ANALYSIS

5G and beyond: A test for "technological sovereignty" in Europe?

Isabel Skierka, Researcher at the European School of Management and Technology Berlin; PhD candidate at TalTech University, Estonia; non-resident fellow at GPPi, Berlin

December 2019 [This article was submitted in late December 2019. Therefore, developments after that point in time are not considered in this article.]

About the Author

Isabel Skierka is a researcher with the Digital Society Institute at ESMT Berlin, where she focuses on cybersecurity policy in Germany and Europe (including IoT security and safety), electronic identity management, and the intersection of geopolitics and technology. She is also pursuing a PhD at the Ragnar Nurkse Department of Innovation and Governance at Tallinn University of Technology in Estonia in which she explores cybersecurity crisis management. She is a non-resident fellow with the think tank Global Public Policy Institute (GPPi) in Berlin, and serves as a member of multiple multi-stakeholder organizations in the field of digital policy. Prior to joining ESMT, Isabel worked with GPPi, NATO, at the European Commission's DG Connect (as a Bluebook trainee), and as a visiting researcher at the Institute of Computer Science of the Free University of Berlin. Isabel holds a master's degree in international conflict studies from the War Studies Department of King's College London and a bachelor's degree in European studies from Maastricht University, including an exchange at Sciences Po in Paris.

In the heated debate over Chinese vendors' participation in the roll-out of 5G mobile networks, Europe has so far refrained from a black-and-white stance on the issue. For months, the United States has pressured European allies to exclude Chinese vendors such as Huawei from 5G networks on national security grounds.

In the end, European Union (EU) member states have been navigating a 'middle way' between an outright ban, following countries like the United States or Australia, and a completely vendor-agnostic approach. In October 2019, the EU Network Information Security (NIS) cooperation group (composed of representatives from EU member states, the European Commission and the EU's cybersecurity agency ENISA) published a joint risk assessment which provides a thorough overview of the technical, but also the non-technical, political challenges related to securing 5G networks.[1] The report emphasizes the need for robust IT security risk management and other technical measures, but also warns member states of deploying equipment from suppliers that are likely to be "subject to interference from a non-EU country" due to respective legislation and a lack of "democratic checks and balances". It also names "non-EU states or state-backed actors" as a primary threat to 5G network security. The wording's code for the Chinese tech giant Huawei and China itself is hard to miss. A set of Council Conclusions published in early December 2019 echoed these concerns.[2] On this basis, the EU is poised to publish a 'toolbox' of technical, legal, and political risk mitigation measures by 31 December 2019.[3]

The challenges that the EU faces with 5G go beyond cyber and national security threats. For Europe, the rollout of the 5G infrastructure has become a geopolitical test on several levels. Will Europe be a shaper or taker of 5G technology and the new era of industrialization it promises to propel? How will it be able to control the security and reliability of such key digital infrastructures in the long-term? Eventually, how should EU member states manage their dependencies on foreign technologies and strengthen their "technological sovereignty" – a political priority of the incoming EU Commission led by Ursula von der Leyen?[4] The latter might be the most important strategic issue the EU will need to tackle in the long-term and will be decisive for the Union's ability to shape its own future in the digital age.

It is against this wider geopolitical backdrop that EU member states will need to decide the handling of 5G security risks and potential dependencies on Chinese suppliers, like Huawei, in their telecommunications networks. The precondition for a unified approach is unity among EU member states.

The German debate – a precedent for Europe?

In Germany, the question of Huawei's involvement in the rollout of 5G networks has perhaps triggered the most intense public debate of all countries in Europe. The

While the inclusion of Huawei in the rollout of 5G networks carries significant political and economic risks, German industry also has a lot to lose. Excluding Huawei from the network would likely result in some form of retaliatory action from Beijing that could harm the German economy

country's decision about 5G security will send an important signal to other EU members – Germany has the largest national economy and largest telecommunications market in Europe. While the inclusion of Huawei in the rollout of 5G networks carries significant political and economic risks, German industry also has a lot to lose. Excluding Huawei from the network would likely result in some form of retaliatory action from Beijing that could harm the German economy and specific industries, such as the car industry. Chinese officials and more recently, the Chinese ambassador to Germany, have already hinted at this possibility.[5]

In this context, the German government had originally planned to adopt a purely technical approach to 5G security. Days after the EU's join risk assessment's publication on 9 October 2019, the German government released a catalog of draft telecommunications security requirements. Drafted by two lower level government agencies – the Federal Network Agency (BNetzA) and the Federal Office for Information Security (BSI) – the catalog argued that security would be guaranteed above all by the technical certification of software and hardware from 5G technology providers and inspection of the source code.[6] In addition, operators of public telecommunications networks would have to request a "declaration of trustworthiness"[7] from the equipment vendor. The equipment vendors' corporate structure and the context of the legal and political environment in which it operates – key aspects raised in the EU joint risk assessment – would not have to be evaluated. Under these conditions, network operators would have been able to source the majority of 5G network components from Chinese equipment manufacturers such as Huawei and ZTE.

