# Non-Decision Decisions in the Huawei 5G Controversy

## Policy in Japan, the United Kingdom, and Germany

*The Chinese company Huawei has presented the governments of several middle powers with a policy dilemma. On the one hand, Huawei's affordable 5G network technology is attractive to telecommunications operators in these countries, which do not have domestic producers of this equipment. On the other hand, the U.S. government and intelligence agencies in other countries maintain that Huawei gear presents intolerable network security risks, a charge that the Chinese government and Huawei forcefully reject as they insist Huawei deserves access to foreign markets. Facing the question of whether and how to allow the installation of Huawei's 5G equipment in their domestic networks, the governments of Japan, the United Kingdom, and Germany have been caught between the competing demands of the two rivalrous superpowers and faced internal divisions among communities of government experts. At first glance, Japan, the UK, and Germany each appear to have responded to the Huawei dilemma in a different way. The Japanese government moved quickly and without formal announcement to exclude Huawei from its market, while publicly denying a ban. The UK government initially allowed Huawei to supply some of its national 5G infrastructure, but then reversed itself to ban the company's equipment outright after a U.S. regulatory change. The German government has yet to officially ban Huawei, but has taken successive steps to curtail the Chinese company's continued involvement in its domestic networks. In spite of their apparent differences, the three national responses to the Huawei dilemma share a fundamental commonality: all amount to "non-decision decisions" on the question of whether and how to allow Huawei to supply domestic 5G networks. That is, in one way or another, each government avoided making an explicit, definitive, and singular policy decision on the issue. After developing the concept of a "non-decision decision," we explain why these maneuvers are not isolated responses to a specific policy conundrum, but may presage a mode of middle power coping with competing demands from two increasingly rivalrous superpowers.*

## Introduction

Since the end of the Cold War, middle powers[1] across North America, western Europe, and Pacific Asia have sought to steer a course between leaning toward the United States and the People's Republic of China (PRC). For the most part, they have managed this delicate feat in spite of fluctuating tensions between the two superpowers. For at least the first two decades of the post-Cold War period, U.S.-allied or U.S.-aligned middle powers maintained or even enhanced their security relationships with the United States. After 9/11, these multi-facetted security

[1] We use "middle powers" as an analytical convenience, recognizing the designation to be imperfect and contested. By "middle powers" we mean major economic and security powers, roughly coterminous with the membership of the G20, that are neither China nor the United States, two states whose outsize economic and security roles earn them the distinction of "superpowers."

partnerships came to include more substantial intelligence sharing and later evolved to encompass new activities, such as joint freedom of navigation operations in the disputed waters of East Asia. At the same time, these middle powers expanded trade relations with an increasingly prosperous PRC. For many of these countries, the PRC became both an indispensable source of critical goods, such as pharmaceutical inputs, and an important destination for exports, ranging from iron ore to automobiles. Despite ups and downs in the complex U.S.-PRC relationship, these middle powers have grown into both long-standing security partners to the United States and significant trade partners to PRC.

Today, middle powers navigating these dual roles face new dilemmas. As the U.S.-PRC rivalry has intensified, the position that middle powers have carved out relative to the superpowers has grown from a source of opportunity into a constraint. They now face choices that present more difficult trade-offs between incompatible U.S. and PRC demands on specific policy issues. As U.S.-PRC differences have grown beyond traditional trade issues to encompass the security implications of new high-technology products and services, the superpowers' demands on middle powers have also come to include insistence on their adoption of specific domestic technology policies.

In this article, we examine how three middle powers have confronted such dilemmas through a study of their responses to the prospect of the Chinese company Huawei supplying their domestic 5G networks. We investigate how Japan, the United Kingdom, and Germany each responded to the dilemma arising from Chinese pressure to allow Huawei's 5G equipment into their markets and U.S. pressure to ban these very same products from their networks.

All three countries have had reason to prioritize maintaining or even strengthening trade relations with the PRC. All three are also U.S. allies for whom continued security and intelligence cooperation with the United States has been important. Moreover, both the UK and German governments have contended with domestic technology experts divided in their assessments of Huawei's equipment and the security risks it poses. In this sense, the Huawei dilemma has presented these middle-power governments with the challenge of navigating not only competing external demands, but also divided domestic constituencies and communities of experts engaging a new policy domain.

