BIGS

BRANDENBURGISCHES INSTITUT
für GESELLSCHAFT und SICHERHEIT

THE HIDDEN COST OF UNTRUSTED VENDORS IN 5G NETWORKS

STATE OF DISCUSSION AND ESTIMATIONS

FOR GERMANY

Johannes Rieckmann, Tim Stuchtey

Country Study

commissioned by

U.S. Department of State

Brandenburg Institute for Society and Security gGmbH

December 2020

Contact and further information:

Brandenburg Institute for Society and Security gGmbH (BIGS)
Executive Director: Dr. Tim H. Stuchtey
Dianastrasse 46
14482 Potsdam

Phone: +49-331-704406-0
Fax: +49-331-704406-19

E-mail: direktor@bigs-potsdam.org
www.bigs-potsdam.org

This study was funded by a grant from the United States Department of State. The opinions, findings and conclusions stated herein are those of the authors and do not necessarily reflect those of the United States Department of State.

Inhalt

Executive Summary 4

Introduction 6

Current Situation and State of Debate (as of Oct 31, 2020) 7

4G (LTE) 7

5G 8

5G Telecommunication Providers 9

Timeline for Building 5G Network 11

Government 11

Parliament 15

Alleged Costs of Market Intervention by Banning Untrusted Vendors 16

Obvious Costs of Malicious Vendors 17

Hidden Costs of Untrusted Vendors 17

Test Centre 17

Regulatory Costs 18

Costs of Data Breaches 19

Quantification of magnitude of potential losses 20

Shift of Demand 21

Redundant infrastructure 25

Costs of Rip and Replace 25

Summary 27

Sources 29

Executive Summary

Today the 4G mobile network in Germany is dominated by technology from untrusted vendors. A total amount of EUR 5.08 billion was generated by the LTE-frequency (4G) auction in 2015, with Vodafone, Deutsche Telekom and Telefónica Deutschland winning the tender. The auction for 5G frequencies raised EUR 6.55 billion, with Drillisch Netz (1&1) as an additional bidder. All, or at least the majority of German telecommunications companies, seem to be currently planning to exclude vendors regarded as untrusted from their 5G core network, having previously planned to use untrusted technology. However, at least the two big players (Deutsche Telekom AG and Vodafone GmbH) still plan to use Huawei for their RAN network.

In a paper from 2016, the German government outlined its 5G strategy, the main goal of which is for Germany to become the leading market for 5G applications. The IT Security Act 2.0, as of December 2020 still in the draft bill stage, will be decisive for the rollout of the 5G infrastructure. A crucial detail will be the consensus building in the interministerial assessment of vendors and components. Adoption of the law is expected by spring 2021.

Based on somewhat disputable assumptions, a study from Oxford Economics estimates a negative economic effect as a result of restricting competition in the provision of 5G network equipment in Germany, amounting to, put into perspective by us, a EUR 3.18 increase in average annual investment costs for 5G infrastructure per number of current mobile phone contracts, and EUR 83.11 per capita loss in GDP in 2035 due to a delayed 5G rollout.

We must contrast this with some of the quantifiable costs of not excluding untrusted vendors. The costs of an unlikely blackout scenario of three days due to an all-out international cyber conflict would amount to about EUR 12.94 billion. A more realistic scenario might be a more furtive pouring of sand into the gearbox, over a longer period of time.

A bundle of costly measures is necessary to control and to protect against this more realistic scenario:

- A test centre to control for malicious bugs in the frequent software updates of a 5G network would cost up to EUR 60 million per year.
- Regulatory costs are harder to meaningfully sum up and allot, but exceed the former amount.
- The costs of data breaches through untrusted 5G networks in Germany could hit EUR 18 billion by 2024.
- We estimate that more than half of the market with business customers, or EUR 4.6 billion, will have a tendency to shift toward MNOs with only trusted technology in their 5G networks.
- The presence of untrusted vendors in a future German 5G communication network might force the government to invest in a redundant infrastructure that is fully controlled by the German state, coming with costs in the hundreds of millions.

Deutsche Telekom estimates the cost of a speedy rip and replace of equipment, again put into perspective by us, at around EUR 65 per mobile phone customer. Compared with the quote

from British Telecommunications, which has a similar dependence on Huawei as Deutsche Telekom, that number seems quite high to us. We also believe that a rip and replace at a later point in time, after a considerable rollout of 5G network equipment including that of untrusted vendors, would most likely come at a higher price.

Overall, we have been able to show for Germany, theoretically in the policy paper and empirically in this country study, that the total societal costs, i.e. including externalities, are higher over time than the potential savings that arise for mobile network operators when they use non-trusted network technology to deploy 5G. This form of market failure must be cured through adequate regulation in order to realise the growth-enhancing potential of 5G technology in the coming decade. The opportunity for this exists with the current IT Security Act 2.0, if implemented consistently. However, if the high proportion of untrusted technology remains, as we are seeing in Germany with 4G networks, considerable costs for protective measures in the IT sector will be incurred by the German economy and security-relevant government institutions.

Introduction

This country study is a complement to our policy paper on the hidden costs of untrusted vendors in 5G networks. Following a brief overview regarding frequencies and mobile network operators in Germany, including their market position and stance regarding procurement and usage of network equipment, we take a look at the current timeline of 5G rollout in Germany. We provide the reader with a concise overview regarding the upcoming regulation, which is in the form of the draft of the Second IT Security Act, and its likely impact, if implemented well. After briefly assessing a purely competitive analysis by a British institute in terms of its underlying assumptions, and by putting their core results into perspective, we turn, for comprehensiveness, to the obvious costs that could arise, for example, from sabotage and attacks on the communications network in the context of geopolitical tensions. By contrast, hidden costs, which can be quantified for Germany in some of the areas discussed in the policy paper, are much more likely to occur and at the same time are more challenging to quantify.

Current Situation and State of Debate (as of Oct 31, 2020)

4G (LTE)

The first 4G (LTE) auction was held between April and May 2010. The competitors Deutsche Telekom, Vodafon, Telefónica and E-Plus acquired a volume of 370-Mhz frequencies in the 800-Mhz, 1800-Mhz, 2000-Mhz and 2600-Mhz ranges. The auctioned frequency blocks were distributed among the licensed mobile network operators (MNO) as follows:

- **Vodafone D2:** A total of 12 frequency blocks for EUR 1,422,503,000,
- **Telefónica O2 Germany**: In total, 11 frequency blocks for EUR 1,378,605,000,
- **Deutsche Telekom:** A total of 10 frequency blocks for EUR 1,299,893,000 and
- **E-Plus (Erste MVV Mobilfunk Vermögensverwaltungsgesellschaft)**: A total of 8 frequency blocks for EUR 283,645,000.[1]

In 2013, the acquisition of E-Plus by the holding company of O2, the Spanish provider Telefónica, led to a consolidation on the market. Telefónica paid five billion euros and 17.6 percent in own shares.[2] As a result, the numbers three and four on the German market merged to form the new market leader with over 40 million cell phone customers, ahead of Deutsche Telekom and Vodafone.[3] In 2020 market shares are as follows:

- **Vodafone:** 50.7 million customers, EUR 5 billion revenue
- **Deutsche Telekom:** 46.2 million customers, EUR 8.2 billion revenue
- **Telefónica:** 43.6 million customers, EUR 6.6 billion revenue
- **1&1 Drillisch:** 10.2 million customers, EUR 0.75 billion revenue.[4] [5]

From May to June 2015, additional frequencies at the volume of 270-Mhz from the 700-Mhz (digital dividend II), 900-Mhz, 1500-Mhz and 1800-Mhz ranges were auctioned. The frequencies in the 900-MHz and 1800-MHz ranges formed the basis for the development of today's mobile communications networks, in particular for nationwide mobile voice communications.

The auctioned frequency blocks were distributed among the licensed MNOs as follows:

- **Vodafone:** A total of 13 frequency blocks for EUR 2,090,842,000,
- **Telefónica Deutschland**: In total 6 frequency blocks for EUR 1,198,238,000 and
- **Deutsche Telekom:** A total of 12 frequency blocks for EUR 1,792,156,000.[6]

A total amount of EUR 5.08 billion was generated by the LTE-frequency auction in 2015 (see Table 1).

[1] Bundesnetzagentur (2020a).
[2] Spiegel (2013).
[3] Ibid.
[4] Kuhn (2020a).
[5] 1&1 does not operate its own 4G network. The company is currently only a reseller. The customer base is mentioned here. A s with the acquisition of the 5G frequencies, a separate network is to be established.
[6] Bundesnetzagentur (2020b).

Table 1: 4G (LTE) Auction 2015/2016[7] (mobile broad band 700-MHz, 900-MHz, 1800-MHz)

Company	Frequency Volume		Hammer Price
Telefónica Deutschland GmbH & Co. OHG	700 MHz: 900 MHz: 1800 MHz:	2 x 10 MHz 2 x 10 MHz 2 x 10 MHz	1,198,238,000 €
Telekom Deutschland GmbH	700 MHz: 900 MHz: 1800 MHz: 1500 MHz:	2 x 10 MHz 2 x 15 MHz 2 x 15 MHz 20 MHz	1,792,156,000 €
Vodafone GmbH	700 MHz: 900 MHz: 1800 MHz: 1500 MHz:	2 x 10 MHz 2 x 10 MHz 2 x 25 MHz 20 MHz	2,090,842,000 €
Total	**270 MHz**		**5,081,236,000 €**

With relatively few radio stations, the MNOs were able to launch fast internet even in regions that were previously poorly served. The 2015 LTE auction was also subject to conditions for the MNOs. The aim of the Federal Network Agency was to use these frequencies to ensure that the population was provided with broadband internet almost nationwide – as is already the case with mobile voice telephony. The frequency usage rights therefore include a supply obligation for 98 per cent of the population.[8]

5G

Frequencies between 2-GHz and 3.6-GHz were auctioned from March 19 until June 12 2019. The auctioned frequency blocks within the volume 420-Mhz were distributed among the licensed MNOs as follows (see Table 2).

