe catch up in the digitalisation and innovation race?*. Berlin: European Council on Foreign Relations. Available at: https://www.ecfr.eu/podcasts/episode/can_europe_catch_up_in_the_digitalisation_and_innovation_race. (Accessed: 03.2020).

Leonard, M., Oertel, J. and Kleinhans, J. (2020) *To Huawei or not to Huawei*. Berlin: European Council on Foreign Relations. Available at: https://www.ecfr.eu/podcasts/episode/to_huawei_or_not_to_huawei. (Accessed: 03.2020).

Lippert, B., von Ondarza, N. and Perthes V. eds. (2019) *European Strategic Autonomy - Actors, Issues, Conflicts Of Interests*. Berlin: Stiftung Wissenschaft und Politik.

Murnane, K. (2019) *Ookla Launched an Interactive Map Showing All the 5G Networks in the World*. Forbes. Available at: https://www.forbes.com/sites/kevinmurnane/2019/05/15/ookla-launches-an-interactive-map-showing-all-the-5g-networks-in-the-world/#23057bd77a08. (Accessed: 04.2020).

NIS Cooperation Group (2020) *Cybersecurity of 5G networks EU Toolbox of risk mitigating measures*. Available at: https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures. (Accessed: 04.2020).

Noble, M., Multimear, J. and Vary, R. (2019) *Who is leading 5G development?*. twoBirds Pattern. Available at: https://www.twobirds.com/~/media/pdfs/who-is-leading-5g-development.pdf?la=en&hash=AB57AC4B01AD1F8BE641A590222DE8BDA1D8B082&hash=AB57AC4B01AD1F8BE641A590222DE8BDA1D8B082. (Accessed: 04.2020).

Särekanno, U. (2018) *Strategic Autonomy in the Digital Age (High-Level Hearing)*. Brussels: European Political Strategy Centre. Available at: https://wayback.archive-it.org/12090/20191129073205/https://ec.europa.eu/epsc/events/strategic-autonomy-digital-age_en. (Accessed: 03.2020).

Schmidt, V. (2008) *Discursive Institutionalism: The Explanatory Power of Ideas and Discourse*. Annual Review of Political Science. ResearchGate.

Smith, M. (2018) *Transatlantic security relations since the European security strategy: what role for the EU in its pursuit of strategic autonomy?*. Journal of European Integration.

Spanish Ministry for Foreign Affairs and Cooperation (2020) *Report on Science, Technology and Innovation Diplomacy*. Available at: http://www.exteriores.gob.es/Portal/es/SalaDePrensa/Multimedia/Documents/Report%20on%20scientific%20technological%20and%20innovation%20diplomacy.pdf. (Accessed: 04.2020).

SWP-Stiftung Wissenschaft und Politik (the German Institute for International and Security Affairs) (2020) Available at: https://www.swp-berlin.org/en/about-swp/. (Accessed: 04.2020).

World Economic Forum (2020) *The Fourth Industrial Revolution*. Available at: https://intelligence.weforum.org/topics/a1Gb0000001RIhBEAW?tab=publications. (Accessed: 04.2020).

Webb, W. (2018) "*Chapter 1: Introduction to 5G The role of the Mobile Network Operator"* in *The 5G Myth: When Vision Decoupled from Reality*. Vol Third edition. Boston: De|G Press.

## Bibliography Analysis

AfD – minor interpellation (16.08.2019) *Surveillance in the 5G mobile network*. Available at: https://www.bundestag.de/presse/hib/654508-654508. Accessed: 04.2020).

AfD – motion (14.02.2019) *Protection of critical 5G infrastructure*. Available at: https://www.bundestag.de/presse/hib/593324-593324. (Accessed: 04.2020).

Das Parlament (18.02.2019) *Dispute over digital policy – Opposition blames government for failures*. Available at: https://www.deepl.com/translator#de/en/Streit%20um%20Digitalpolitik%0AOpposition%20hält%20Regierung%20Versäumnisse%20vor. (Accessed: 04.2020).

Digital Agenda Committee – meeting (13.03.2019) *5G roll-out concerns committee*. Available at: https://www.bundestag.de/presse/hib/628608-628608. (Accessed: 04.2020).

FDP – denied motion (16.10.2019) *Digitisation meets diplomacy - sending innovation ambassadors*. Available at: https://dip21.bundestag.de/dip21/btd/19/141/1914101.pdf. (Accessed: 04.2020).

Federal Government (18.11.2019) *Mobile communications strategy – One billion euros against dead zones*. Available at: https://www.bundesregierung.de/breg-de/themen/digitalisierung/mobilfunkstrategie-1693528. (Accessed: 04.2020).

Foreign Affairs Committee – consultation (11.11.2019) *Experts assess risks of a Huawei participation for 5G differently*. Available at: https://www.bundestag.de/mediathek?videoid=7398783#url=L21lZGlhdGhla292ZXJsYXk/dmlkZW9pZD03Mzk4Nzgz&mod=mediathek. (Accessed: 04.2020).

Foreign Affairs Committee – public expert discussion (13.03.2019 a) *Experts against exclusion of providers for the 5G mobile phone standard*. Available at: https://www.bundestag.de/mediathek?videoid=7332303#url=L21lZGlhdGhla292ZXJsYXk/dmlkZW9pZD03MzMyMzAz&mod=mediathek. (Accessed: 04.2020).

