NOTES
DE L'IFRI

NOTES DU CERFA, No. 187

JUNE
2025

The "Huawei Saga" in Europe revisited

German Lessons for the Rollout of 6G

Tim Nicholas RÜHLIG

The Study Committee on Franco-German Relations (Cerfa)

Geopolitics and Technology Center

The French Institute of International Relations (Ifri) is a research center and a forum for debate on major international political and economic issues. Headed by Thierry de Montbrial since its founding in 1979, Ifri is a non-governmental, non-profit foundation according to the decree of November 16, 2022. As an independent think tank, Ifri sets its own research agenda, publishing its findings regularly for a global audience.

Taking an interdisciplinary approach, Ifri brings together political and economic decision-makers, researchers, and internationally renowned experts to animate its debate and research activities.

The activities and publications of the Study Committee on Franco-German Relations – Cerfa – receive support from the *Centre d'analyse de prévision et de stratégie du ministère de l'Europe et des Affaires étrangères* and the *Frankreich-Referat* of the *Auswärtiges Amt*.

ISBN: 979-10-373-1056-9

Cover: Logo Huawei on the flags next to the brand's headquarters in Düsseldorf, Germany – September 22, 2024 © Alexander Fedosov/Shutterstock.com

How to quote this publication:

Tim Nicholas Rühlig, "The "Huawei Saga" in Europe Revisited: German Lessons for the Rollout of 6G", *Notes du Cerfa*, No. 187, Ifri, June 2025.

Ifri

27 rue de la Procession 75740 Paris Cedex 15 – FRANCE

Tel. : +33 (0)1 40 61 60 00 – Fax : +33 (0)1 40 61 60 60

Email: accueil@ifri.org

Website: Ifri.org

The Cerfa

The Study Committee on Franco-German Relations (Cerfa) was founded by an intergovernmental treaty between the Federal Republic of Germany and the French Republic in 1954. It is funded in equal shares by the French Ministry of Foreign Affairs and by the German *Auswärtiges Amt*. Cerfa's mission is to analyze the state of French-German relations on the political, economic, and international scales; to emphasize questions and concrete issues posed by these relations on a governmental scale; and to present proposals and concrete suggestions to increase and harmonize the relations between the two countries. This mission results in the organization of encounters and debates on a regular basis, gathering high-ranking civil servants, experts, and journalists, as well as in research activities in areas of common interest.

Paul Maurice is Secretary General of Cerfa and, together with Marie Krpata and Jeanette Süß, Fellow Researchers, as well as Hans Stark, Counselor on Franco-German relations, he is responsible for the publications of Cerfa. Catherine Naiker acts as Cerfa's assistant.

Author

Tim Nicholas Rühlig is Senior Analyst at the European Union Institute for Security Studies (EUISS), focusing on Europe-China relations, Chinese foreign and tech policy, and Hong Kong politics. His work explores China's role in global standardization, the US-China tech rivalry, and implications for Europe. Previously, he served as China Fellow at the European Commission's DG I.D.E.A., advising the President. He is also an associate researcher at the Swedish Institute of International Affairs (UI) and the founder of the Digital Power China (DPC) consortium, a European network analyzing China's digital influence.

He regularly advises EU policymakers and sits on the European Commission's High-Level Forum on Standardisation and the China Task Force of the European Standardization Organizations. He published "China's Foreign Policy Contradictions" (Oxford University Press, 2022) and chairs the high-tech working group of the CHERN network. A member of the ETNC, which he coordinated in 2018. Tim Rühlig holds a PhD from Frankfurt University and degrees in International Relations, Political Science, and Cultural Anthropology. Past roles include fellowships at the German Council on Foreign Relations (DGAP), UI, and Frankfurt University, as well as research stays in Stockholm and Beijing. He also founded China Digital Analytics for tailored policy analysis.

Abstract

This paper examines the evolving debate over Chinese telecommunications vendor Huawei's role in Europe's 5G infrastructure, focusing on Germany as a critical case study. While the European Union (EU) attempted to coordinate a collective response through its 5G Toolbox, member states diverged significantly in balancing political, economic, and technological considerations. Germany, despite its economic ties to China and status as Europe's largest telecom market, only reached a tentative agreement in July 2024—one that appears largely symbolic. The paper argues that Germany's compromise reflects persistent institutional divisions and a reluctance to decisively reduce reliance on Chinese technology, even in the face of geopolitical and security concerns. The analysis suggests that with 6G on the horizon, Europe must learn from its fragmented 5G response. A future 6G strategy should prioritize network diversity, enhanced encryption, and reduced dependency on high-risk suppliers to preserve European sovereignty and digital resilience. The paper concludes by urging a more unified and binding EU framework for managing the rollout of next-generation wireless infrastructure.

Résumé

Cette *Note* examine le débat complexe autour du rôle du fournisseur chinois de télécommunications Huawei dans le déploiement de la 5G en Europe, en prenant l'Allemagne comme étude de cas centrale. Bien que l'Union européenne (UE) ait tenté de coordonner une réponse commune via sa « boîte à outils 5G », les États membres ont suivi des approches divergentes, pris entre considérations politiques, économiques et technologiques. L'Allemagne – malgré ses liens économiques étroits avec la Chine et son statut de premier marché européen des télécommunications – n'a trouvé qu'un accord vague en juillet 2024, dont la portée semble surtout symbolique. La *Note* soutient que ce compromis reflète des divisions institutionnelles persistantes ainsi qu'une réticence à réduire de manière décisive la dépendance aux technologies chinoises, en dépit des préoccupations croissantes en matière de sécurité et de géopolitique. L'analyse souligne qu'à l'approche de la 6G, l'Europe doit tirer les leçons de sa réponse fragmentée à la 5G. Une stratégie 6G tournée vers l'avenir devrait miser sur la diversité des réseaux, un chiffrement renforcé et une moindre dépendance aux fournisseurs jugés à haut risque, afin de préserver la souveraineté européenne et la résilience numérique. En conclusion, la *Note* appelle à la mise en place d'un cadre européen plus cohérent et juridiquement contraignant pour encadrer le déploiement des futures infrastructures sans fil.

Table of contents

Introduction

"If Germany were to take a decision that leads to Huawei's exclusion from the German market, there will be consequences" – former Chinese ambassador to Germany Wu Ken[1]

The rollout of the next generation of mobile infrastructure, better known as 5G, has become the subject of political discussion across the European continent since 2018. At its core lies the question of whether the equipment of Chinese vendors, primarily Huawei, should be used, and if so, to what degree. Critics fear enormous political and security challenges. Chinese security services could infiltrate European critical infrastructure through Huawei technology.[2] Others counter that there is no evidence for such security concerns.[3] Huawei's technology is of high quality, and excluding Chinese vendors could come with huge economic costs if China decides to retaliate.[4] The threat of Ambassador Wu Ken, obviously alluding to the high exposure of the German car industry to the Chinese market, is just one of several examples of such threats.[5]

In making their decision, most member states of the European Union (EU) have weighed security, economic and technological arguments in dealing with Huawei 5G technology. Germany, Europe's largest economy, is a latecomer in this process. The German government concluded its assessment only in July 2024. Media reports suggest that it has decided to exclude Chinese vendors.[6] A closer reading of the decision suggests otherwise. This is remarkable as it continues a long naivete in Germany's dealings with critical infrastructure. Before the outbreak of Russia's full-scale invasion of Ukraine, the German government prioritized economic interests over security concerns when sourcing energy from Russia, even