At first glance, each country appears to have responded to the Huawei dilemma with its own distinct approach. Japan acted early to restrict Huawei's role in supplying 5G technology while publicly denying that it was doing so. The UK at first allowed Huawei's limited participation, but then reversed itself for what it characterized as technical reasons beyond its control. Germany has not explicitly banned Huawei, but it has increasingly tightened conditions on the use of its products so as to make Huawei's participation ever more unlikely in practice.

The differences between these three responses conceal more important similarities. In spite of variation in the form and timing of their approaches, all three governments have in effect imposed or approach imposing a complete ban on Huawei's 5G equipment. Moreover, all three governments arrived at this outcome by avoiding an explicit decision to definitively exclude Huawei. In this respect, all three cases illustrate a consequential instance of a "non-decision

decision," which we define as a decision that avoids an explicit, definitive, and/or singular selection of one discrete policy option over others. A non-decision decision is one that a government makes in a tacit or implicit fashion – without formal declaration. For a middle power caught between the competing demands of two rival great powers, a non-decision decision may be a least-worse course of action, since it avoids an identifiable policy choice that would be unfavorable to either great power and risk inviting its retaliation. This paper traces the three countries' responses over time, proposing an explanation for their underlying common non-decision decision to adopt a de facto long-run complete ban on Huawei 5G equipment. After developing the concept of a non-decision decision, we situate this mode of policymaking against trends in relations between great and middle powers in the age of securitized technology and discuss its implications.

## The Huawei policy challenge

The governments of Japan, the UK, and Germany contemplated a similar range of measures to respond to the prospects of domestic telecommunications operators installing Huawei's 5G equipment.[2] Early in their processes, all three excluded the possibility of allowing mobile network operators to install Huawei equipment in the most sensitive "core" parts of their infrastructure, where it would have introduced the greatest vulnerabilities. This determination left them with the options of allowing national telecommunications providers (operators) to use Huawei gear in the non-core portions of their networks or prohibiting them from doing so, a move which would amount to a total ban on installing Huawei 5G equipment. While Huawei and Beijing sought to prevent such a total prohibition, the U.S. government insisted that nothing short of a complete ban could sufficiently reduce risks to network security.[3]

All three countries faced economic incentives to avoid a full ban. All three had national operators who had already made substantial investments in Huawei 4G and 5G equipment. None had national firms that could provide alternatives to Huawei's equipment, at least in the short term. If Huawei were banned, all would incur delays in their rollout of nationwide 5G infrastructure, inflicting disadvantages on consumers and domestic mobile-dependent industries alike. In each country, influential interest groups, most prominently large network operators, opposed complete bans on Huawei gear.

[2] While EU-level structures are active in 5G policy, decisions about restricting vendors remain national, member-state prerogatives. In this sense, the German case is comparable to those of EU non-members Japan and the UK.

[3] For context, see Bob Seely, Peter Varnish, and Hemmings, John, "Defending Our Data: Huawei, 5G and the Five Eyes," Henry Jackson Society, May 16, 2019, 9–15, https://henryjacksonsociety.org/publications/defendingourdata/; Nigel Inkster, "The Huawei Affair and China's Technology Ambitions," *Survival* 61, no. 1 (2019): 105–11, https://doi.org/10.1080/00396338.2019.1568041; Bruno Mascitelli and Mona Chung, "Hue and Cry over Huawei: Cold War Tensions, Security Threats or Anti-Competitive Behaviour?," *Research in Globalization* 1 (December 2019): 1–6, https://doi.org/10.1016/j.resglo.2019.100002; Xin Liu, "Chinese Multinational Enterprises Operating in Western Economies: Huawei in the US and the UK," *Journal of Contemporary China* 30, no. 129 (2021): 368–85, https://doi.org/10.1080/10670564.2020.1827351.