Table 2: 5G Auction 2019

Company	Frequency Volume	Hammer Price
Telefónica Deutschland GmbH & Co. OHG	9 frequency blocks	1,424,832,000 €
Telekom Deutschland GmbH	13 frequency blocks	2,174,943,000 €
Vodafone GmbH	12 frequency blocks	1,879,689,000 €
Drillisch Netz (1&1)	7 frequency blocks	1,070,187,000 €[9]
Total	**41 frequency blocks**	**6,549,651,000 €**

A total amount of EUR 6.55 billion was generated by the 5G frequency auction in 2019 (see Table 3 and Table 4). For the first time, a new MNO (Drillisch Netz AG, also referred to as 1&1) was among the three major established MNOs at the 5G auction.

[7] Ibid.

[8] Ibid.

[9] Bundesnetzagentur (2019).

Table 3: 5G Auction 2019[10]

	Drillisch Netz AG	Telefónica Germany GmbH & Co. OHG	Telekom Deutschland GmbH	Vodafone GmbH
2 GHz	2 x 10 MHz	2 x 10 MHz	2 x 20 MHz	2 x 20 MHz
3.6 GHz	50 MHz	70 MHz	90 MHz	90 MHz
Total	70 MHz	90 MHz	130 MHz	130 MHz

5G Telecommunication Providers

Deutsche Telekom purchased by auction 4 frequency blocks in the 2 GHz band as well as 9 lots in the 3.6 GHz band worth EUR 2.17 billion[11] in the 5G spectrum auction in 2019. Their 5G rollout activities have already started, with the goal of connecting the 20 largest cities in Germany to the network. Deutsche Telekom is relying heavily on network technology from Huawei in their 4G network. They planned to use Huawei technology even more for 5G. However, they now state in their company blog that they are committed to a multi-vendor strategy for their suppliers. 30 per cent of the technology originates from American manufacturers, while 25 per cent originates from European and Chinese companies as well as smaller Asian or local suppliers.[12] For their 5G expansion they are utilising both Ericsson as well as Huawei technology for their existing antenna network.[13] Furthermore, Telekom Deutschland states that their sales with Huawei have been declining for the past three years and that they do not allow Chinese technology in their mobile communications core network.[14] In July 2020, following the successful modernisation of existing 2G/3G/4G networks, Telekom Deutschland commissioned Ericsson to deploy the 5G Radio Access Network (RAN) over the next few years.[15]

In June 2019, **Vodafone Germany** acquired 2x20 MHz of the expiring 2.1 GHz spectrum and 1x90 MHz of 3.6 GHz spectrum in the recent auction for EUR 1.88 billion.[16] Vodafone relies on Huawei equipment, yet it recently stated that it intends to remove Huawei equipment from the sensitive core parts of its mobile networks over the next 5 years for EUR 200 million.[17] However, Vodafone warned the German government against completely excluding the Chinese network supplier. According to Vodafone, excluding Huawei from the German 5G network would delay the rollout by up to five years and cause significantly higher costs.[18] Despite these circumstances, the roll out of the 5G network is proceeding more rapidly than originally announced. According to Vodafone, the ten million people planned for the end of 2020 are already covered by the faster 5G network.[19] By the end of 2020, even more than 15

[10] Bundesnetzagentur (2020c).
[11] Deutsche Telekom (2019), p. 22.
[12] Broszio (2020).
[13] Ibid.
[14] Koch, Scheuer, Iwersen (2020).
[15] Ericson (2020).
[16] Vodafone (2020), p. 256.
[17] Sweney (2020).
[18] Sawall (2020).
[19] Heuzeroth (2020a).

million people in Germany are to be supplied with 5G. Vodafone has revised its target number for the end of 2021 upwards to 30 million people.[20]

Telefónica Deutschland, part of the Spanish Telefónica Group, has acquired 90 MHz of valuable spectrum and invested EUR 1.42 billion in new licenses.[21] Telefónica stated that they have planned their 5G expansion with Nokia as well as Huawei equipment.[22] Currently, about half of the Telefónica mobile network is equipped with Huawei technology and the other half is supplied by Nokia.[23] However, Telefónica recently stated that they will abandon Huawei from the core network, but still want to use Chinese technology in the Radio Access Network.[24] According to press releases, Telefónica and 1&1 Drillisch have disputes on pricing, as 1&1 Drillisch is currently using Telefónica's network system.[25] This dispute has potential negative consequences for their cooperation in the 5G network expansion.[26]

1&1 Drillisch, part of the German group United Internet, remains today a large telecommunication service provider without a mobile network, completely relying on roaming access from MNOs. With 5G, they want to become an MNO.[27] 1&1 thus wants to establish itself as the fourth competitor in Germany. This is also helped by an agreement between 1&1 and the Federal Ministry of Transport and Digital Infrastructure, as well as the Federal Ministry of Finance, to fill "white spots" by building hundreds of mobile phone sites.[28] While the other three MNOs have already reached millions of customers with 5G, the newcomer has fallen behind. 1&1 Drillisch has abandoned the plan to launch its network for its first customers by 2021. The reason for the delay is the stalled negotiations with the incumbent providers on the shared use of radio networks (national roaming).[29] No contracts will be awarded to a network provider until an agreement has been reached. While originally 1&1 was thought to plan with ZTE, the company now reportedly plans the 5G rollout as Open-RAN, most likely without Huawei, similar to Rakuten in Japan.[30] The newcomer will therefore not be operational until 2022 at the earliest. For the core network, though, the decision-making process seems not to be over yet, with the use of ZTE components seeming likely.[31]

Accordingly, all or at least the majority of German telecommunications companies will most likely not use Huawei components in their 5G core network (see Table 4 below).[32]

[20] Ibid.
[21] Telefónica (2019), p. 2.
[22] Reuters (2019).
[23] Koch & Scheuer (2020a).
[24] Ibid.
[25] Handelsblatt (2020).
[26] n-tv (2020).
[27] 1&1 Drillisch (2019), p. 4.
[28] Ibid.
[29] Kuhn (2020a).
[30] Manager Magazin (2020).
[31] Weidner (2020).
[32] Heuzeroth (2020b).

Table 4: Overview of Component Usage

	Deutsche Telekom AG	Vodafone GmbH	Telefónica Deutschland Holding AG	1&1 Drillisch AG (New MNO)
Core Network 4G	Use of Huawei components	Use of Huawei components	Use of Huawei components	/
Core Network 5G	Exclusion of Huawei	Exclusion of Huawei	Exclusion of Huawei	No decision yet
RAN 4G	Use of Huawei components	Use of Huawei components	Use of Huawei components	/
RAN 5G	No ban of Huawei components	No ban of Huawei components	Open-RAN (no ban of Huawei components)	Open-RAN (likely without Huawei/ ZTE)

Based on our own research and following background discussions with a technical expert familiar with the subject, about half of both Deutsche Telekom's and Vodafone's 4G RAN are equipped with Huawei network technology (based on the number of customers serviced).[33] Strand Consult[34] reports even higher proportions; 65% for Deutsche Telekom and 55% for Vodafone (and 50% for Telefónica). According to a background discussion with a technical expert, Huawei technology in Vodafone's 4G RAN is mainly deployed in all Eastern and Northern German states. In the other federal states, Vodafone relies mainly on Ericsson in their 4G RAN.

Timeline for Building 5G Network

Government

In a paper from 2016, the German government outlined its 5G strategy. The main goal is to become the **leading market for 5G applications**.[35] That means enabling the German industry to introduce market innovations such as autonomous driving, and the use of 5G technology in production processes. The goal is to start the 5G rollout in 2020 and to become 5G-connected by 2025.

Following the auction of the 5G licenses, the second law to increase the security of information technology systems (Second IT Security Act – **IT-SiG 2.0**), as of December 2020 still in the draft bill stage, will be decisive for the rollout of the 5G infrastructure. The German government wants to introduce a double test procedure for Chinese components.[36] The Federal Office for Information Security (Bundesamt für IT-Sicherheit – **BSI**) will check the

[33] Koch, Scheuer, Iwersen (2020).
[34] Strand Consult (2020), p.19.
[35] BMVI (2017), p. 3.
[36] Stempfle (2020).

technical components, the Federal Office for Intelligence (Bundesnachrichtendienst – **BND**) will add their assessment, and the Foreign Office (Auswärtiges Amt) together with the Ministry of Economics (**BMWi**) and the Ministry of the Interior (**BMI**) will make the final decision. With regard to 5G, both telecommunications and critical infrastructure operators are to report **critical IT components** to public authorities (in particular to the BSI).[37] **Vendors of critical components** must sign a guarantee declaration and **untrusted vendors** can be banned if they do not pass the test for trustworthiness.[38] [39]

In this respect, the focus is mainly on article 1, §9b – prohibition of the use of critical components. Furthermore, section 2 states, "*Critical components according to section 1 may only be utilized if the manufacturer has issued a declaration of confidence to the operator of the critical infrastructure (guarantee declaration). This declaration covers the entire supply chain of the manufacturer. (..) The guarantee statement must state, among other things, whether and how the manufacturer can adequately ensure that the critical component does not have any technical properties that could have an abusive influence on the security, integrity, availability or functionality of the critical infrastructure, in particular for the purpose of sabotage, espionage or terrorism.*"[40]