1. "China Threatens Retaliation Should Germany Ban Huawei 5G", Bloomberg, December 14, 2019, available at: www.bloomberg.com.
2. D. Sabbagh and J. Henley, "Huawei Poses Security Threat to UK, Says Former MI6 Chief", *The Guardian*, May 16, 2019, available at: www.theguardian.com; T. Uren, "The Technical Reasons Why Huawei Is Too Great a 5G Risk", ASPI, June 14, 2018, available at: www.aspi.org.au.
3. "No Huawei 'Smoking Gun' in Europe, French Cyber Chief Says", Bloomberg, January 30, 2020, available at: www.bloomberg.com.
4. J. Matthes, "China-Handel 2022: Ungleichgewicht und Abhängigkeit weiter verstärkt", *Institut der deutschen Wirtschaft*, IW-Kurzbericht 9, February 9, 2023, available at: www.iwkoeln.de; M. Reynolds and M. P. Goodman, "China's Economic Coercion: Lessons from Lithuania", CSIS, May 6, 2022, available at: www.csis.org.
5. S. Kruse and L. Winther, "Banned Recording Reveals China Ambassador Threatened Faroese Leader at Secret Meeting", Berlingske, December 10, 2019, available at: www.berlingske.dk; "Ambassador Gui Congyou Gives an Exclusive Interview with SVT on 5G Issues Concerning Chinese Companies in Sweden", Chinese Embassy to Sweden, available at: www.chinaembassy.se; M. Peel and A. Barker, "China Envoy to EU Hits Out at Huawei Security 'Slander'", *Financial Times*, January 27, 2019, available at: www.ft.com.
6. "Bund verbietet Huawei-Komponenten im 5G-Netz", *Tagesschau*, July 11, 2024, available at: www.tagesschau.de.

deepening its dependencies with the Nord Stream projects. Despite this experience, Germany has not sought to reduce its dependence on Chinese mobile infrastructure. More than one year after the full-scale invasion was launched, Konstantin von Notz, member of the German parliament for the Green Party, warned: "The handling of Chinese technology appears to be just as naive as the handling of Russian gas."[7]

While Germany's National Security Strategy and its China Strategy identify the security of critical infrastructure as crucial, the market share of Chinese components in the Radio Access Network has not declined; indeed, it is expected to remain stable at around 60% at least until 2028 (see Figure 1, p. 17).

Simultaneously, the global wireless industry is already starting the process of developing and standardizing the next generation of wireless infrastructure. This forthcoming 6G network is expected to be rolled out in Europe from around 2030.

With this background, this paper revisits the discussions across Europe in general and Germany in particular to draw lessons for the rollout of 6G. This carries particular political relevance as the administration of US President Donald Trump is likely to renew its pressure on Europe to (further) reduce Chinese equipment in the network across the continent. Already during the first Trump administration, Huawei equipment was an issue of controversy in the relations between Europe and the United States (US).[8] Some of the previous threats could, however, also undermine the US's ability to influence Germany's decision. For example, then US Ambassador Richard Grenell threatened to stop intelligence sharing with Germany – a threat that turned out to be empty.[9]

To unfold this argument, this paper first summarizes the importance of 5G and 6G, explaining why mobile networks have become a subject of political discussion (1). Next, it reviews the European 5G discussion along the triad of political, economic and technological viewpoints. European countries have weighed these arguments differently and therefore arrived at different solutions with divergent effects. This contrasts with the EU's attempt at a unitary policy when developing the 5G toolbox with all EU member states (2). Turning to a specific case study, the paper delves into the German discussion since 2018 that finally led to its recently released decision (3). The paper concludes with an outlook and policy recommendations (4).

7. M. Balser et al., "Unter den Augen Chinas ", *Süddeutsche Zeitung*, March 10, 2023, available at: www.sueddeutsche.de.
8. K. Friis and O. Lysne, "Huawei, 5G and Security: Technological Limitations and Political Responses", *Development and Change*, Vol. 52, No. 5, October 2021, pp. 1174-1195.
9. "Merkel gegen Ausschluss von Huawei beim 5-G-Netzausbau", *Manager Magazin,* March 20, 2019, available at: www.manager-magazin.de.

Wireless infrastructure – the backbone of society and the economy

5G, long believed to transform our societies,[10] has not fulfilled the high expectations. It was hoped that ultra-reliable and low-latency communications (URLLC) with response times as low as one millisecond would enable close to real-time services such as remote medical surgery, self-driving cars and industry automation. Massive machine-type communications (mMTC) should connect a very large number of devices, enabling, for example, the Internet of Things (IoT), smart cities and automated agricultural processes, to name just a few use cases. While such groundbreaking applications of 5G remain in their infancy, 5G has delivered enhanced mobile broadband (eMBB) with higher data service speeds, managing more traffic as well as virtual and augmented reality (VR/AR).

In Europe, URLLC and mMTC are scarce because such functionality requires the rollout of an entirely new core network, the so-called 5G standalone (5G SA). Instead, most European network operators only "updated" the existing 4G/LTE infrastructure to a 5G non-standalone network (5G NSA). The reason that few 5G SA networks exist is that mobile operators shy away from investments that do not meet the demands of their current customers. To tap the enormous industrial potential, companies could roll out Mobile Private Networks (MPNs) on their premises. However, companies equally shy away from such investments. In addition, Europe has freed relatively little mid-band spectrum that provides for the ideal technological characteristics of wireless networks for industrial innovation.

However, the hypothetical potential of wireless network technology remains crucial. Countries such as South Korea, China and India are rolling out 5G SA, have far more MPNs contracted and have freed much more mid-band spectrum. These countries believe that, in the late phase of 5G and with the rollout of 6G, many of the use cases that experts expected with the introduction of 5G will become a reality and boost the competitiveness of their companies.

10. M. Tuerk, "How 5G Networks Will Change America", *Forbes*, February 27, 2019, available at: www.forbes.com.

Such potentials are not only an opportunity. Our societies will likely become increasingly dependent on mobile networks for critical functions across society. From industrial production to healthcare to traffic and mobility, large parts of societies and economies of the future could rely on wireless connectivity. As a consequence, society will become more vulnerable to attacks on and the malfunction of its mobile networks. The damage potential of such incidents could be catastrophic as connectedness and dependence increase.

It is with this background that Europe has controversially discussed whether it should allow Chinese vendors to participate in the rollout of its 5G critical infrastructure over the last few years.

Quo vadis, Europe? The Huawei debate revisited

To this day, the role that Chinese vendors Huawei and ZTE should play in Europe's 5G infrastructure remains controversial across the continent. Three sets of arguments for and against using Chinese vendors in 5G are particularly important: *political* arguments suggesting that Chinese suppliers should be excluded; *economic* arguments favoring the involvement of Chinese vendors; and *technical* arguments with points both in favor of and against the inclusion of Chinese suppliers.

Political sets of argument

Many critics of Chinese telecommunications equipment argue that technological (over-)dependencies on the People's Republic of China (PRC), coupled with divergences in political values, carry enormous political risks. A crucial challenge is the highly concentrated global market of the Radio Access Network (RAN) that could lead to high dependency on the Chinese tech firm Huawei. In fact, when the rollout of 5G started, many European states relied heavily, if not exclusively, on Chinese RAN suppliers (see Figure 1, p. 17). At the core of the argument is the fact that dependency on 5G vendors does not end with the purchase because mobile infrastructure requires regular maintenance that is usually supplied by the vendor.

In times of geopolitical tensions, dependency on the maintenance of critical digital infrastructure could be used to blackmail Europe and restrict the EU's freedom to act. This perspective implies that Huawei cannot be treated like any other private sector company that seeks economic profit, but should be regarded as a political tool under the control of China's authoritarian rulers.[11] Huawei has countered this view by emphasizing that the company is almost fully owned by its employees and is not a state-owned enterprise (SOE) like ZTE, another Chinese telecom vendor.

At first glance, Huawei's line of defense appears convincing. However, there are also reasons for doubt. The company is privately owned by its employees, but ownership does not necessarily come with control over the company. While there is also little reason to believe that the company has a particular interest in serving political purposes, Huawei has not only profited from party-state support, but is operating in a specific political,

11. R. Umback, "Huawei and Telefunken. Communications Enterprises and Rising Power Strategies", ASPI, Strategic Insights 135, available at: www.aspi.org.au.

legal and economic environment that makes it impossible for the company to be fully independent. As I have argued in detail elsewhere,[12] four factors suggest that Huawei could be subject to party-state control.