Frankfurter Allgemeine (13.05.2020) *IT Security Act – Huawei must fear*. Available at: https://www.faz.net/aktuell/wirtschaft/wer-baut-das-5g-netz-in-deutschland-auf-huawei-muss-bangen-16766713.html. (Accessed: 04.2020).

Frankfurter Allgemeine (05.05.2020 a) *Sovereignty is not a gift*. Available at: https://www.faz.net/aktuell/wirtschaft/digitec/fraunhofer-chef-neugebauer-so-bleibt-deutschland-dran-16744072.html. (Accessed: 04.2020).

Governmental response to AfD minor interpellation (2019) *Six 5G application fields promoted*. Available at: https://www.bundestag.de/presse/hib/676140-676140. (Accessed: 04.2020).

Governmental response to AfD motion (24.04.2019) *Ensuring the technical integrity of the future 5G mobile infrastructure*. Available at: https://dip21.bundestag.de/dip21/btd/19/096/1909621.pdf. (Accessed: 04.2020).

Governmental response to AfD motion (14.05.2019 a) *Security in the roll-out of 5G networks*. Available at: https://www.bundestag.de/presse/hib/642564-642564. (Accessed: 04.2020).

Governmental response to FDP minor interpellation (12.06.2019) *Nationwide 5G roll-out with the help of a state mobile infrastructure company*. Available at: https://dip21.bundestag.de/dip21/btd/19/108/1910892.pdf. (Accessed: 04.2020).

Governmental response to FDP motion (14.01.2020) *Deployment of technology of Chinese companies in projects and infrastructure of federal ministries and federal authorities*. Available at: https://dip21.bundestag.de/dip21/btd/19/164/1916471.pdf. (Accessed: 04.2020).

Governmental response to FDP motion (08.04.2019) *Use of Huawei technology in German mobile networks*. Available at: https://dip21.bundestag.de/dip21/btd/19/091/1909194.pdf. (Accessed: 04.2020).

Parliamentary debate (28.11.2018) *Controversy over the government's digital strategy*. Available at: https://www.bundestag.de/dokumente/textarchiv/2018/kw48-de-aktuelle-stunde-digitalgipfel-2018-580808. (Accessed: 04.2020).

Parliamentary debate (20.12.2019) *Cybersecurity in the context of 5G technology*. Available at: https://www.bundestag.de/dokumente/textarchiv/2019/kw51-de-5g-technologie-673100. (Accessed: 04.2020).

Süddeutsche Zeitung (09.05.2020) *Debate on draft of IT security law*. Available at: https://www.sueddeutsche.de/wirtschaft/telekommunikation-debatte-ueber-entwurf-von-it-sicherheitsgesetz-dpa.urn-newsml-dpa-com-20090101-200509-99-996196. (Accessed: 04.2020).

Süddeutsche Zeitung (17.02.2020 a) *Doubts about accusations by the US against Huawei*. Available at: https://www.sueddeutsche.de/wirtschaft/huawei-5g-usa-spionage-1.4801181. (Accessed: 04.2020).

Süddeutsche Zeitung (24.02.2020 b) *Focus on Europe in the US fight against Huawei*. Available at: https://www.sueddeutsche.de/wirtschaft/telekommunikation-im-us-kampf-gegen-huawei-steht-europa-im-fokus-dpa.urn-newsml-dpa-com-20090101-200224-99-48958. (Accessed: 04.2020).

Süddeutsche Zeitung (03.05.2020 c) *5G is spreading in Brandenburg*. Available at: https://www.sueddeutsche.de/wirtschaft/telekommunikation-bonn-5g-mobilfunk-breitet-sich-in-brandenburg-aus-dpa.urn-newsml-dpa-com-20090101-200503-99-918367. (Accessed: 04.2020).

Süddeutsche Zeitung (06.05.2020 d) *How Telekom plans to conquer the US market*. Available at: https://www.sueddeutsche.de/wirtschaft/telekommunikation-wie-die-telekom-den-us-markt-erobern-will-dpa.urn-newsml-dpa-com-20090101-200506-99-952927. (Accessed: 04.2020).

Süddeutsche Zeitung (21.02.2020 e) *Huawei gets 5G contracts from 47 European providers*. Available at: https://www.sueddeutsche.de/wirtschaft/telekommunikation-huawei-erhaelt-5g-vertraege-bei-47-europaeischen-providern-dpa.urn-newsml-dpa-com-20090101-200221-99-09877. (Accessed: 04.2020).

Süddeutsche Zeitung (11.02.2020 f) *Union parties do not want to exclude Huawei from 5G network*. Available at: https://www.sueddeutsche.de/wirtschaft/telekommunikation-unionsfraktion-will-bei-5g-netz-keinen-ausschluss-von-huawei-dpa.urn-newsml-dpa-com-20090101-200211-99-866039. (Accessed: 04.2020).

Süddeutsche Zeitung (29.01.2020 g) *Why Huawei divides politics so much*. Available at: https://www.sueddeutsche.de/wirtschaft/huawei-5g-netzausbau-deutschland-1.4776270. (Accessed: 04.2020).

## Declaration of authorship

I hereby declare that this thesis titled 'Consequences of the German 5G discourse for the development of the EU's strategic autonomy' is my unaided work. All direct or indirect sources used are acknowledged as references. This research study was not previously presented to another examination board and has not been published.

Madrid, the 3rd of July 2020.

Marta Isabel Vorwald de Vega