Ultimately, section 5 states that a manufacturer of a critical component is not trustworthy if

1. *"he has violated the obligations and assurances entered into the guarantee declaration,*
2. *its facts stated in the guarantee statement are untrue,*
3. *he does not adequately support security checks and penetration analyses to the required extent on his product and in the production environment,*
4. *he fails to immediately report known or disclosed vulnerabilities or manipulations to the critical infrastructure manager and does not remedy them, or*
5. *the critical component has or has had technical properties that are or were capable of improperly affecting the security, integrity, availability or operability of the critical infrastructure."*[41]

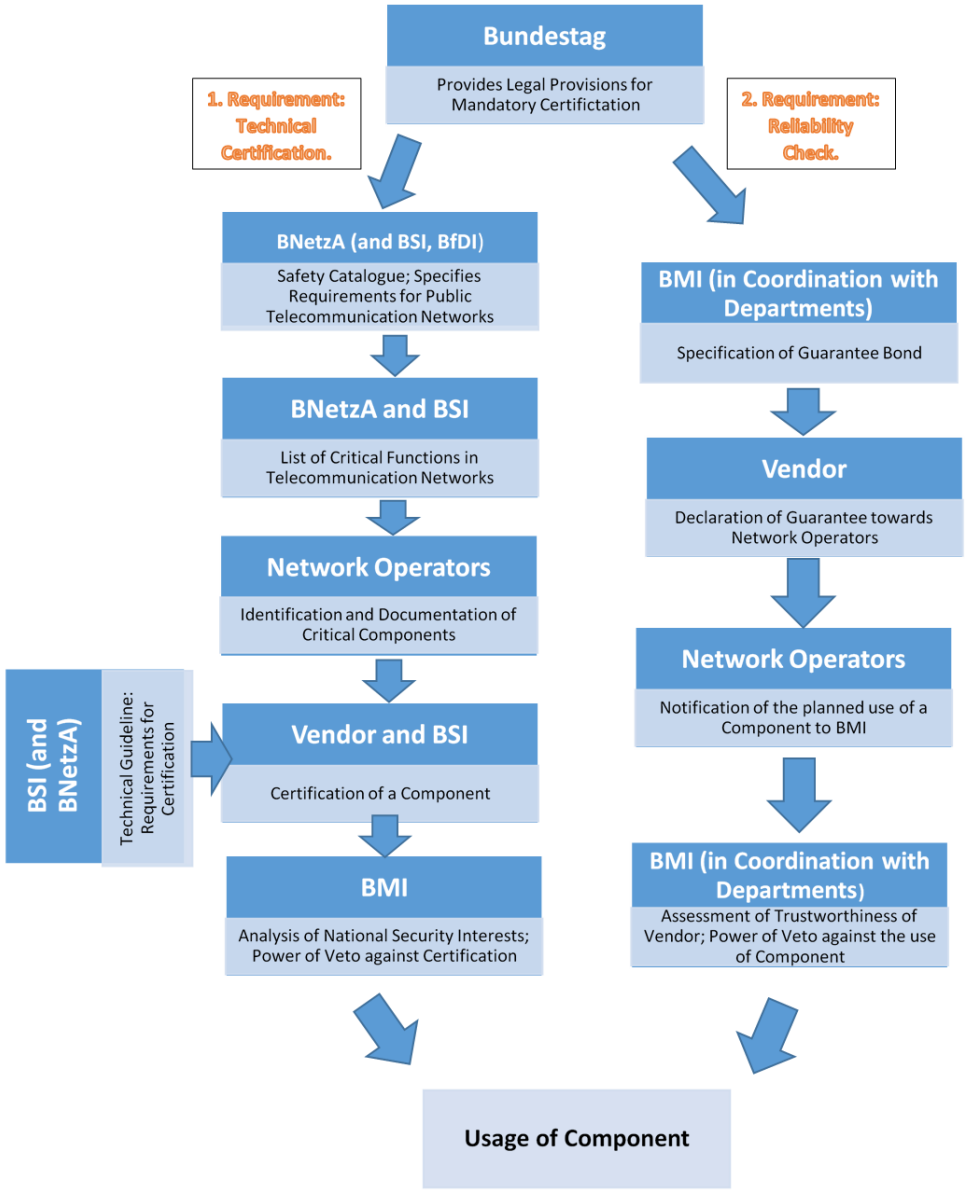
All in all, the draft of the IT-Security Act 2.0 is interpreted as making it particularly hard for Chinese vendors to participate in the building of 5G networks in Germany. While the draft uses phrases indicating that the Ministry of Interior is to seek agreement with other ministries concerned when prohibiting the use of any of the manufacturers' critical components, when looking at the departments involved, it appears indeed likely that the usage of mentioned components (see illustration 1 for a visualisation of the process) will only be accepted if no ministry objects. This assessment seems to be shared by experts like Herpig and Kleinhans from Stiftung Neue Verantwortung SNV, who point out[42] that the scope of the planned law goes far beyond technical IT and cybersecurity, which is made clear, among other things, by

[37] BMI (2020), Draft Law p. 9, 23, 27.
[38] Heidrich & Kenji Kipker (2020).
[39] BMI (2020), Draft Law p. 20f.
[40] Ibid.
[41] Ibid.
[42] SNV (2020), p. 9.

the fact that the Federal Ministry of the Interior is mentioned in this context and not the subordinate Federal Office for Information Security BSI. Herpig and Kleinhans regard this perspective as reinforced by the fact that both the contents of the warranty declaration and the risk assessment of the manufacturer of the critical component have to be carried out in agreement with the respective ministries concerned. They judge the interministerial assessment, including security policy concerns, as being essential.

The seeking of agreements is planned to take place in an ongoing and regular exchange in the form of an interministerial *jour fixe* between the houses concerned (Ministry of Interior, Ministry of Economics, as well as Foreign Office and Federal Chancellery, at head of unit level).

Illustration 1: IT-Security Act 2.0 Procedure for Critical Component Check



Source: DSI 2020/Own Diagram.

Note: Bundestag = German Federal Parliament; BNetzA (Bundesnetzagentur) = Federal Network Agency; BSI (Bundesamt für Sicherheit in der Informationstechnik) = Federal Office for Information Security; BfDI (Bundesbeauftragter für den Datenschutz und die Informationsfreiheit) = Federal Commissioner for Data Protection and Freedom of Information; BMI (Bundesministerium des Inneren) = Federal Ministry of the Interior, Building and Community.

Parliament

In February 2020, the **CDU/CSU** party group in the Bundestag adopted a position paper on the roll out of the 5G network. According to the joint position, the CDU/CSU members of parliament advocated maintaining high security standards when expanding the network without excluding specific network vendors.[43] This position corresponds to the Federal Government's, although not everyone in the party shares this approach.[44]

In contrast, the **SPD** faction, coalition partner in the government, reached an understanding as early as the end of 2019 that, if non-state-controlled interference, manipulation or espionage cannot be ruled out, untrustworthy manufacturers will be excluded from expanding and operating 5G networks.[45]

The two positions of the coalition partner were synthesised in the **Federal Government**'s agreement as follows: No vendor will be excluded per se, but critical infrastructures will in the future not only be subject to a mere (technical) security-related review, but also to a trustworthy/reliability check of the vendor (see Illustration 1).[46]

The **AfD** has positioned itself and pleads for the exclusion of Huawei and other companies that might compromise the competitiveness of Germany as a business location as well as the technological sovereignty of Germany.[47]

The **Greens** in the Bundestag have warned of a participation of the Chinese technology company Huawei in the build-up of the German 5G network. They claim that the use of Huawei components involves risks that are extremely difficult to foresee. The Greens intend to set up a catalog that defines conditions for the digital infrastructure. This should ensure security and sustainability, but also democracy, human rights and the rule of law. Companies should only be involved in the IT infrastructure if they comply with these conditions.[48]

In a declaration of the **FDP** party group in the fall of 2019, the party demands that "state authorities do not acquire products from Chinese companies whose products are the core of the system of boundless mass surveillance of the people of China. In the case of security-critical infrastructure, such as 5G, Europe should be prepared to forego the use of Chinese technology...".[49]

In a position paper of the Working Group III Economics and Finance of the parliamentary group **DIE LINKE** in the Bundestag of August 2019, the working group stated that: "if a politically motivated exclusion of the Chinese vendor Huawei were to occur due to the latent dispute between the United States and China, this would further delay the roll-out of the 5G network."[50] However, there does not seem to be a unanimous position. Some members

[43] Heise (2020).
[44] Kamp (2020).
[45] SPD-Fraktion im Bundestag (2019).
[46] Hegemann (2020).
[47] Deutscher Bundestag (2019).
[48] Neuerer (2019).
[49] FDP-Fraktion im Bundestag (2019).
[50] DIE LINKE-Fraktion im Bundestag (2019a).

perceive the 5G issue concerning Huawei as purely American paternalism and pursuit of their own economic interests.[51]

Alleged Costs of Market Intervention by Banning Untrusted Vendors

Oxford Economics published an economic impact study commissioned by Huawei in June 2020 on their estimations of detrimental effects arising from a restriction of competition in 5G network equipment in the European market.[52] They base their estimations on assumed differences in network equipment prices, speed of rollout, and economic growth.

For Germany, Oxford Economics estimates an impact of restricting competition by excluding Huawei on average annual investment costs for 5G infrastructure, in what they call the central cost scenario, as high as EUR 479 million (with a range of EUR 232 million for the low to EUR 726 million for the high cost scenario).[53] With 150.7 million mobile phone contracts in Germany,[54] this would translate into an additional cost per contract of around EUR 3.18 (see Table 5). They estimate a permanent loss in GDP based on this delay amounting to EUR 6.9 billion (range 2.3 to 15.3) by the year 2035. To put that into perspective: based on the 2019 population of 83.02 million people, the loss of GDP would amount to EUR 83.11 per capita.