First, private ownership is no guarantee of independence from party-state influence. Preferential market access, state subsidies, procurement and the exercise of guidance and control through party cells are some of the mechanisms for the party-state to steer privately owned companies.[13]

Secondly, in the absence of an independent judiciary, laws do not constrain Chinese Communist Party influence but are rather a means of party control. Article 7 of the Intelligence Law enacted in 2017 and amended in 2018 requires any organization and citizen to support, assist in and cooperate in national intelligence work.[14]

Thirdly, reportedly, Huawei has profited greatly from party-state support. The *Wall Street Journal* has claimed that the company had achieved its current position by receiving as much as $75 billion in tax breaks, financing and cheap resources in the past 25 years. According to the report, Huawei profited from $46 billion in cheap loans, credit lines and other support from state lenders alone. Between 2008 and 2018, the company saved $25 billion in taxes due to state incentives to promote the tech sector. In addition, the company would have profited from cheap loans for its customers provided by Chinese banks. The China Development Bank and the Export-Import Bank of China are reported to have lent $30 billion to Huawei customers.[15] Already in 2013, Nathaniel Ahrens was pointing out the irony of the SOE ZTE having to turn to the equity markets while the privately owned Huawei relied on state funds.[16]

Fourthly, the highly complex governance structure of Huawei comes with several potential loopholes. The employees of Huawei own the company and elect representatives that steer the company. However, this Employee Ownership Plan (ESOP) is run by the trade union. Some researchers have referred to China's Trade Union Law that enshrines the leadership of the Chinese Communist Party over all trade unions.[17] It is unclear whether this also applies to ESOP. What is certain, however, is that while the Huawei employees elect their representatives to govern the company democratically, the nomination process of these representatives is not transparent. In other words, the owners of Huawei can select the

12 T. Rühlig, "Who Controls Huawei? Implications for Europe", *Utrikespolitiska institutet*, May 11, 2020, available at: www.ui.se.
13. C. J. Milhaupt and W. Zheng, "Beyond Ownership. State Capitalism and the Chinese Firm", *The Georgetown Law Journal*, Vol. 103, No. 3, 2015, pp. 665-722.
14. "PRC National Intelligence Law", *China Law Translate*, available at: www.chinalawtranslate.com.
15. C. Yap, "State Support Helped Fuel Huawei's Global Rise", *Wall Street Journal*, December 25, 2019, available at: www.wsj.com.
16. N. Ahrens, "China's Competitiveness. Myth, Reality, and Lessons for the United States and Japan. Case Study: Huawei", CSIS, February 2013, available at: https://csis-website.com.
17. "Trade Union Law of the People's Republic of China", ILO, available at: https://natlex.ilo.org.

representatives, exercising their right to control the company, only from a pre-selected choice of candidates. This could open up the possibility of party influence over Huawei.[18]

In short, the political viewpoint is concerned about the highly concentrated RAN market, the need for regular maintenance work and the resultant dependency. Critics conclude that a high degree of technological dependency could make Europe vulnerable to political blackmail from China as the Chinese Communist Party may well control Huawei.

Economic sets of argument

In sharp contrast, proponents of 5G cooperation with China rather stress two economic arguments. First, they point out that Chinese vendors have a strong self-interest in remaining a reliable economic partner delivering fail-safe technology. In fact, the reputational loss of Huawei over the last few years is illustrative of this argument. In the early 2020s, Huawei held around 20% of Europe's handset market share. In wake of security concerns, this share has dropped to around 2%. In other words, undermining trust in Huawei's products would not be in China's interest because Huawei makes good profits in Europe. In addition, Chinese firms rely on imports from the West. In 2021, 53% of Chinese imports, worth no less than €1.25 trillion, came from the West.[19]

Second, China could retaliate against European companies if EU member states excluded Chinese technology from their networks. Europe depends on the PRC economically and could suffer from Chinese economic coercion. Chinese goods account for 12.8% of all imports to Germany, for example. In the last ten years, 6-8% of German exports were bound for China.[20] Formal and informal trade restrictions against Lithuania, Sweden and the Netherlands have demonstrated that the Chinese government is willing to coerce the EU economically.[21] In theory, this could lead political decision-makers to strive to reduce dependencies on China. In practice, however, these arguments are almost exclusively put forward by those who warn of the costs of replacing Huawei network gear.

In short, from an economic viewpoint, Europe and China have a mutual interest in cooperating technologically. The PRC relies on imports and exports from Europe. It has no interest in risking its reputation and would therefore abstain from malign actions against the EU. It is in

18. "Who Controls Huawei? Implications for Europe", op. cit.
19. S. G. Iglesias and J. Matthes, "Chinas Abhängigkeit vom Westen bei Importen und Technologien", *IW-Report*, No. 15, Institut der deutschen Wirtschaft, March 2023, available at: www.iwkoeln.de.
20. "China-Handel 2022: Ungleichgewicht und Abhängigkeit weiter verstärkt", op. cit.
21. M. Reynolds and M. P. Goodman, "China's Economic Coercion: Lessons from Lithuania", CSIS, May 2022, available at: www.csis.org.

Europe's self-interest, on the other hand, to cooperate with China and avoid economic retaliation and economic coercion.

Technical sets of argument

Technical arguments, finally, have been brought forward by both proponents and critics of cooperation with Chinese vendors. Five Eyes countries' intelligence services warn of technical risks should Chinese technology be included in 5G infrastructure.

While it is not clear whether 5G is generally less secure than the current 4G/LTE networks, the complexity of 5G networks poses a new security challenge. This complexity is the result of the multitude of applications and devices that will be part of future 5G networks. This is made possible by the increased use of software-defined virtualization, which shifts sensitive operations from the core network to the edge. This makes the attack surface larger and means that a distinction between a sensitive core network technology and a less-sensitive edge and its RAN no longer applies.[22]

The sensitivity and vulnerability of 5G networks has led to fears that the participation of Chinese vendors in the deployment of 5G could come with inherent security risks. At the heart of these concerns are two fears: Chinese sabotage of and espionage through 5G infrastructure.

Sabotage is the most severe concern: China could gain access to European 5G infrastructure that would allow it to shut down the entire network, and thereby target the whole of European society and its economy. This "kill switch", as it is commonly known, would essentially undermine the availability of 5G networks that will be necessary for machine-to-machine communication as well as for self-driving cars and interconnected medical devices, such as pacemakers. It may be unlikely that China would shut down an entire 5G network and risk irreparable damage to Huawei's reputation in times of peace. However, such a kill switch could be used for partial shutdowns, accompanied by coercive threats, or used in the event of an interstate war. Chinese cyberattacks on US critical infrastructure, known as "Volt Typhoon", have reinforced such concerns. In this case, Chinese hackers have prepositioned themselves in US critical infrastructures like ports and power grids without using their sabotage capabilities yet. Instead, they check in only to see whether they still have access to the critical infrastructure that they could manipulate in case of escalated conflict with the US.

The risk of Chinese espionage alludes to a scenario in which China uses its access to 5G infrastructure for economic and political espionage on

22. T. Rühlig and M. Björk, "What to Make of the Huawei Debate? 5G Network Security and Technology Dependency in Europe", Utrikespolitiska Institutet, January 2020, available at: www.ui.se.

European companies, governments and individuals. China is already responsible for the lion's share of global cyber espionage.[23]

These two risk scenarios are feasible. Independent evaluations found software engineering and cybersecurity problems in Huawei equipment that the company was not solving quickly.[24] At the same time, there is no proof that China is using such vulnerabilities or that Huawei is designing backdoors on purpose.[25]

This lack of a smoking gun, however, should not reassure Europeans, the argument goes. 5G is a critical infrastructure. It would be reckless only to react to what has already happened without considering risks. The risks are real and severe.

In sharp contrast, proponents of technology cooperation with China argue that to tap the technological potential of 5G requires the development of highly innovative solutions. In their view, Chinese tech firm Huawei has been an innovation leader in the field. Excluding Huawei, they argue, could slow the rollout of 5G and hinder Europe's technological advance.