However, the German government's approach did not consider the non-technical political and economic risks of a long-term dependency on Chinese suppliers. Local intelligence legislation allows the Chinese government to coerce companies like Huawei or ZTE into cooperating with national intelligence agencies and potentially facilitate espionage or sabotage of 5G infrastructures abroad. Apart from the frequently emphasized risks for national security, relying on a foreign tech giant entails considerable economic and industrial disadvantages. European competitors like Nokia and Ericsson will have difficulties surviving in the face of an increasingly powerful Chinese tech giant that is likely subsidized[8] by its national government. The absence of any strategy for 5G security and industrial policy from the German government's approach from fall 2019 was striking. By delegating the decision on 5G security

to the technocratic level, the German government evaded political responsibility for an issue of high geopolitical significance.

According to media reports[9], the German chancellor herself intervened in order to prevent restrictions against Chinese suppliers. Likely motives include the fear of Chinese retribution against German companies such as Volkswagen, Siemens, or BASF, which heavily rely on the Chinese market. This approach remarkably differs from that of other European countries. France or Italy, for example, have awarded government ministers or security services with the powers to examine and decide over network operators' plans to roll out 5G on the grounds of national security concerns.[10]

Yet, the tides have been turning in Germany and triggered a vivid parliamentary debate which could, after all, lead to a de facto restrictions of Huawei equipment in Germany. Not long after the draft guidelines' publication, a group of parliamentarians rebelled against the government and demanded the chancellor to submit the decision on 5G to the German parliament instead of declaring it a fait accompli.[11] Among them were a number of prominent members of Merkel's own party, the Christian Democratic Union (CDU), thereby also turning the debate into a leadership test for the chancellor. Throughout the months of November and December, various coalitions, both among governing parties and opposition parties, formed in parliament, all debating and working on new 5G security criteria.[12]

At the time of writing (mid-December), the government coalition has been deliberating to adopt tougher criteria for vendors to participate in the 5G network rollout, including the political and legal conditions that any given vendor is exposed to in its country of origin.[13] Such language and propositions made into a public position paper by the Social Democratic Party (SPD) coalition partner and an informal paper from members of the CDU/CSU parties would allow a de facto ban of Chinese vendors, at least from critical parts of future 5G networks.[14] Merkel's CDU is expected to explore a common position in January.[15]

Meanwhile, Telefónica Deutschland, which is Germany's second largest telecoms operator confirmed that Huawei would help build its network. Vodafone, the third largest operator, warned that an exclusion of Huawei would delay its 5G rollout up to five years, and Germany's largest and partially state-owned operator Deutsche Telekom will freeze spending on new 5G equipment due to political uncertainty.[16]

Whatever the final outcome will be, the German case is an example for how decisions on the deployment of strategic technologies and issues of national security as well as 'technological sovereignty' can be openly and democratically debated by the

According to media reports, the German chancellor herself intervened in order to prevent restrictions against Chinese suppliers. Likely motives include the fear of Chinese retribution against German companies such as Volkswagen, Siemens, or BASF, which heavily rely on the Chinese market.

legislative and executive. Despite the long time it took decision makers to grasp the importance of the issue and engage in a serious debate, it could set a precedent for future similarly strategic discussions.

Decisions in other EU member states as well as the EU 5G cybersecurity toolbox to be published by the end of December will give further impetus to the development of a common, or divided, EU position on the geopolitics of 5G.

Beyond 5G: "Technological sovereignty" in Europe

Although on the surface, the debate about 5G security centers around cyber security and national security concerns, its major strategic dimension is that of what the European Commission refers to as "technological sovereignty".[17] Technological sovereignty is a widely used political term that remains yet to be defined, let alone operationalized. In European political discourse, it refers to the ability of an actor (a state, a company or an individual) to act and decide independently in the digital realm. A precondition for technological sovereignty is a certain degree of control over key competences and technologies as well as the ability to decide among alternative technologies and capabilities provided by trustworthy partners, and the ability to further develop these, if necessary.[18] In this context, sovereignty does not equal autarky. Rather, it consists precisely in the ability of entering into dependencies while being able to master them through the capacity to assess and (to a certain degree) control technologies and capabilities.

Hence, how can Europe "strengthen its technological sovereignty" – a proclaimed goal by the new European Commission? Since European countries are increasingly dependent on foreign technology suppliers, particularly in the areas of cloud and data infrastructure and software, mobile and desktop operating systems, as well as semiconductors and microprocessors, this will be no easy task. Ironically in the context of the 5G debate, one of the few technology fields in which European companies are still leading, is that of mobile communications equipment. Two of the three Radio Access Network market leaders, Ericsson and Nokia, are European and competitors of Huawei. In the context of the 5G debate, a first step should therefore be to strengthen European manufacturers and to level the playing field for them on the European market. This will require not only security guidelines, but, in the long-term, competition and industrial policy measures.