Table 5: Impact of restricting competition put into perspective

Increase in average annual investment costs for 5G infrastructure over the next decade	**3.18€** per mobile phone contract
Estimated permanent loss in GDP due to delay in 5G rollout in 2035	**83.11€** per capita

Source: Own calculations, based on Oxford Economics (2020), Kuhn (2020b), and Statistisches Bundesamt (2020b).

We consider several of the assumptions underlying Oxford Economics estimations unrealistic and believe the results are overstated. We summarise our criticism in the appendix, but the most relevant points are perhaps the following ones:

1. Economic theory (e.g. literature on bilateral bargaining in oligopsony) and real world examples (e.g. Airbus and Boeing[55]) show that even in a duopoly, competition can be fierce.
2. There are already and will be more new market entrants (e.g. Samsung).
3. OpenRAN will soon make MNOs less dependent on system vendors such as Ericsson and Huawei which will have a major impact on prices.

[51] Ibid (2019b) & DIE LINKE-Fraktion im Bundestag (2020).

[52] Oxford Economics (2020), p.40. They furthermore assess the absolute number of customers suffering from a delay of access to 5G by the year 2023 technology as amounting to 11.9 million people (range 6.3 to 16.7).

[53] For the European Union, they value the increase in average annual investment costs in the intermediate of their three scenarios of 19 percent, translating into EUR 2.4 billion. The absolute number of people being affected by a delayed rollout of the 5G network rooted in exclusion of Huawei from competing in the market is assessed to be, in total, 46.9 million. For 2035 – 15 years from now – Oxford Economics estimate a reduction of annual GDP of EUR 32.4 billion (in 2020 prices).

[54] Kuhn (2020b): adding up the 2019 number of mobile contracts of Deutsche Telekom (46.2 million), 1&1 Drillisch (10.2 million), Telefónica (43.6 million) and Vodafone (50.7 million).

[55] Baldwin & Krugman (1988).

4. The real push for productivity from 5G will not materialise until critical applications are available.

Obvious Costs of Malicious Vendors

As demonstrated in Chapter 5, the most obvious costs of untrusted vendors occur when the network is being used to sabotage an entire economy. For this "Armagedon Scenario", the effect of such an act of sabotage on the German gross domestic product (GDP) will probably at any rate be comparable to that of a few days of a general strike or a full lock down during a pandemic. Based upon working days' elasticity of demand, and calculations conducted by the German Bundesbank,[56] each lost working day corresponds to 0.125 percentage points[57] of GDP. Taking the German 2019 GDP of EUR 3449 billion[58] as a basis, an interruption of working life of three days would translate into an absolute amount of about EUR 12.94 billion, without taking into consideration cascading and other second-round effects (e.g. the costs of a then-unavoidable and precipitous post-incident reactive rip and replace). Most probably, in fact, getting the communication network fully fixed within three days would be a naive pipe dream. A six-day shutdown would already cost EUR 25.88 billion, equaling almost 0.75% of the German GDP.

While the blackout scenario is unlikely (disregarding maybe a one-time shot in an international confrontation), a more realistic one might be a more furtive pouring of sand into the gearbox, over a longer time, thus thwarting the German industry communication infrastructure and the economy. This kind of more gradual obstruction could either target the economy as a whole, or be aimed at sectors of strategic importance, e.g. the German automobile sector, with its industry 4.0 production.

Hidden Costs of Untrusted Vendors

Test Centre

As described in chapter 6.2, among the hidden costs of including untrusted vendors in a German 5G communication network will be the additional cost to control if the goodwill was not abused. These control costs include test centres and testbeds in dedicated research and development laboratories to analyse the untrusted hard- and software. For this purpose, a **German National Telecoms Laboratory (GNTL)** would be required – at national level mainly due to the presence of an untrusted vendor controlled by the government of another nation, being a geopolitical systemic rival of the European Union and her partner countries and regions.

As no such institution currently exists, a workaround to assess a ballpark figure of the expected costs of such an institution is to look at existing German institutions comparable to the prospective GNTL in terms of organisation structure, infrastructure, manpower, and

[56] Deutsche Bundesbank (2012), p.59; Hansen & Meyer (2018), p.18.

[57] Assuming a 20- workdays month (240 workdays a year), one percentage point corresponds to 2.4 workdays. Three days of downtime, for example, due to a kill switch-induced communication blackout would thus correspond to a 0.375% reduction in GDP.

[58] Statistisches Bundesamt (2020).

financial endowment. What may come close is something like the Fraunhofer Heinrich Hertz Institute in Berlin. The annual budget amounted to almost EUR 57 million in 2018, financed by means of tax money (EUR 34 million) and funds coming from the private sector (EUR 23 million).[59] Given the size of the German economy, and its future dependence on 5G infrastructure, the allocation of a corresponding budget for a GNT seems to be a rather conservative evaluation. We estimate Germany's National Test Centre could cost up to EUR 60 million per year.

Regulatory Costs

The German National Regulatory Control Council (*Nationaler Normenkontrollrat*), founded in 2006 in order to support and realise the federal government's program for "Bureaucracy Reduction and Better Regulation", regularly evaluates the budgetary impact of laws and regulations for German administration, economy and citizens. Those estimated compliance costs solely refer to direct outcomes (additional staff, material expenses, certification costs, auditing, etc.), which are required to implement and comply with certain regulations. Regarding cybersecurity, the IT-Security Act from 2015 (see Table 6) and the upcoming IT-Security Act 2.0 (see Table 7, shall pass the Bundestag until spring 2021) are examples of such relevant regulations.

Table 6: Expected compliance costs IT Security Act 2015

Cost type	**Expected amount**	**Required Expenses (extracts)**
Administration		
Non-recurring expenses	EUR 6 million	Material costs
Annual expense	EUR 36 million	Staff (425 additional posts) at BSI (220), BKA[60] (80), BfV[61] (50), other authorities (75)
	EUR 2 million	Material costs
Economy		
Non-recurring expenses	Not mentioned	Not mentioned
Annual expenses	EUR 9 million (this amount did not include expenses for updating and adapting IT-Systems, certification for IT-standards, auditing, employment of contact points)	Reporting security incidents

[59] Fraunhofer HHI (2019), p. 6.

[60] Bundeskriminalamt (German Federal Bureau of Investigation)

[61] Bundesamt für Verfassungsschutz (German Federal Office for the Protection of the Constitution, domestic intelligence service)

Within the third draft of the IT-Security Act 2.0, considerations about compliance costs have also already been bound.

Table 7: Expected compliance costs IT Security Act 2.0 (planned 2021)

Cost type	Expected amount	Required Efforts (extracts)
Administration		
Non-recurring expenses	EUR 28.765 million	Material expenses at BSI and BKA
Annual expense	EUR 68.8 million	Staff (948 additional posts) at BSI (799), BKA (90), BNetzA (34), BDBOS[62] (21), Federal Ministry of Interior (4)
	EUR 57 million	Material costs
Economy		
Non-recurring expenses	EUR 70.000	Staff
Annual expense	EUR 3 million	Staff
	EUR 6 million	Other costs

Of course, not all the costs mentioned here are only caused by untrusted technology in 5G networks. Some of the resources are needed to oversee the compliance of MNOs with regulation. However, the presence of untrusted vendors in the market increases the need for more detailed and extended regulations. Therefore, parts of the aforementioned costs are directly or indirectly linked with untrusted vendors in IT networks.

In addition to those hidden costs, which result from the implementation and complexity of legislations, market players must bear the risk and the costs of involuntary violations of those regulations as well as potential penalties for operating possibly banned equipment. Violations of the IT Safety Act in Germany lead to penalties amounting to two per cent of the global annual revenue with a ceiling of EUR 10 million, in particular cases four percent of the annual revenue up to EUR 20 million.

Costs of Data Breaches

The presence of untrusted vendors in 5G networks will increase the risk of data breaches. In order to estimate the magnitude of the related fraction of costs of data breaches, we link the following components.

The starting point is the annual number of – reported – data breaches in Germany. For 2020, we are talking about 25,036 data breaches.[63] The average costs stemming from a single breach amount to EUR 4.45 million. We furthermore take into account the development of cybercrime, which is an emerging market, so to speak. An annual growth rate of cybercrime of 15 per cent[64] is assumed. We assume that one third of this relates to data in transit.[65]

[62] Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (Federal Agency for Digital Radio of Security Authorities and Organizations)
[63] IBM (2020).
[64] Morgan (2020).
[65] The three phases of the data life cycle are (1) ingestion (acquisition from local sensors), (2) data in transit and (3) data at rest. Lord (2019).

The current degree of dependency of MNOs in Germany on untrusted vendors is high, in terms of percentage and compared to other countries.[66] According to Strand Consult,[67] a share of 65 percent of network equipment in the network run by Deutsche Telekom (38.7% market share) has been produced by Huawei, with 55 per cent for Vodafone (24.4% market share) and 50 per cent[68] for Telefónica (36.9% market share).

With a degree of dependency of German MNOs, weighted by market share, on untrusted vendors of 57.03% (and equaling at least 50 per cent in the future, in the absence of market regulation)[69], and an assumed proportion of 5G traffic within Western Europe of 26 per cent[70] of overall traffic by 2022 and 29 per cent[71] by 2024, we can estimate expected losses caused by data breaches caused by the presence of untrusted vendors by the calculus outlined on page 47 of the policy paper.