Unitary toolbox, divergent policies: 5G legislation in the EU

All three viewpoints show that Europeans view the issue of 5G cooperation with Chinese vendors primarily through the lens of risks: political viewpoints emphasize security risks, economic viewpoints highlight the risk of economic coercion, and the technological viewpoint is concerned with either cybersecurity or a lack of technological competitiveness. This focus on risk has led European governments to understand the value of a unified approach: a united EU is less vulnerable.

Although network security falls under the sovereignty of EU member states, they have developed a common "EU 5G toolbox", published in January 2020. [26] Simulating nine risk scenarios, the EU Network and Information Systems Cooperation Group (NIS Cooperation Group) proposed a number of measures to member states.[27] Most crucially, the EU's toolbox explicitly states that not only technological but also strategic

23. K. Kaska et al., "Huawei, 5G and China As a Security Threat", NATO Cooperative Cyber Defence Centre of Excellence, March 28, 2019, available at: https://ccdcoe.org.
24. "Annual Report", Huawei Cyber Security Evaluation Centre Oversight Board, March 2019, available at: https://assets.publishing.service.gov.uk.
25. R. Steveson, "How Huawei Became a Target for Governments", Bloomberg, January 23, 2019, available at: www.ndtvprofit.com.
26. "Cybersecurity of 5G Networks. EU Toolbox of Risk Mitigation Measures", NIS Cooperation Group, January 23, 2020, available at: https://digital-strategy.ec.europa.eu/.
27. The NIS Cooperation Group consists of representatives of all EU member states, the European Commission and the EU's cybersecurity agency, ENISA. Its task is to achieve a common understanding of threats to network and information systems across the Union. The group is vital for the exchange of information and for developing common analysis and recommendations to mitigate such risks.

(read: geopolitical) concerns should drive the European approach, which requires a combination of technological and non-technological means to mitigate. "Technical measures" are supplemented by "strategic measures" and "supporting actions". In essence, the toolbox contains:

- measures to strengthen network security by means of imposing requirements on mobile network operators, such as stricter access controls, monitoring and limitations on the outsourcing of sensitive functions and maintenance work;
- an assessment of the risk profile of vendors;
- restrictions on suppliers considered to be high-risk, including their exclusion from critical and sensitive parts of the 5G network, which explicitly includes more than just the Core Network;
- a diversification policy to include several vendors, which aims to avoid dependencies and lock-in effects with single suppliers, in particular high-risk suppliers.

Between the lines, the toolbox goes even further, particularly highlighting the effectiveness of non-technological measures. This places the EU toolbox closer to the political viewpoints mentioned above.

While the toolbox has been developed by all member states, the document is legally non-binding. Even though the toolbox reads as a rather tough statement, the member states participating in the NIS Cooperation Group have adopted different policies to implement it. Strikingly, political, economic and technical viewpoints, as discussed above, have played a role in the discussion of many states, but were weighed differently.

With explicit reference to national security concerns and focusing on *political* and *technological* arguments, Sweden decided to issue an explicit ban on Chinese technology in the rollout of critical 5G components.[28] On similar grounds, Italy and France have adopted new legislation that provides veto power not just to technological agencies, but to the offices of their heads of government. This makes the issues at stake explicitly political decisions. The Italian legislation further raises the bureaucratic hurdles for operators to use non-European suppliers' equipment – to the extent that it is increasingly uneconomic for them to choose Huawei or ZTE. France issues licenses for the usage of 5G technology for only 3-8 years, which is an incentive for French operators to purchase non-Chinese equipment that is considered less likely to be denied a license.[29]

28. "Four Companies Approved for Participation in the 3.5 GHz and 2.3 GHz Auctions", PTS, October 20, 2020, available at: www.pts.se; "Huawei to Be Removed from UK 5G Networks by 2027", UK Government, July 14, 2020, available at: www.gov.uk.
29. "Golden Power", Government of Italy, available at: www.governo.it. "Décret n° 2019-1300 du 6 décembre 2019 relatif aux modalités de l'autorisation préalable de l'exploitation des équipements de réseaux radioélectriques prévue à l'article L. 34-11 du code des postes et des communications

In other states, the *economic* frame has been resonating more, even though concerns rooted in the technological and political frames always co-exist. The most prominent example is Germany – discussed in detail below – but in Spain also this plays a prominent role:

> Spain may not be the most exposed to economic interaction with China, but we need China for our development. This is why we consider cautiously whether Huawei can be banned.[30]

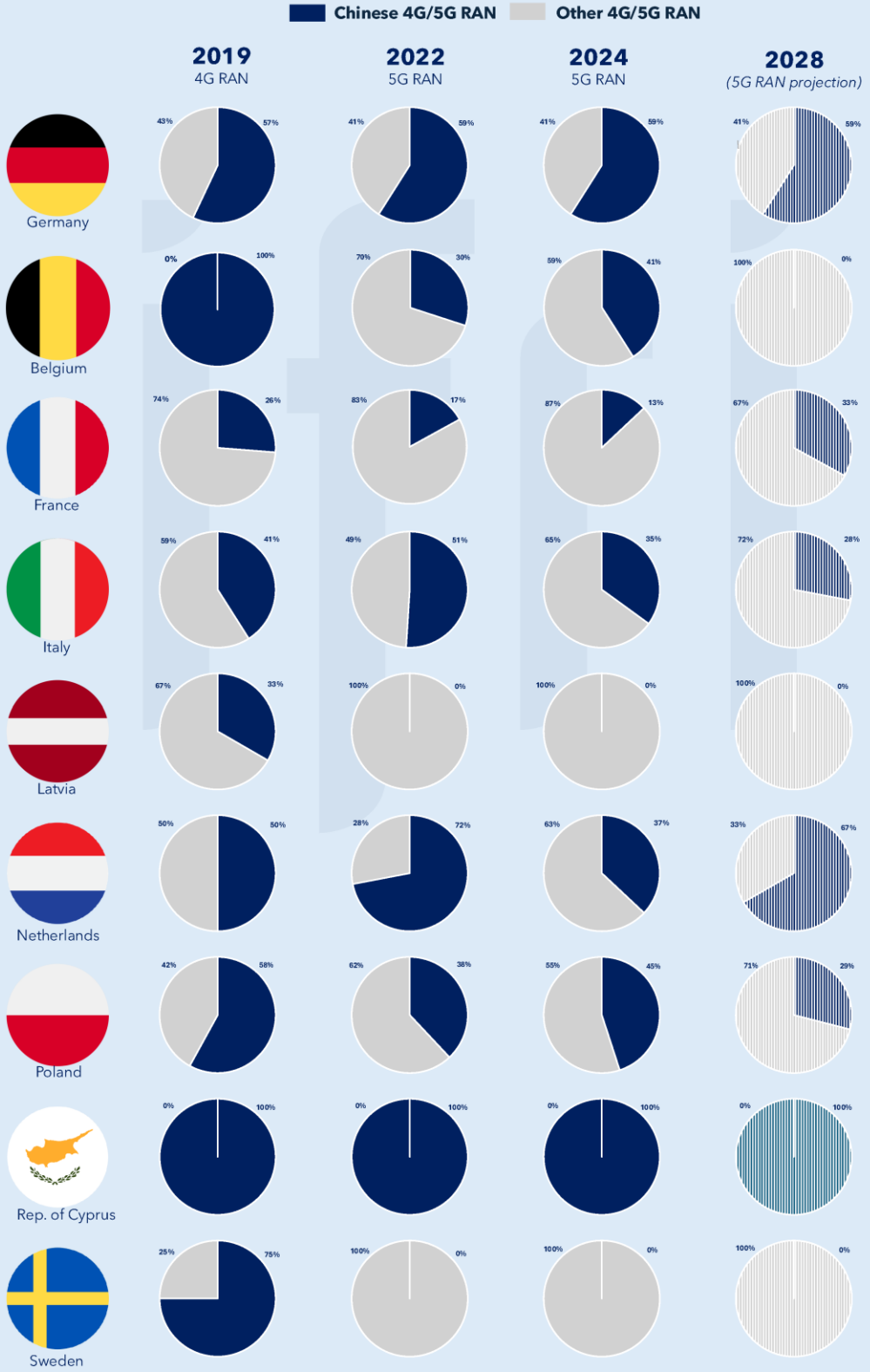
Technological and economic arguments, finally, have made Hungary remain open to Chinese 5G technology, in that digital competitiveness, both in terms of economic relations with the PRC and the high quality of Huawei equipment, is seen as crucial to Hungary's economic development. The government has further stressed that there is no evidence for the technical and political concerns outlined above.[31] In all countries, all three sets of arguments are being considered. However, these viewpoints have been weighed differently across the EU. As a result of divergent policy, the market share of Chinese vendors has developed very differently across the continent (see Figure 1, p. 17).