Enhancing its members' capacity to act more independently in the digital realm will require the EU to strengthen its own industrial base in key technology sectors, as well as managing necessary dependencies in an interdependent and global economy and supply chain through trade and diplomatic tools.

As a first step, decision-makers in Europe should therefore determine which key technologies and competencies they themselves should produce and command, and in which areas they can enter into dependencies. This must be accompanied by a strategy for managing dependencies on foreign technology providers, which inevitably arise in the global value chain. With which partners can and should EU member states cooperate in the long term, and in what frameworks? The trustworthiness of the political and legal system as well as previous experience with partners within an alliance should play an important role as part of this assessment.

Although on the surface, the debate about 5G security centers around cyber security and national security concerns, its major strategic dimension is that of what the European Commission refers to as "technological sovereignty"

Moreover, governments should actively promote innovation and strengthen their own industrial base in key technology fields, such as robotics, artificial intelligence capabilities (talent and technologies), and edge computing. States should invest into research and development and applied innovative projects (also in cooperation with the private sector), leverage their role as procurer to promote selected technologies and create legal certainty for the use of new technologies. The Union has already started with the Important Projects of Common European Interest (IPCEI) tool in the field of microelectronics, or the European Network of Competence Centers in Cybersecurity under the Horizon 2020 tool.[19] In order to strengthen transparency and control possibilities of IT, but also innovation possibilities, EU legislators could oblige manufacturers and suppliers to open up technologies and achieve greater interoperability. EU member states should also examine and strengthen competition law and other instruments that level the playing field for companies on European market.

On the external dimension, Europe will need to level the playing field by adapting rules for trade, foreign direct investment, and procurement. All while safeguarding the principles of an open and competitive European economy, the EU might need to extend state-aid control beyond EU companies, support European firms with investment funds -both in the fields of research and development as well as implementation -, and strengthen its foreign direct investment screening tool.[20]

If Europe wants to retain its ability to shape its own digital future more generally, these are essential steps to take in the near future. The region's long-term command over digital technologies will perhaps be its most strategic asset and a precondition for the assertion of political and economic influence in the future.

Endnotes

1 EU NIS Cooperation Group, "EU coordinated risk assessment of the cybersecurity of 5G networks", 9 October 2019, Brussels. Retrieved from: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62132

2 Council of the European Union, "Council Conclusions of the significance of 5G to the European Economy and the need to mitigate security risks linked to 5G", 3 December 2019, Brussels. Retrieved from: https://www.consilium.europa.eu/media/41595/st14517-en19.pdf

3 European Commission, "Press release - EU-wide coordinated risk assessment of 5G networks security", 9 October 2019, Brussels. Retrieved from: https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security

4 European Commission, "The von der Leyen Commission: for a Union that strives for more", 10 September 2019, Brussels. Retrieved from: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_5542

5 Noah Barkin, "Europe's Backlash Against Huawei Has Arrived", Foreign Policy, 27 November 2019. Retrieved from: https://foreignpolicy.com/2019/11/27/europe-huawei-backlash-merkel-germany-summit/

6 Bundesnetzagentur, "Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung von personenbezogenen Daten nach § 109 Telekommunikationsgesetz – Stand 09.10.2019", 9 October 2019. Retrieved from https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/KatalogSicherheitsanforderungen/KatalogSicherheitsanforderungen2.pdf?__blob=publicationFile&v=2

7 In principle, this amounts to a "no spy clause" between vendor and network operator. In that clause, suppliers would have to assure that they are legally and effectively able to refuse the disclosure of confidential customer information to third parties. However, the "declaration" mechanism lacks any verification, enforcement or evaluation mechanisms.

8 Ellen Nakashima, „U.S. pushes hard for a ban on Huawei in Europe, but the firm's 5G prices are nearly irresistible", 29 May 2019, The Washington Post. Retrieved from: https://www.washingtonpost.com/world/national-security/for-huawei-the-5g-play-is-in-europe--and-the-us-is-pushing-hard-for-a-ban-there/2019/05/28/582a8ff6-78d4-11e9-b7ae-390de4259661_story.html

9 Moritz Koch, Dietmar Neuerer, Stephan Scheuer, „Merkel öffnet 5G-Netz für Huawei", 14 October 2019, Handelsblatt. Retrieved from https://www.handelsblatt.com/politik/deutschland/netzausbau-merkel-oeffnet-5g-netz-fuer-huawei/25107766.html