Through this, we estimate costs stemming from additional data breaches due to the presence of untrusted vendors in 5G networks as amounting to EUR 16.4 billion by 2022 (when 5G will have started to play a considerable role in business and private life) and EUR **18 billion** in 2024 (when 5G will be commonplace). This must be regarded as a conservative estimate, as the relative importance of M2M use cases is growing disproportionally, which the described calculus does not yet reflect. It therefore produces an underestimation.

Quantification of magnitude of potential losses

Another way to look at potential losses, this time with a more holistic focus, is the grading of consequences of attack types within a Rossi-Forel scale. The attack types taken into consideration include the following:

A) Complete outage of telecommunication infrastructure of a single MNO, affecting business and private phone communication (voice, text, data)

B) as A), but also affecting IoT, industry 4.0, traffic etc.

C) Attack on data and software (public administration, business, private) resulting in encryption, inaccessibility or deletion of data

D) as C), but additionally including undetected falsification of data and software, potentially leading to accidents and malfunctions

E) Large scale and/or long-term interception of telecommunication (espionage)

[66] This assumption is based upon current figures for 4G RAN equipment.

[67] Strand Consult (2020), p.19.

[68] For Telefónica, this degree will probably diminish in the near future. Chairman José María Álvarez-Pallete López announced recently that "Telefónica is proud to be a 5G Clean Path company. Telefónica Spain and O2 (UK) are fully clean networks, and Telefónica Deutschland (Germany) and Vivo (Brazil) will be in the near future without equipment from any untrusted vendors." (Miragenews, 2020).

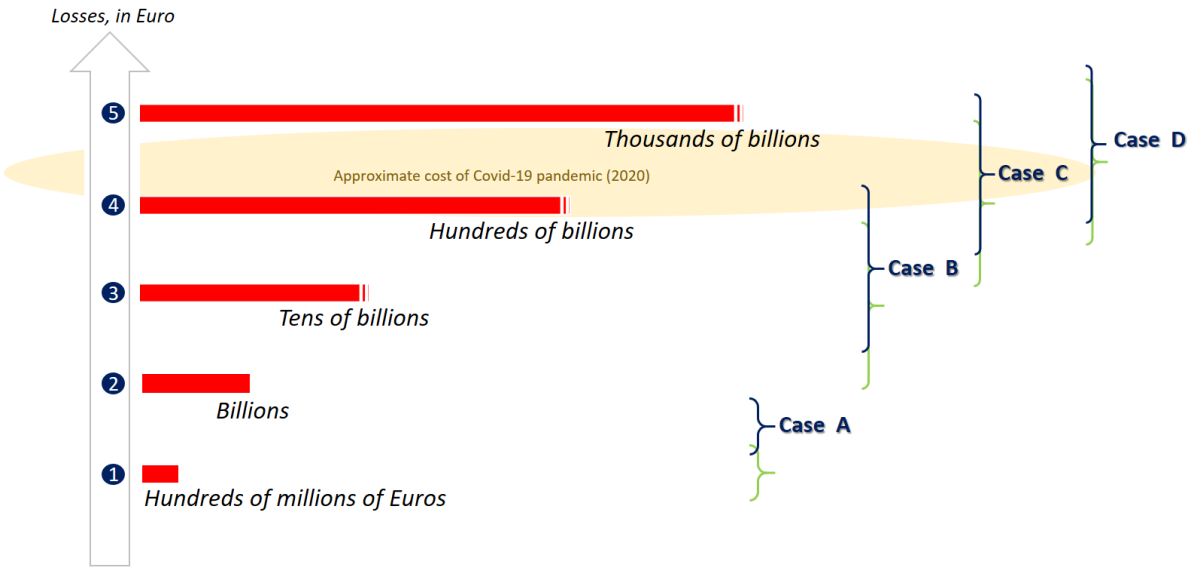
[69] Given free choice and based on observed business decisions in the past, we believe German operators will prefer to opt for at least 50 per cent of Huawei equipment in a 5G network, even when following a multi-vendor strategy.

[70] Qi (2020).

[71] Donkin (2018).

The impact of type E can hardly be assessed. Based upon the assumption of an average dependency of MNOs on Germany of 55 per cent[72] on network equipment provided by untrusted vendors and the level of the gross domestic product in Germany of EUR 3.4 trillion,[73] we can derive potential impacts of the types A through D to roughly quadruple the respective impact level in our neighboring economy France (see illustration 2). For details on this quantification method, see the country study for France.

Illustration 2: Scale of potential losses, Germany



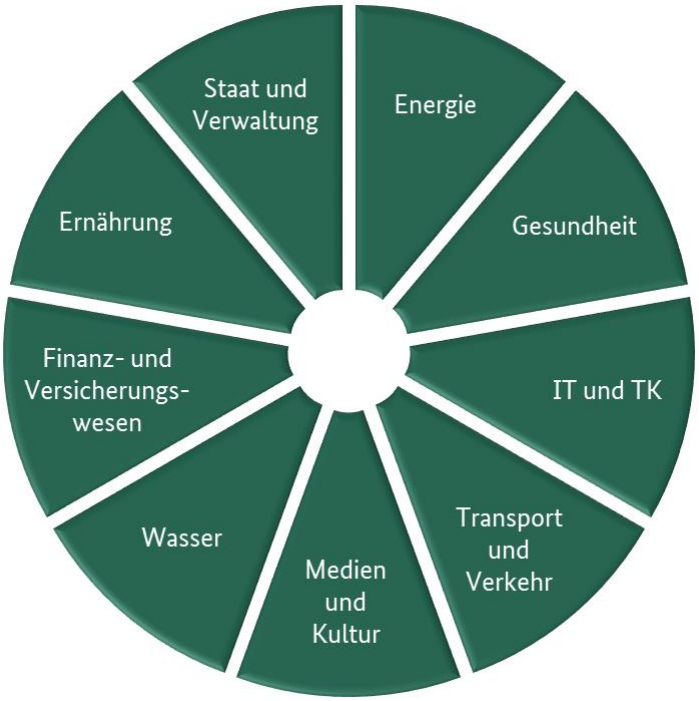
Magnitude of scale of loss potential linked to attack types. Green lines in the drawing indicate the respective magnitude in neighbor country France.

Shift of Demand

As elaborated in chapter 6.3, security sensitive telecommunication customers will be hesitant to connect to networks which contain untrusted technology. These security-sensitive companies are foremost the IPR-intensive industries, but also those that are critical for the functioning of the economy. In the figure below, you can find the sectors defined as being critical infrastructures (or KRITIS) in Germany (see illustration 3).

[72] Strand Consult (2020), p.19, also see footnote 67.
[73] Eurostat (2020).

Illustration 3: Sectors defined as critical infrastructure, as adopted by the German government in 2009



Source: BBK & BSI (2020)

These sectors are not reflected in national accounting one-to-one. However, it is still possible to derive approximated values for at least some of them. In illustration 4, along with that for several non-critical sectors, the gross value added is listed for relevant critical sectors: public services, health, education (18.8%) financial and insurance service providers (3.9%), information and communication (4.6%), totaling 27.3%.[74]

[74] Statistisches Bundesamt (German Federal Statistical Office, 2020). The definition of critical infrastructure in Germany (BBK 2020 - organisations or institutions of major importance to the state community, the failure or impairment of which would result in sustained supply shortages, significant disruption to public safety or other dramatic consequences) is based on economic sectors. Please note that the sector of education is tabulated by the German Federal Statistical Office in one category with public services and health, and cannot be computationally eliminated here.

Illustration 4: Overall gross value added, Germany, 2019, by sector

Source: modified representation, based on Statistisches Bundesamt [Federal Statistical Office] (2020a) and Statista (2020b)[75]

Assuming that this proportion is reflected in the structure of business customers of the telecommunication sector – a quarter of those belonging to critical infrastructures – we derive that up to 27% of the turnover of the communication sector (public sector and corporate customers) might shift towards MNOs with only trusted vendors. Customers from critical infrastructures may either switch to providers that work exclusively with trusted network equipment vendors, build their own campus networks, or even decide against using 5G technology altogether, at least in security-sensitive applications. Furthermore, future investments in Germany considered by foreign enterprises could be deterred in the presence of communication networks perceived as insecure.

While the first shift – customers switching operators – is rather a business-management consideration for the operators when making decisions about their choice of vendors, it nonetheless falls into the category of hidden costs. Not connecting to 5G networks and the associated foregone productivity gains bears the external cost of the MNOs' decision from whom to procure the network technology.

[75] Statistisches Bundesamt (2020a): Distribution of gross value added in Germany by economic sector in 2019; & Statista (2020b).

The German industry is quite IPR-intensive, with 49.9% compared with the EU average of 45%.[76] Since IP is the major target for industrial espionage, companies are particularly wary of the need to protect the source for competitive advantages. They will shy away from endangering the companies' treasures by exposing them on untrusted networks. Just like KRITIS, they will be willing to pay a premium for the usage of better protected networks, or will not connect to 5G networks at all. Therefore, we estimate that half of valuable business customers will be easily convinced not to leave their business with MNOs that use untrusted technology.

The turnover of the telecommunication service industry with business customers for 2020 in Germany is estimated to amount to EUR 21 billion.[77] The share of the critical infrastructure industry from all business sales we estimated to be 27%. This would translate into an absolute figure of EUR 5.7 billion. The share of the IPR-intensive industry for Germany is 49.9% and thus we estimate the share of MNO's sales with corporate customers to be around the same. That would translate into an absolute figure of 10.5 billion Euro. The foregone productivity gains are hard to estimate and are therefore ignored here. We are aware that there is an overlap between the IPR-intensive and the critical infrastructure industry. However, a large part of KRITIS cannot be considered IPR-intensive, like water supply, agriculture etc. It is therefore safe to say that more than half and up to two thirds of all MNOs' sales with corporate customers are in question here and should have a tendency to migrate towards trusted networks. Taking the total business customer turnover, this translated into annual absolute turnover values of up to EUR 14 billion.