électroniques", Government of France, December 6, 2019, available at : www.legifrance.gouv.fr; "LOI n° 2019-810 du 1er août 2019 visant à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles (1)", Government of France, August 1st, 2019, available at: www.legifrance.gouv.fr; F. Ghiretti, "Europe's Manoeuvring on 5G Technology. The Case of Italy", IAI, September 24, 2020, available at: www.iai.it.

30. Anonymous author interview with a Spanish telecommunications regulator, February 2025.

31. G. Szakacs and K. Than, "Hungarian Minister Opens Door to Huawei for 5G Network Rollout", Reuters, November 5, 2019, available at: www.reuters.com.

Figure 1: Share of Chinese equipment in 4G/5G RAN



Source: Strand Consulting (2025).

Three viewpoints in practice

Germany is, for several reasons, a particularly important case. It is not only the biggest telecommunications market within the EU, with more than 100 million mobile phone subscriptions, but the country is also deeply interwoven with the Chinese economy. German-China trade accounts for around one-third of the total of EU-China trade. In telecommunications, Germany is considered a leading market in Europe, with around 173 million mobile connections.[32] For years, politicians and regulators were waiting for a decision on Huawei to be taken in Berlin. In an anonymous interview, a high-ranking telecommunications official from a northern European country said:

> In the end, it does not matter what we decide. We are all watching Germany. If the Germans keep the market open for Huawei, the rest of the continent will follow. If Germany bans Chinese vendors, there will be effectively no business for Huawei in the entirety of Europe anymore.[33]

This assessment proved to be wrong. Germany was no trendsetter in Europe – not because its decision was ignored by the rest of the EU, but because Germany did not come to a conclusion for a long time. While most other EU member states took legislative action of some sort, Germany adopted only a mostly procedural amendment to its IT Security Act in 2021, which remained largely indecisive on the Huawei question. Only in July 2024 was the issue directly addressed when the German government signed an agreement with the three mobile operators Deutsche Telekom, Vodafone and Telefonica (see below). And whether this solution is going to last remains to be seen.

How did the "Huawei story" unfold in Germany? To understand this, a brief review is required.

It all began in summer 2018, when Australia announced the exclusion of Chinese providers from the rollout of its 5G infrastructure. In the weeks and months to follow, more countries adopted similar measures, including the US. Only weeks after the Australian decision, Huawei representatives in Berlin sought assurance from the German government that it would not even consider an exclusion:

---

32. "The Total Mobile Subscriptions of Telecom Industry in Germany (2020 - 2028, Thousand)", Global Data, available at: www.globaldata.com.

33. Anonymous author interview with a high-ranking telecommunications official from a northern European country, November 2019.

> Huawei was very quick to contact us. They understood very well the potential damage to their business interests in Europe and identified Germany as their most important market in the EU. At that time, we were not foreseeing what was about to come. Our mobile operators characterized Huawei as a reliable partner. Therefore, we saw no reason to think of a ban.[34]

In October 2018, the German government replied to a request from the Green Party in the German parliament: "A concrete legal basis to completely or partially exclude a specific provider from 5G expansion in Germany does not exist and is not planned."[35] Instead, the German government adopted a rather technical approach. In March 2019, it published a list of key security requirements for future networks, which begins with the requirement that "[s]ystems may only be sourced from trustworthy suppliers whose compliance with national security regulations and provisions for the secrecy of telecommunications and for data protection is assured". The document also included the requirement for more extensive auditing and certification of network technology. In a quite detailed manner, it also listed additional security measures such as data traffic control and transparent software deployment. Moreover, it emphasized the need for redundancy in mobile networks and formulated the aim to avoid "monocultures" by "using network and system components from different manufacturers". However, none of these measures is legally binding.[36]

In parallel, Germany's largest mobile provider, Deutsche Telekom, anticipated the potential for more political disruptions due to US export controls and sanctions. It concluded a non-public contract with Huawei to stockpile Huawei components that involved US technology licenses in Europe. According to the contract, spare parts were to be "stored and managed in Huawei's European warehouses," and individual Huawei devices were even delivered to Telekom as a precaution.[37] This not only contrasts with the federal government's assessment of the situation but is remarkable because the federal government holds around 30% of the Deutsche Telekom shares.

In the months and years that followed, the controversy surrounding Huawei also reached the political elite of Germany. The positioning blurred party lines, with some politicians from both center-right and center-left parties opting for and against the inclusion of Huawei. Neither the Christian Democratic Union (CDU) of then-Chancellor Angela Merkel and

34. Anonymous author interview with a German ministry official, January 2022.
35. "Warum Deutschland mit China hadert", *Deutsche Welle*, November 15, 2018, available at: www.dw.com.
36. T. Rühlig et al., "5G And the US–China Tech Rivalry – A Test for Europe's Future in the Digital Age", Stiftung Wissenschaft und Politik, June 2019, available at: www.swp-berlin.org.
37. P. Alaveres de Souza Soares et al., "Deutsche Telekom sicherte sich gegen US-Sanktionen ab", *Handelsblatt*, March 28, 2023, available at: www.handelsblatt.com.

its sister-party in Bavaria, the Christian Socialist Union (CSU), nor the Social Democratic Party (SPD) or the Free Liberal Party (FDP) adopted a united and coordinated stance. Even an attempt to form a consensus within the CDU/CSU group in the German parliament was rather a compromise formula after heated discussions that different factions of the political parties continued to interpret differently.[38] The Green Party is the only major political force in Germany that has consistently advocated decisive measures to reduce if not completely ban Huawei from German 5G networks.

At one end of the spectrum, the mobile network operators, together with the management of the Federal Office for Information Security (BSI) as well as the Chancellery and the Ministry of Digital Infrastructure and Transport, opted for including Huawei in the rollout.[39] A particularly prominent voice has been Transport Minister Volker Wissing (formerly FDP). Others were skeptical, including the Federal Foreign Office, Germany's intelligence agencies and politicians from almost all political parties. The most prominent and vocal voice has been Norbert Röttgen (CDU), former chairman of the parliament's foreign affairs committee:

> We have seen what consequences it can have if we are no longer able to manufacture simple products such as face masks, but are dependent on countries such as China. All the more reason why we should now insist that we do not make ourselves dependent on companies that are at the mercy of Chinese state influence when it comes to the critical infrastructure par excellence, namely our 5G digital nervous system.[40]

Röttgen did not make himself popular with everyone. In an anonymous interview, a staff member of the CDU/CSU group said:

> "… many colleagues are annoyed by his [Röttgen's] position because he sounds like there is only one security concern of Germany relevant for deciding this issue. But this is not just about network security but also the security of our economy and the rollout of 5G. We need to carefully consider the pros and cons of the different options we have. Press statements like his are not helpful."[41]

In the discussion that unfolded across the political spectrum in Berlin, political, economic and technological viewpoints, as outlined above, have all played a major role.