10 Wei Shi, "French parliament passes "Huawei Law" to govern 5G security", 26 July 2019, telecoms.com. Retrieved from: https://telecoms.com/498728/french-parliament-passes-huawei-law-to-govern-5g-security/. Reuters, "Italy approves use of special powers over 5G supply deals", 5 September 2019, Reuters. Retrieved from: https://www.reuters.com/article/us-huawei-tech-5g-italy/italy-approves-use-of-special-powers-over-5g-supply-deals-idUSKCN1VQ1YG

11 Noah Barkin, "Europe's Backlash Against Huawei Has Arrived", Foreign Policy, 27 November 2019. Retrieved from: https://foreignpolicy.com/2019/11/27/europe-huawei-backlash-merkel-germany-summit/

12 See: Moritz Koch, Stephan Scheuer, "Außenminister Maas stellt sich in der Huawei-Frage gegen Kanzlerin Merkel", 20 November 2019, Handelsblatt, retrieved from: https://www.handelsblatt.com/politik/deutschland/5g-mobilfunknetz-aussenminister-maas-stellt-sich-in-der-huawei-frage-gegen-kanzlerin-merkel/25244378.html; Guy Chazan, "Merkel under pressure over Huawei's role in German 5G rollout", 13 December 2019, Financial Times. Retrieved from: https://www.ft.com/content/372c1da6-1d98-11ea-97df-cc63de1d73f4;

13 Guy Chazan, "Merkel under pressure over Huawei's role in German 5G rollout", 13 December 2019, Financial Times.

14 At the time of writing, the SPD has published its position paper, the CDU/CSU has not yet published a common position. See: SPD-Fraktion im Bundestag, "Ein digital souveränes Europa mit sicheren 5G-Netzen", SPD-Position Paper, 17 December 2019, Berlin. Retrieved from: https://t.co/WxTQSFKfb5?amp=1; noahbarkin, "The CDU leadership in parliament adopted this paper on #5G yesterday evening. It is softer in key areas, paving the way (by my reading) for a #Huawei role in the German network. This is significant! Key elements:", 17 December 2019 [Twitter Thread]. Retrieved from: https://twitter.com/noahbarkin/status/1206926297357832192

15 Moritz Koch, "5G-Ausbau: Kanzleramt will vollständiges Huawei-Verbot verhindern", 17 December 2019, Handelsblatt,retrieved from: https://www.handelsblatt.com/politik/international/mobilfunkstandard-5g-ausbau-kanzleramt-will-vollstaendiges-huawei-verbot-verhindern

16 Guy Chazan, "Merkel under pressure over Huawei's role in German 5G rollout", 13 December 2019, Financial Times.

17 The following is based on parts of: Isabel Skierka, "Stellungnahme zur Anhörung des Ausschusses Digitale Agenda zum Thema ‚IT-Sicherheit von Hard- und Software als Voraussetzung für Digitale Souveränität", 11 December 2019, Deutscher Bundestag. Retrieved from: https://www.bundestag.de/resource/blob/672536/b2b63aeeaffe54e40f8c62571cc628c4/Stellungnahme-Skierka-data.pdf; European Commission, "The von der Leyen Commission: for a Union that strives for more", 10 September 2019, Brussels. Retrieved from: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_5542. Sometimes, the term is also referred to similarly as "digital sovereignty" or "digital strategic autonomy".

18 Bitkom, „Digitale Souveränität, Positionsbestimmung und erste Handlungsempfehlungen für Deutschland und Europa", 2015; Forschungszentrum Informatik, Accenture, Bitkom Research, „Kompetenzen für eine Digitale Souveränität", 2015.

19 European Political Strategy Centre of the European Commission, "Rethinking Strategic Autonomy in the Digital Age", EPSC Strategic Notes, July 2019, Issue 30. Retrieved from: https://ec.europa.eu/epsc/sites/epsc/files/epsc_strategic_note_issue30_strategic_autonomy.pdf

20 Mark Leonard, Jean Pisani-Ferry, Elina Ribakova, Jeremy Shapiro, and Guntram Wolff, "Redefining Europe's Economic Sovereignty", June 2019, European Council on Foreign Relations. Retrieved from: https://www.ecfr.eu/publications/summary/redefining_europes_economic_sovereignty

Editor

Katja Theodorakis

Publisher

Konrad Adenauer Stiftung (Australia) Limited
Regional Programme Australia and the Pacific

11/3 Sydney Avenue
Barton, ACT 2600
Australia

Tel: +61 2 6154 9322

www.kas.de/australia

Design, Layout and Typeset

Swell Design Group

Paper

ecoStar+ is an environmentally responsible paper. The fibre source is FSC Recycled certified. ecoStar+ is manufactured from 100% post consumer recycled paper in a process chlorine free environment under the ISO 14001 environmental management system.