However, we would prefer to stay on the conservative end of estimations. Constraining the estimation to mobile telecommunication services, we derive turnover values subject to potential shift of demand as high as EUR 2.5 billion for critical infrastructure industries, and 4.6 billion for IPR intensive industries (for the calculation method, see page 37f. in the policy paper). Again taking into account the indisputable overlap of both industries, it is therefore safe to say that more than half (as IPR alone already accounts for almost 50%, see above) of all MNOs' sales of mobile services to corporate customers are subject to a potential shift. We therefore estimate that more than half of the market with business customers, or **EUR 4.6 billion,** will have a tendency to shift toward MNOs with only trusted technology in their 5G networks.

For KRITIS, it is also foreseeable that using only trusted networks might be required through regulation in the future, and for other businesses, cyber-insurance companies could make it a requirement for their customers. This potential shift of demand from business clients is huge and should in particular worry Deutsche Telekom and Vodafone, since they have the larger portfolio of business customers in Germany. Plus, the benefits of 5G are mainly in

[76] EUIPO (2019).

[77] Dialog Consult/VATM (2019), p. 6. The number includes voice and internet services, data services, interconnection, leased lines, content, terminal equipment and distribution of TV content provided by network operators and their distribution partners. Figures in square brackets indicate the corresponding absolute revenues in the previous year.

business applications, and therefore the MNOs' business with corporate customers should relatively increase.

Deutsche Telekom alone currently has an annual turnover in Germany with their MNO business of EUR 8.2 billion.[78] With 5G, the share of wireless services in the telecommunication market should increase as well as the share of sales with business clients. When more than half of the turnover with business clients in a 5G world is at stake, the EUR 3 billion Deutsche Telekom claims that rip and replace of untrusted technology will cost them (see below in section Costs of Rip and Replace, footnote 82) sounds less frightening. Additionally, since the EUR 3 billion seem to be exaggerated in the first place, if one compares that amount with, for instance, the GBP 500 million (approximately EUR 0.556[79]) communicated by British Telecommunications.[80]

Redundant infrastructure

Another big customer of telecommunication companies can be the government with its various entities. However, if the government comes to the conclusion that its communication is not sufficiently safe in a privately run network, it will operate its own network for its purposes. The presence of untrusted vendors in a future German 5G communication network therefore might force the government to invest in a redundant infrastructure that is fully controlled by the German state. How costly this can be is illustrated by the case of the Netz des Bundes (Federal Network) in Germany.

Initially, the costs had been planned to fall within the range of EUR 100 million for transition from a commercial network provider to the government network, plus EUR 92.2 million per year for the operation. It turned out, however, that the project suffered from severe delays of about six years, with costs multiplying almost by a factor of four (currently amounting to about EUR 426 million).[81]

Costs of Rip and Replace

There is a high proportion of network equipment built into existing 4G network infrastructure, in the range of 50 to 65 per cent for the three major MNOs in Germany (see above in section Costs of Data Breaches for details). In the case of a regulatory decision requiring a rip and replace of this equipment in the near future, or a business decision to do so for other reasons, MNOs will have to face considerable costs (with possible claims for indemnities not considered here). Deutsche Telekom, one of the major telecommunication providers in Germany, numeralised this scenario in an internal memo prepared for a CEO-level meeting with at least EUR 3 billion.[82] This corresponds to approximately **EUR 65 per mobile phone customer**, given their 46.2 million customers (contracts and prepaid cards).[83]

[78] Statista (2020a). This includes turnover with corporate and private customers.
[79] Currency conversion based on exchange rate 1.11224, valid on July 14, 2020.
[80] Reuters (2020).
[81] For more details on this, see chapter 6.3.
[82] Koch & Scheuer (2020b).
[83] Deutsche Telekom (2019).

The fact that the press was granted insight into an internal document of that nature might point towards an attempt of more or less subtle exertion of influence on the policy-making process at a point in time deemed favorable. It is unclear whether a full cost accounting would generate the same number after the IT security law 2.0 in Germany is passed.

A rip and replace at a later point in time, after considerable rollout of 5G network equipment including that of untrusted vendors, will most likely come at a higher price.

Summary

Depending on the subject and cost category looked at, we estimate annual hidden costs of failing to exclude untrusted vendors as ranging from as few as EUR 60 million for the operation of a test centre to more than EUR 18 billion for consequences of data breaches. The pillars shown below in illustration 5 are not mutually exclusive.

The takeaway point here is not an absolute figure, but the graphic clarification that the looming costs of a possible moderate delay in rollout of 5G networks is a comparatively small price a society has to pay. This is particularly the case given the current and foreseeable shortage of applications and real life use cases of 5G technology, apart from faster internet connections.

The IT Security Act 2.0 must be well crafted to be an effective tool. While it must not be a law directed against specific companies for reasons of principle, the protection of security policy interests must be given the appropriate weight in the weighing and coordination processes of the ministries involved.

The law should come into force soon and be implemented swiftly to provide clarity for market participants. It is undoubtedly foreseeable that the People's Republic of China will exert pressure on German decision-makers to secure access to German data networks. But the commitment to open markets and free trade does not contradict regulated access to security-critical infrastructures, which are also the basis for future growth.

It must be ensured that the lowest common denominator is not decisive for the depth of intervention in departmental coordination, also in view of the necessary reaction speed in a software-defined communications network and the technical complexity of decision-making. On the contrary, for economic reasons as well, it may be prudent to err on the side of caution.

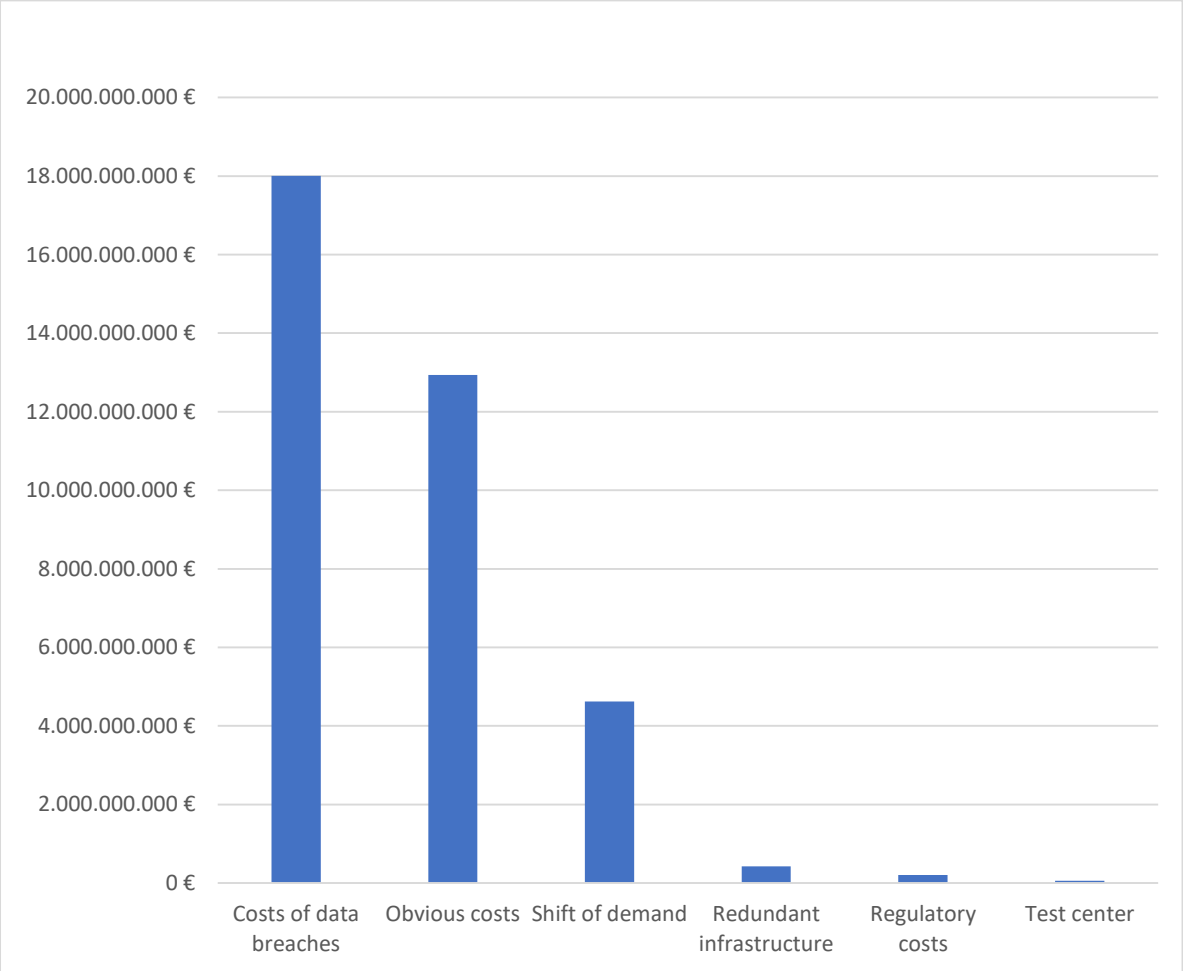
Otherwise, in the medium term, there is a risk of considerable losses in competitiveness for German SMEs and for the labor market of major corporations. The hidden costs are therefore not obvious, as they will either arise at a later date or will have to be shouldered by third parties who had nothing to do with the decisions that made them possible in the first place.