38. CDU/CSU Fraktion im Deutschen Bundestag, *Deutschlands digitale Souveränität sichern. Maßstäbe für sichere 5G-Netze setzen*, Berlin, Unions Fraktion im Bundestag, 2020.
39. The BSI is Germany's federal agency in charge of IT and network security. It is an independent agency under the Ministry of the Interior.
40. "Röttgen gegen Huawei-Beteiligung bei deutschem 5G-Ausbau", *Handelsblatt*, May 17, 2020, available at: www.handelsblatt.com.
41. Anonymous author interview with a CDU/CSU staff member, January 2022.

To begin with, the Federal Office for the Protection of the Constitution (Bundesamt für Verfassungsschutz), Germany's counterintelligence agency, has warned frequently about using Huawei network gear. For example, the vice-president of the agency warned of cooperating with companies that could be subject to strong party-state influence. He added that his agency saw "a problem" with Deutsche Telekom's heavy reliance on and cooperation with Huawei.[42] As he was referencing dependencies and the close ties of Huawei to the party-state, these statements are a clear case of a political argument, as outlined above. Another example is Reinhard Brandl (CSU). He went as far as criticizing Interior Minister Nancy Faeser (SPD) for "giving a free hand" to the Chinese Communist Party.[43]

Commenting on a revised version of the IT Security Act of 2021, Falko Mohrs (SPD) explicitly identified political trustworthiness as a crucial criterion that the German parliament had negotiated into the revised law:

> The fact that we have a trustworthiness check and that we also consider information obtained by security services and the Federal Intelligence Service [are inscribed in the IT Security Act…] to assess whether a manufacturer is to be considered problematic is the result of parliamentary pressure. The SPD and parts of the CDU have made it clear that we do not want to compromise on security.[44]

Mohrs' remarks highlight the importance of vendor trustworthiness, as outlined above, as one of the political sets of arguments.

Equal to such considerations, concern about economic retaliation has played a vital role in the German discussion. Considering the risk of economic decoupling as a result of growing political distrust, then Economics Minister Peter Altmaier (CDU) argued against excluding Huawei: "What will happen if other countries say: I don't trust French wine?"[45]

Jens Zimmermann, a member of parliament for the SPD, has put forward a more sophisticated defense, arguing that supply chains in mobile infrastructure technology have become transnational. In his view, it is almost impossible to do without Chinese components.[46] Following this logic, an exclusion of Huawei and ZTE would undermine critical supply chains and thereby endanger Germany's economic and technological development.

42. D. Neuerer, "Verfassungsschutz sieht Huawei-Verbindung zu Telekom und Bahn kritisch", *Handelsblatt*, March 3, 2023, available at: www.handelsblatt.com.
43. D. Neuerer, "Deutschlands oberste Cybersicherheitsbehörde setzt Huawei-Technik ein", *Handesblatt*, April 5, 2023, available at: www.handelsblatt.com.
44. J. Kuhn, "Streit um die 'Lex Huawei'", *Deutschland Funk*, December 18, 2020, available at: www.deutschlandfunk.de.
45. T. Benner, "5G und Huawei: Anatomie eines Politikversagens", *Internationale Politik*, July 23, 2024, available at: https://internationalepolitik.de.
46. "Deutschlands oberste Cybersicherheitsbehörde setzt Huawei-Technik ein", op. cit.

Beyond mere party politics, Huawei's embedding into German research and economic structures has also created economic incentives to maintain the Chinese tech company's presence in Germany's mobile infrastructure. For example, Munich is home to Huawei's European research center, which is not only highly innovative, measured by the number of patent applications, but an important employer. Around 450 highly qualified researchers work in the center.[47]

Huawei's technological expertise has been opening doors for the company. German universities such as RWTH Aachen and research institutes such as the Fraunhofer-Gesellschaft are keen to cooperate. This creates not only trust but also a sense of research and economic dependency:

> There can be no denial: Huawei has become an integral part of our economic and technological ecosystem in Germany. [...] They are cooperating with many [German] researchers and are part of the industry associations.[48]

In fact, Huawei is an active member of clubs and associations, contributing to working groups and expert committees. For example, Huawei co-leads the "Communication Technologies Working Group" at the digital association Bitkom.[49]

Interestingly, the BSI has put forward a combination of economic and technological arguments to justify its opposition to a ban on Huawei technology. In 2019, Arne Schönbohm, then BSI president, argued that it was "irrelevant" for risk management whether a component was fabricated in China, Korea or Sweden. To this technological argument, he added:

> "If political trust alone is to be the basis for investment decisions, then we are destroying the division of labor that we have in the world, the basis of our economic prosperity."[50]

Following from this logic, the BSI is not only against a ban of Huawei but is using the Chinese technology for its in-house communication networks.[51] Ever since, the BSI has been less vocal publicly, but interviews suggest that it remains one of the actors that is more skeptical of restrictions on Chinese vendors.

The mobile operators, in turn, have mostly used technological arguments to support Huawei. In November 2019, Telefónica wrote a letter to members of the German parliament warning of the consequences of a

47. "Huawei", 6GTimes, available at: www.times6g.eu.
48. Anonymous author interview with a representative of the Federal Ministry for Education and Research, May 2024.
49. "Arbeitskreis Kommunikationstechnologien", Bitkom, available at: www.bitkom.org.
50. "Wirtschaftsspionage ist kontrollierbar", *Frankfurter Allgemeine Zeitung*, August 7, 2019, available at: www.faz.net.
51. "Deutschlands oberste Cybersicherheitsbehörde setzt Huawei-Technik ein", *op. cit.*

possible exclusion of Huawei.[52] The then head of Vodafone Germany, Hannes Ametsreiter, further argued that "excluding Huawei would lead to the 5G rollout being delayed by up to five years".[53] Similarly, Deutsche Telekom has warned of an impending "Armageddon" scenario should Huawei be excluded from the 5G rollout. This is a remarkable assessment as Deutsche Telekom's US subsidiary in the United States has successfully rolled out 5G from the very beginning without any Huawei technology.

United in opposition against a possible ban on Huawei, the three mobile operators have repeatedly threatened the German government with a demand for compensation if they have to replace existing Huawei components.[54]

Bavarian Prime Minister Markus Söder (CSU), in turn, has questioned the quality of non-Chinese alternatives to Huawei, thereby considering Chinese technology as effectively having no alternative:

> The current discussion about Huawei and 5G shows how we are doing: In the past, it would have been quite clear that Germany would go for a Siemens network, but now we have to choose between difficult alternatives. We need our own expertise again."[55]

This statement is remarkable; Söder neglects the fact that two global wireless infrastructure manufacturer champions are European – Sweden's Ericsson and Finland's Nokia. A similar misrepresentation is found in Alexander Graff Lambsdorff's argument that "it would be the best if we had a European champion. For this, we would need a bit longer to get it all done."[56] Graff Lambsdorff, who is now Germany's ambassador to Russia, was not only a member of the German but also the European parliament. Similarly, Minister Wissing implied that an exclusion of Huawei would have led to a supply shortfall of 5G in Germany. Defending the government's decision of July 2024, he argued: "It was important to us that there would be no loss of mobile coverage for the population and that the 5G expansion would not come to a standstill."[57]

The argument that not using Huawei would lead to the risk of worse quality in later deployment of 5G has also been part of Minister Faeser's defense line. In July 2024, she argued that other countries that had taken a

52. T. Benner, "Seven Lessons from the German 5G Debate", Heinrich Böll Foundation, December 30, 2021, available at: https://il.boell.org.
53. "Warnung vor Huawei-Ausschluss bei 5G", *Süddeutsche Zeitung*, October 30, 2020, available at: www.sueddeutsche.de.
54. "Mit allen juristischen Mitteln Huawei Rip-out verhindern", Golem, March 12, 2023, available at: www.golem.de.
55. "'An der Schwelle zur blockierten Republik'", *Die Welt*, January 17, 2020, available at: www.welt.de.
56. "Kritik an Huawei ist verboten (Lutz van der Horst)", *ZDF heute show*, March 29, 2019, available at: www.youtube.com.
57. "Chinesische Bauteile sollen aus deutschem 5G-Netz verschwinden", *WirtschaftsWoche*, July 11, 2024, available at: www.manager-magazin.de.

less cooperative approach in dealing with the Huawei question had to contend with "serious consequences for the population" in terms of access to mobile infrastructure.[58]

However, technological risks of espionage and sabotage have also been cited against Huawei in the German discussion. One example is an expert hearing in the parliament's foreign affairs committee that discussed the risk of sabotage and espionage:[59]

> We are sincerely concerned about network security in Germany. We have plenty of experience with Chinese espionage and we keep discussing the growing risks to the availability of critical digital infrastructure. For good reason do we identify China as a systemic rival to Europe. And therefore, we need to address such serious risks stemming from a Chinese technology firm.[60]

In short, political, economic and technological viewpoints as outlined above have shaped the German discussion, with different actors highlighting and prioritizing competing arguments. This has prompted Germany to search for a compromise formula to meet these different arguments – which is typical for Europe. What is specific in Germany is that all viewpoints have remained strong and prevented the country from taking a clear decision.

In 2021, the government appeared to have found such a compromise formula when the German parliament adopted the revision of the country's IT Security Act. At its core, the new version of the law includes a consultation mechanism between the different ministries and agencies to assess the risks. If there is no agreement by consensus at the working level, it escalates to the political level. Huawei could only be excluded if the Ministry of the Interior, the Ministry of Foreign Affairs, the Ministry of Economic Affairs and the Chancellery jointly agree to it. In essence, this did not settle the discussion in substance but rather established a procedural approach, postponing the actual decision.

According to Section 9b of the revised law, vendors must also provide a guarantee declaration. This applies regardless of where the manufacturer is based, i.e., also for Chinese manufacturers. The suppliers must guarantee in advance the trustworthiness of their "critical" products. This is done by a plain declaration. If such guarantee declarations prove to be incorrect or even false after verification, this can lead to sanctions and the exclusion of a manufacturer.

58. "Chinesische Bauteile sollen aus deutschem 5G-Netz verschwinden", op. cit.
59. "Experten gegen Ausschluss von Anbietern beim Mobilfunkstandard 5G", Deutscher Bundestag, March 13, 2019, available at: www.bundestag.de.
60. Anonymous author interview with a German ministry official, October 2023.

All these are only soft guarantees. In essence, the IT Security Act did not answer the delicate question of whether to include Huawei or not. Konstantin von Notz, a German MP from the Green Party, therefore argued:

> The problem with what the coalition government has now done is that it has basically postponed the decision until after the general election. It has not clarified the criteria and obfuscated the conflict between the German telecommunications industry and those who are quite critical of China.[61]

Following this IT Security Act, the BSI began its certification program for 5G components in July 2022. According to German media reports, the BSI's examination did not reveal any technical evidence of hidden backdoors in Huawei components. With the BSI's ongoing certification program, the dispute over Huawei technology was considered to be over. However, this turned out to be a false assumption. Critical press reports remained part of the publication discussion – even if less frequent.[62] Following a visit by Chancellor Olaf Scholz (SPD) to the US in March 2023, the Federal Ministry of the Interior took up the initiative again. It sent an email to the three mobile network operators requesting a list of all Huawei components in the mobile infrastructure. In its email, the ministry cited fears of a possible impairment of public security.[63]

Compared to Germany's previous actions and discussions, the Ministry of the Interior adopted tough language. In an internal paper of September 2023, the BMI even spoke of "considerable structural dependencies on Huawei" in the public 5G networks, which would result in an "urgent need for action" from a legal perspective: "A complete and immediate prohibition of all Huawei and ZTE components would take full account of security policy concerns, but according to current knowledge would result in considerable restrictions on network operation," the ministry wrote.[64]

Compared to such tough language, the action that the German government took in July 2024 was rather minimal. Instead of a revision of the law, it concluded a "public law contract" with the network operators, the details of which are kept secret. The main points enshrined in the contract are, however, publicly known.[65] The compromise between different ministries contains a two-step process:

61. "Streit um die 'Lex Huawei'", op. cit.
62. Of particular relevance has been the coverage by *Handelsblatt* journalist Dana Heide, who has critically assessed and questioned government policies and their implementation on a regular basis.
63. "Mit allen juristischen Mitteln Huawei Rip-out verhindern", op. cit.
64. "5G und Huawei: Anatomie eines Politikversagens", op. cit.
65. "Stärkung der Sicherheit und technologischen Souveränität der deutschen 5G-Mobilfunknetze: Bundesregierung schließt Verträge mit Telekommunikationsunternehmen", Bundesministerium des Inneren, July 11, 2024, available at: www.bmi.bund.de.

- By 2026, the network operators Deutsche Telekom, Vodafone and Telefónica have to remove all critical components supplied by Huawei and ZTE from their Core Networks.
- By 2029, the operators have to remove Huawei and ZTE technology providing critical functionality to the management and control layer of the Radio Access Network (RAN).

The German government framed the decision as a decisive step to increase Germany's network security. This rhetoric is at least surprising. A closer examination of the government's decision shows that it has little effect on network security.

Its mention of "critical components" and "critical functions" references the "List of Critical Functions". According to the list, the entire Core Network, as well as the network management, is critical, but the RAN (GNodeB) is not. Already before the contract was signed, the Core Network of Germany's public wireless infrastructure was almost entirely free of technology provided by high-risk vendors. Huawei has not been awarded any of the contracts for the core network concluded in recent years. Only Telefónica still has residual Chinese shares in the core network. The company had planned to remove it long before the contract with the German government was signed. Therefore, the first of the two steps mentioned in the decision is purely symbolic, with close to no practical impact and no cost to the operators. Non-public networks contain a significant share of Huawei technology in the Core Network (e.g., Deutsche Telekom Enterprise's network) and are not affected by the decision.

In step two, the operators have to remove Chinese technology from the management and control software of the antennas and access network. This only affects the operating support system. In other words, no hardware needs to be replaced, only software.

Furthermore, the decision only mentioned 5G technology. By the time the decision affects the RAN, Germany will have transitioned from 5G to 6G. While one could assume that the decision also applies to future generations of wireless technology (and this is the understanding of senior government officials, according to private conversations), the German government's public statement refers only to 5G.

The German government further agreed with the operators to create an "Alliance for Open Interfaces", comprising the government, all operators and industry partners (including wireless technology vendors) to jointly develop solutions for implementing and promoting the objectives agreed in the contracts. The forum is intended to establish a structured dialogue on open interfaces, 6G standards, network protection, and information and cybersecurity. What may sound like a rigorous solution could allow the continued use of Chinese-developed software in Germany's RAN beyond 2029 (see below).

The complete rip and replace of Chinese technology, which was advocated by several ministries (Ministries of the Interior, Economics and Climate and the Federal Foreign Office), at least in particularly sensitive locations such as Berlin and sites of NATO and the German Armed Forces, is off the table.

In sum, the German decision does not lead to any significant change in the German wireless market and will therefore not significantly increase its network security. In this context, it is important to note that the RAN software that runs on the basebands provides for strong control capabilities. The dominant interpretation is, however, that the German compromise does not require the replacement of baseband RAN software. If this interpretation is correct, the security gain is very limited because only removing the operation service system and/or the Network Element Management layer, but not the full RAN software, leaves decisive control functionality to be run by Chinese software.

The economic interests of the operators as advocated by the Ministry of Digital and Transport have trumped reasonable security considerations as voiced by the Ministries of the Interior, Economics and Climate Action, Defense and the Federal Foreign Office. The Ministry of Digital and Transport repeated Deutsche Telekom's argument that a more comprehensive replacement of Huawei technology would be too costly and time-consuming, thus affecting the already deficient rollout and quality of German mobile infrastructure.

The success of this argument is remarkable, as several EU member states have drastically reduced the market share of Chinese vendors in their RAN market without such consequences (see above). Granted, other member states reduced the market share as part of the 5G rollout when equipment had to be replaced in any case. However, it is hardly convincing that Germany could not afford any significant replacement within the next 4-5 years when other member states took much more drastic measures within only two years.