There are also non-monetary costs to consider. A non-obvious but very weighty point is the potential unwillingness of allied intelligence services to share security-related intelligence with the German government or its subordinate services in the future, if that intelligence could leak out for technical reasons.

Overall, we have been able to show for Germany theoretically in the policy paper and empirically in this country study that the total societal costs, i.e. including externalities, are higher over time than the potential savings that arise for mobile network operators when they use non-trusted network technology to deploy 5G. This form of market failure must be cured through adequate regulation in order to realise the growth-enhancing potential of 5G technology in the coming decade. The opportunity for this exists with the present IT Security Act 2.0, if this is implemented consistently. However, if the high proportion of untrusted technology remains, as we are seeing in Germany with the 4G networks, considerable costs

for protective measures in the IT sector will be incurred by the German economy and security-relevant government institutions.

Illustration 5: Range of exemplary quantifications of hidden costs (Germany, non-exclusive)



Source: Own calculations

Sources

1&1 Drillisch (2020): Annual Report 2019. [Online]. Available: https://imagepool.1und1-drillisch.de/v2/download/berichte/2020-03-26-1und1-Drillisch_GB_2019_ENG.PDF, accessed Nov. 2020.

Baldwin, R., & Krugman, P. (1988): Industrial policy and international competition in wide-bodied jet aircraft. In Trade policy issues and empirical analysis (pp. 45-78). University of Chicago Press.

BBK & BSI (2020): Kritische Infrastrukturen – Definitionen und Übersicht. [Online]. Available: https://www.kritis.bund.de/SubSites/Kritis/DE/Einfuehrung/einfuehrung_node.html, accessed Nov. 2020.

BMI [Federal Ministry of the Interior] (2020): "Referentenentwurf IT-Sicherheitsgesetz 2.0" [Draft Law], from the 19 November, https://intrapol.org/wp-content/uploads/2020/11/Entwurf-IT-SiG-2.0-19.11.2020.pdf, accessed Nov. 2020.

BMVI [Federal Ministry of Transport and Digital Infrastructure] (2017). 5G-Strategie für Deutschland. [Online]. Available: https://www.bmvi.de/blaetterkatalog/catalogs/350336/pdf/complete.pdf, accessed Nov. 2020.

Broszio S. (2020). "Diversity instead of dependence", *Deutsche Telekom Blog Post from the 7th July,* https://www.telekom.com/en/blog/group/article/telekom-committed-to-a-multi-vendor-strategy-603524, accessed Nov. 2020.

Bundesnetzagentur (2019). Frequenzversteigerung beendet. [Online]. Available: https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2019/20190612_Frequenzauktion.html, accessed Nov. 2020.

Bundesnetzagentur (2020a). Frequenzvergabeverfahren 2010. [Online]. Available: https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Breitband/MobilesBreitband/Frequenzauktion/Z_Auktion2010.html;jsessionid=FA2008E86C15AFD121E1204CA817EC03?nn=268128, accessed Nov. 2020.

Bundesnetzagentur (2020b). Mobiles Breitband – Projekt 2016. [Online]. Available: https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Breitband/MobilesBreitband/Frequenzauktion/Z_Auktion2016.html;jsessionid=22D33945A2D907C392487C189FBB99D8?nn=268128, accessed Nov. 2020.

Bundesnetzagentur (2020c): Frequenzauktion 2019. [Online]. Available: https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Breitband/MobilesBreitband/Frequenzauktion/2019/Auktion2019.html;jsessionid=FA2008E86C15AFD121E1204CA817EC03?nn=268128, accessed Oct. 2020.

Deutsche Bundesbank (2012): "Kalendarische Einflüsse auf das Wirtschaftsgeschehen", Monatsbericht Dezember, p.59.

Deutscher Bundestag (2019): Antrag Drucksache 19/16047. [Online]. Available: http://dip21.bundestag.de/dip21/btd/19/160/1916058.pdf, accessed Nov. 2020.

Deutsche Telekom (2019). The 2019 Financial Year. [Online]. Available: https://report.telekom.com/annual-report-2019/servicepages/downloads/files/entire_dtag_ar19.pdf, accessed Oct. 2020.

Dialog Consult / VATM (2018): 22. TK-Marktanalyse Deutschland 2020. Ergebnisse einer Befragung der Mitgliedsunternehmen im Verband der Anbieter von Telekommunikations- und Mehrwertdiensten e. V. im dritten Quartal 2020. [Online]. Available: https://www.vatm.de/wp-content/uploads/2020/10/VATM_TK-Marktstudie-2020_061020.pdf, accessed Nov. 2020.

DIE LINKE-Fraktion im Bundestag (2019a). "Digitale Infrastruktur ist Teil der modernen Daseinsvorsorge"*, Positionspapier des AK III Wirtschaft und Finanzen der Fraktion DIE LINKE im Bundestag from the 13th August,* https://www.linksfraktion.de/themen/positionspapiere/detail/digitale-infrastruktur-ist-teil-der-modernen-daseinsvorsorge/, accessed Nov. 2020.

DIE LINKE-Fraktion im Bundestag (2019b). "5G - das schnelle Netz für Städter mit großen Geldbeuteln", *Pressemitteilung von Anke Domscheit-Berg der Fraktion DIE LINKE im Bundestag from the 19th March,* https://www.linksfraktion.de/presse/pressemitteilungen/detail/5g-das-schnelle-netz-fuer-staedter-mit-grossen-geldbeuteln/, accessed Nov. 2020.

DIE LINKE-Fraktion im Bundestag (2020). "Souveränität verteidigen", In the wording of Klaus Ernst, Frankfurter Rundschau from the 23rd August, https://www.linksfraktion.de/themen/nachrichten/detail/souveraenitaet-verteidigen/, accessed Nov. 2020.

Donkin, C. (2018): 5G connections to hit 1.5B by end-2024 – Ericsson. [Online]. Available: https://www.mobileworldlive.com/featured-content/home-banner/5g-connections-to-hit-1-5b-by-end-2024-ericsson, accessed Nov. 2020.

Ericsson (2020). "Deutsche Telekom and Ericsson strengthen partnership with 5G deal", *Ericsson Press Release from the 22nd July,* https://www.ericsson.com/en/press-releases/2020/7/deutsche-telekom-and-ericsson-strengthen-partnership-with-5g-deal, accessed Nov. 2020.

EUIPO [European Union Intellectual Property Office](2019): "Impact of intellectual property rights intensive industries in the European Union", https://euipo.europa.eu/ohimportal/en/web/observatory/ip-contribution, accessed Nov 2020.

Eurostat (2020): GDP and main components (output, expenditure and income). [Online] Available: http://appsso.eurostat.ec.europa.eu/, accessed Nov. 2020.

FDP-Fraktion im Bundestag (2019): *"Souveräner Dialog auf Augenhöhe - Deutschlands und Europas Aufgaben zur Verteidigung westlicher Werte im Systemwettbewerb mit China", Beschluss der Fraktion der Freien Demokraten im Deutschen Bundestag from the 6th September,* https://www.fdpbt.de/sites/default/files/2019-09/190906_Beschluss_Systemwettbewerb_mit_China.pdf, accessed Nov. 2020.

Fraunhofer HHI (2019): „ Jahresbericht 2016 / 2017 / 2018,". [Online]. Available: https://www.hhi.fraunhofer.de/fileadmin/PDF/Jahresbericht/Jahresbericht_16_17_18_DE.pdf, accessed Oct. 2020.

Handelsblatt (2020): "Preisstreit mit Telefónica setzt United Internet und 1&1 Drillisch zu", *Handelsblatt from the 21st September,* https://www.handelsblatt.com/technik/it-internet/telekommunikation-preisstreit-mit-telefonica-setzt-united-internet-und-1und1-drillisch-zu/26204180.html, accessed Oct. 2020.

Hansen, A. & Meyer, D. (2018): "Wie viel kosten uns die arbeitsfreien Feiertage?", ifo Schnelldienst Kommentar, p.18.

Hegemann, L. (2020). “Bundesregierung will Hersteller bei 5G-Ausbau notfalls ausschließen”*, Zeit from the 21st November*, https://www.zeit.de/digital/internet/2020-11/it-sicherheit-gesetz-g5-netz-ausbau-huawei, accessed Nov. 2020.

Heise (2020). “5G-Netze: Unionsfraktion für Sicherheitsstandards, kein Ausschluss von Huawei”, Heise from the 11th February, https://www.heise.de/newsticker/meldung/5G-Netze-Unionsfraktion-fuer-Sicherheitsstandards-kein-Ausschluss-von-Huawei-4658356.html, accessed Nov. 2020.

Hendrich, J. & Kenji Kipker, D. (2020): “Wie das IT-Sicherheitsgesetz 2.0 Bürger und Unternehmen regulieren soll”, Heise from the 27th July, https://www.heise.de/hintergrund/Wie-das-IT-Sicherheitsgesetz-2-0-Buerger-und-Unternehmen-regulieren-soll-4842913.html, accessed Nov. 2020.

Heuzeroth, T. (2020a): “5G kommt schneller als gedacht – wird aber zuerst enttäuschten”, Welt from the 12th November, https://www.welt.de/wirtschaft/webwelt/article219823856/Vodafone-und-Telekom-5G-kommt-schneller-als-gedacht.html, accessed Nov. 2020.