The decision within the German government was decisive, as the Chancellery sided with the Ministry of Digital and Transport. The Chancellery mostly referenced legal liability as a reason for its position. It was feared that network operators could demand compensation from public authorities in court if they had to replace Huawei network gear. Notably, other ministries, including the Ministry of Justice, do not share these legal concerns. Most likely, the general concern about worsening economic relations with China at times of uncertainty before the US presidential elections had taken place, along with major economic challenges resulting from Germany's decoupling from Russian fossil fuels, could also have shaped the Chancellor's assessment.

However, the decision could be amended long before 2029. The new Trump administration might put pressure on Germany, or the new CDU-led German government could put a tougher decision in place. Ironically, however, the government's decision has increased the legal risk for the German government to be held liable for the costs of potential future decisions because operators now have a contractual basis they can refer to if they want to challenge any further tightening of rules in the coming years.

The Huawei saga in Germany might not be over yet.

Moving towards 6G: outlook and policy recommendations

This paper demonstrates that Europe has adopted very different approaches to the role of Huawei in its critical 5G infrastructure – despite the existence of a unitary 5G toolbox in the EU (see Figure 2, p. 30). Three sets of viewpoints – political, economic and technological – have been weighed differently across the continent. Even within EU member states these arguments have been controversially discussed. In Germany, finding a trade-off between them took until July 2024 – and the new government might reconsider this decision.

The review of these experiences carries enormous relevance for the EU. As 5G has not lived up to its potential, 6G will be introduced in the early 2030s and could reach the systemic relevance that 5G was supposed to achieve. Hence, more than 5G, the EU will be faced with the question of the security of its mobile infrastructure. It is also not unlikely that the Trump administration will renew its pressure on Europe to remove Chinese network gear from its infrastructure.[66] At the same time, the case of Germany illustrates that the effectiveness of US pressure should not be overestimated. Neither US pressure nor its attempts to convince Germany have been decisive for Germany's course; it has resisted demands from Washington DC. This is even more remarkable as the country's National Security Strategy and its China Strategy clearly reflect the risks resulting from infrastructure dependencies. The case of Nord Stream and the reliance on Russian fossil fuels has further proven that such risks are real.

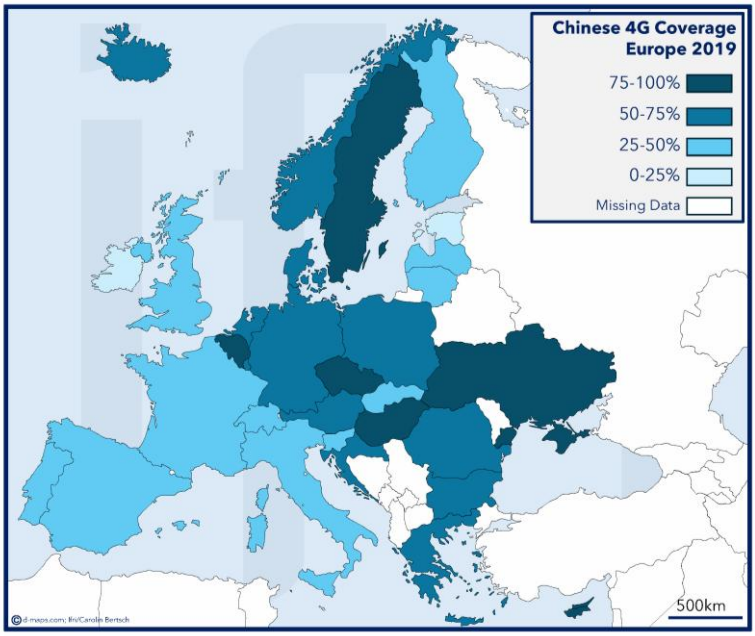
The EU and its member states are faced with enormous risks that it can best address in unity. Reducing dependency, fending off economic coercion and generating network security will be easiest if Europe adopts a unitary approach. A 6G toolbox should therefore provide less room for divergent implementation than the 5G toolbox. A new 6G toolbox should be clearer in its recommendations. Ideally, the EU member states would commit in a legally binding way to implement the toolbox agreed upon, but this is highly unlikely.

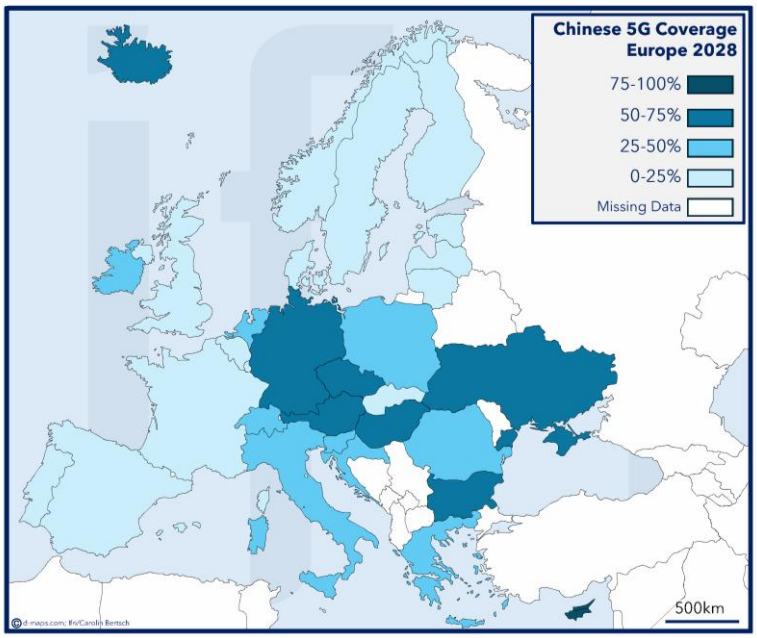
Strikingly, a total ban on Huawei might not be necessary. To increase network security, other means are more effective. Network redundancy and diversity are the best means of mitigating sabotage risks. Encryption

66. M. Valliet, "Convince and Coerce: U.S. Interference in Technology Exchanges Between its Allies and China", *Étude de l'Ifri*, Ifri, February 2022, available at: www.ifri.org.

is most useful to avoid espionage.[67] However, the further reduction of dependencies on Chinese technology will be critical in order to maintain Europe's sovereignty.

Figure 2 – Chinese 4G Coverage Europe 2019, and Chinese 5G Coverage Europe 2028





67. "What to Make of the Huawei Debate?", *op. cit.*

Latest publications of Cerfa

- J. Ross, N. Téterchen, The Franco-German Brigade and the Revival of European Defense, *Ifri Memos*, April 8, 2025 (available in French and German)
- M. Krpata, Friedrich Merz and the Zeitenwende 2.0. A "New Era" for Transatlantic Relations?, *Notes du Cerfa*, No. 186, March 2025 (available in French and German)
- A. Lensing, The German Greens as an Alliance Party: The End of an Illusion?, *Notes du Cerfa*, No. 185, March 2025 (available in French)
- V. Dubslaff, The Rise of the AfD and the Choice of Radicalism, *Notes du Cerfa*, No. 184, March 2025 (available in French)
- J. Süß, The Liberal Democrats in the German Federal Elections: A Party Fighting for Survival, *Notes du Cerfa*, No. 183, March 2025 (available in French)
- N. Batteux, The SPD in the Run-Up to the 2025 General Election: from Chancellor's Party to Junior Coalition Partner?, *Notes du Cerfa*, No. 182, March 2025 (available in French)
- M. Baloge, The CDU in the 2025 Elections: A Road to the Chancellery, Paved with Challenges, *Notes du Cerfa*, No. 181, March 2025 (available in French)
- P. Maurice, Germany in the Electoral Campaign to the Early Elections on February 23 - The Challenges of a high-risk Voting, *Ifri, Editorial*, January 2025 (available in French)

27 rue de la Procession 75740 Paris Cedex 15 – France

Ifri.org