Heuzeroth, T. (2020b): “Im deutschen 5G-Kernnetz wird Huawei keine Rolle spielen”, Welt from the 15th November, https://www.welt.de/wirtschaft/article220137122/Im-deutschen-5G-Kernnetz-wird-Huawei-keine-Rolle-spielen.html, accessed Nov. 2020.

IBM (2020): Cost of a Data Breach Report. [Online]. Available: https://www.ibm.com/security/digital-assets/cost-data-breach-report/, accessed Nov. 2020.

Kamp, M. (2020): “Erste Konturen einer neuen deutschen Chinapolitk”, Neue Züricher Zeitung from the 30 October, https://www.nzz.ch/pro-global/asien/n-roettgen-erste-konturen-einer-neuen-deutschen-chinapolitik-ld.1581815?reduced=true, accessed Nov. 2020.

Koch, M., Scheuer, S. & Iwersen, S. (2020): “Die Huawei-Connection: Wie die Telekom immer abhängiger von China wurde”, Handelsblatt from the 7th July, https://www.handelsblatt.com/technik/it-internet/telekommunikation-die-huawei-connection-wie-die-telekom-immer-abhaengiger-von-china-wurde/25980888.html?ticket=ST-3367413-YvIhSv7H0YhuoiiZFqXQ-ap2, accessed Oct. 2020.

Koch, M. & Scheuer, S. (2020a): “Telefónica verzichtet auf Huawei im 5G-Kernnetz" Handelsblatt from the 3 June, https://www.handelsblatt.com/politik/deutschland/netzausruester-telefnica-verzichtet-auf-huawei-im-5g-kernnetz/25880036.html, accessed Nov. 2020.

Koch, M. & Scheuer, S. (2020b): “”Armageddon”-Szenario: Telekom spielt Huawei-Bann durch" Handelsblatt from the 16th June, https://www.handelsblatt.com/technik/it-internet/ausschluss-von-netzausruester-armageddon-szenario-telekom-spielt-huawei-bann-durch/25918402.html?ticket=ST-3320249-5KKptczSxbOQREKfwacP-ap4, accessed Nov. 2020.

Kuhn, T. (2020a): “Ich habe nicht mal ein Smartphone”, WirtschaftsWoche from the 20th November, https://www.wiwo.de/my/unternehmen/it/chef-von-united-internet-ich-habe-nicht-mal-ein-smartphone/26638036.html?ticket=ST-258223-kLcv95FKzjkMxXVo6VuQ-ap3, accessed Nov. 2020.

Kuhn, T. (2020b): “5G von 1&1: Rosinenpicker oder diskriminierter Neueinsteiger?”, WirtschaftsWoche from the 21st November, https://www.wiwo.de/my/unternehmen/dienstleister/mobilfunknetze-5g-von-1und1-rosinenpicker-oder-diskriminierter-neueinsteiger/26638060.html, accessed Nov. 2020.

Lord, N. (2019): “Data Protection: Data In Transit vs. Data At Rest”, https://digitalguardian.com/blog/data-protection-data-in-transit-vs-data-at-rest, accessed Dec. 2020.

Manager Magazin (2020): “Huawei-Bann würde Telekom Milliarden kosten, United Internet will es ohne etablierte Ausrüster schaffen”, Manager Magazin from the 17 June, https://www.manager-magazin.de/unternehmen/artikel/huawei-bann-wuerde-telekom-milliarden-kosten-united-internet-geht-neuen-weg-a-1307768.html, accessed Nov. 2020.

Miragenews (2020): “Tide is Turning Toward Trusted 5G Vendors“. https://www.miragenews.com/tide-is-turning-toward-trusted-5g-vendors , accessed Jan.2021.

Morgan, S. (2020): Official Annual Cybercrime Report. [Online]. Available: https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/, accessed Nov. 2020.

Nationaler Normenkontrollrat: Stellungnahme des Nationalen Normenkontrollrates gem. § 6 Abs. 1 NKRG: Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (NKR-Nr. 3044), 4. December 2014. Berlin.

Neuerer, D. (2019). “Grüne planen Anti-Huawei-Initiative im Bundestag”*, Handelsblatt from the 13th December,* https://www.handelsblatt.com/politik/deutschland/it-sicherheit-gruene-planen-anti-huawei-initiative-im-bundestag/25330408.html?ticket=ST-3723883-P4oRsDxsr3C2MtIozY0e-ap5, accessed Nov. 2020.

n-tv (2020): *“*Streit zwischen 1&1 und Telefónica eskaliert”*, n-tv from the 21 September*, https://www.n-tv.de/wirtschaft/Streit-zwischen-1-1-und-Telefonica-eskaliert-article22050078.html, accessed Oct. 2020.

Oxford Economics (2020) Restricting Competition in 5G Network Equipment throughout Europe. An Economic Impact Study. June 2020

Qi, E. (2020): 5G Mobile Connections Will Cross the Milestone of 1.7 Billion in 2023. [Online]. Available: https://www.counterpointresearch.com/5g-mobile-connections/, accessed Nov. 2020.

Reuters (2019): “Telefónica Deutschland hält an Huawei als 5G-Partner fest”, *Reuters from the 11th December,* https://de.reuters.com/article/deutschland-telefonica-deutschland-idDEKBN1YF12G, accessed Nov. 2020.

Reuters (2020): “BT says Huawei ban can be absorbed in 500 million pounds already earmarked”, July 14, 2020, https://www.reuters.com/article/idUSKCN24F2A2, accessed Jan. 2021.

Sawall, A. (2020): “Huawei-Ausschluss würde 5G-Ausbau um 5 Jahre verzögern”*, Golem from the 30th October,* https://www.golem.de/news/vodafone-deutschlandchef-huawei-ausschluss-wuerde-5g-ausbau-um-5-jahre-verzoegern-2010-151826.html, accessed Nov. 2020.

SNV (2020): „Stellungnahme zum Referentenentwurf ‘IT-Sicherheitsgesetz 2.0‘ – in der Fassung vom 01.12.20201 – des Bundesministeriums des Innern, für Bau und Heimat“. [Online]. Available: https://www.stiftung-nv.de/de/publikation/stellungnahme-zum-referentenentwurf-it-sicherheitsgesetz-20-der-fassung-vom-09122020-0, accessed Jan. 2021.

SPD-Fraktion im Bundestag (2019): “Ein digital souveränes Europa mit sicheren 5G-Netzen", SPD-Fraktion from the 17th December, https://www.spdfraktion.de/themen/digital-souveraenes-europa-sicheren-5g-netzen, accessed Nov. 2020.

Spiegel (2013): O2 kauft E-Plus. [Online]. Available: https://www.spiegel.de/wirtschaft/unternehmen/milliardendeal-im-mobilfunk-telefonica-kauft-e-plus-a-912516.html, accessed Nov. 2020.

Statista (2020a). Statistiken zur Deutschen Telekom. [Online]. Available: https://de.statista.com/themen/124/deutsche-telekom/, accessed Nov. 2020.

Statista (2020b) Verteilung der Bruttowertschöpfung* in Deutschland nach Wirtschaftszweigen im Jahr 2019. [Online]. Available: https://de.statista.com/statistik/daten/studie/252123/umfrage/anteil-der-wirtschaftszweige-an-der-bruttowertschoepfung-in-deutschland/#professional, accessed Nov. 2020.

Statistisches Bundesamt (2020a):“ National accounts, gross domestic product 2019”, Wiesbaden, https://www.destatis.de/DE/Themen/Wirtschaft/Volkswirtschaftliche-Gesamtrechnungen-Inlandsprodukt/Tabellen/bip-bubbles.html, accessed Oct 2020.

Statistisches Bundesamt (2020b): Population. https://www.destatis.de/EN/Themes/Society-Environment/Population/Current-Population/_node.html#sprg267530, accessed Dec. 2020.

Stempfle, M. (2020): “Doppeltes Prüfverfahren für Huawei”*, Tagesschau from the 30th September*, https://www.tagesschau.de/wirtschaft/5g-huawei-pruefverfahren-sicherheit-101.html, accessed Nov. 2020.

Strand Consult (2020): Understanding the Market for 4G RAN in Europe: Share of Chinese and Non-Chinese Vendors in 102 Mobile Networks - Version 1.1 -, p.19.

Sweney, M. (2020): “Vodafone to remove Huawei from core European networks”, *The Guardian from the 5th February,* https://www.theguardian.com/business/2020/feb/05/vodafone-to-remove-huawei-from-core-european-networks, accessed Nov. 2020.

Telefónica (2019): Consolidated Financial Statements for 2019. [Online]. Available: https://www.telefonica.de/investor-relations-en/annual-report.html, accessed Oct. 2020.

Vodafone Group Plc (2020): Annual Report 2020. [Online]. Available: https://www.vodafone.com/content/dam/vodcom/files/vdf_files_2020/pdfs/vodafone-annual-report-2020.pdf, accessed Nov. 2020.

Voland, T. & Büsch, P. (2020): “Nächster Versuch – BMI legt neuen Entwurf des IT SiG 2.0 vor”, *Politik und Kommunikation from the 18th June,* https://www.politik-kommunikation.de/gesetz-des-monats/naechster-versuch-bmi-legt-neuen-entwurf-des-it-sig-20-vor-1781324920#:~:text=W%C3%A4hrend%20die%20strafrechtlichen%20Vorschriften%20aus,Erh%C3%B6hung%20der%20m%C3%B6glichen%20Bu%C3%9Fgeldzahlungen%20vor, accessed Nov. 2020.

Weidner, M. (2020): “1&1 Drillisch: Erste Basisstationen für neues Mobilfunknetz”, *Teltarif from the 27th January,* https://www.teltarif.de/1und1-drillisch-mobilfunknetz-basisstation/news/79409.html, accessed Nov. 2020.