Moreover, all three countries enjoyed trade relationships with the PRC that were likely to be affected by a complete ban. PRC officials warned both the UK and German governments that moves to ban Huawei would meet economic retaliation. Even in the absence of an explicit threat, the Japanese government had reason to fear reprisals. Japan had experienced Chinese consumer boycotts of Japanese goods in response to actions that Beijing deemed unfavorable, an important consideration as China remains an important destination for Japanese exports and investment. The Chinese government's more recent restriction of rare earth exports to Japan in an apparent act of economic coercion reinforced concerns about retaliation.[4] In the wake of Brexit, the UK government sought to bolster trade ties with China and the United States to offset lost markets in the European Union. The UK arguably needed access to Chinese markets more than ever. Germany was home to numerous automobile and other manufacturers with sizeable China-destined exports vulnerable to retaliation.

At the same time, all three governments had reasons to adopt a complete ban. Each sought to preserve intelligence-sharing and other security cooperation with the United States, their most powerful ally. U.S. Secretary of State Mike Pompeo warned that the U.S. government would be reluctant to share intelligence with governments whose networks were compromised by the introduction of Huawei equipment. In this respect, the UK had the most to lose as a member of the Five Eyes intelligence-sharing partnership, but German officials also received a similar warning.[5] Defense and security officials in all three countries insisted that the intelligence relationship with the United States should not be compromised.

In all three countries, important constituencies opposed Huawei's participation in national 5G infrastructure on domestic security and public safety grounds. As in the United States, critical voices in these three countries warned that a role in national 5G infrastructure would give Huawei, a company closely tied to the PRC government, opportunities for espionage and other unauthorized data collection, empower it to disrupt critical functions, and afford it leverage deriving from these capacities. At the same time, in the UK and Germany, agencies dedicated to network security and familiar with Huawei equipment insisted that they could manage the risks associated with the company's participation in 5G infrastructure.

In spite of these similar circumstances, the three governments at first navigated the dilemma differently, only to reach similar policy outcomes. The Japanese government imposed a de facto ban on Huawei equipment in 5G networks. The UK government imposed only a partial ban on Huawei's 5G equipment until mid-2020, when, amid mounting domestic opposition, it abruptly reversed course. A complete ban on new installation took effect in 2021. The German government at first appeared to impose only a partial ban, but, after delaying the announcement

[4] Christina Lai, "Acting One Way and Talking Another: China's Coercive Economic Diplomacy in East Asia and Beyond," *The Pacific Review* 31, no. 2 (2018): 169–87, https://doi.org/10.1080/09512748.2017.1357652.
[5] Stephen Castle, "Pompeo Attacks China and Warns Britain Over Huawei Security Risks," *The New York Times*, May 8, 2019, sec. Technology, https://www.nytimes.com/2019/05/08/technology/pompeo-huawei-britain.html; David Brunnstrom, "Pompeo Tells Germany: Use Huawei and Lose Access to Our Data," *Reuters*, May 31, 2019, https://www.reuters.com/article/us-usa-germany-idUSKCN1T10HH.

of a final decision on the matter, implemented additional measures that make Huawei's participation in national 5G infrastructure unlikely.

Given the three countries' similar circumstances, the divergence in the form and timing of their responses presents an apparent puzzle, but a closer look reveals an underlying commonality. Neither of the three governments made a single explicit decision to definitively exclude Huawei or PRC-origin vendors. Japan's decision was not explicit. The UK's decision was deflected. Germany's decision was not definitive.

This paper advances the argument that the three governments, facing a decision on Huawei 5G that would be costly no matter how it was struck, all employed a strategy that minimized negative effects on their relations with both the PRC and the United States. All three sought to preserve a high-value trade relationship with one and a cherished security partnership with the other. Moreover, all three cases illustrate the extent to which the making of policy for trade, technology, and domestic infrastructure has grown intertwined with security policy.

The selection of these three cases serves the two overarching purposes of this study: concept development and illustration. Our first goal is to identify, characterize, and conceptualize what we argue is an overlooked mode of foreign policy conduct by middle powers: the non-decision decision. We derive this general concept inductively from a close examination of three cases that, at first glance, appear to present distinct outcomes but, upon closer inspection, reveal a common underlying logic. The selected cases allow us to trace how governments resort to this mode when facing a bind, establishing the plausibility and explanatory potential of the concept in specific, comparable contexts. Our cases are selected with this purpose in view, rather than to make for a quasi-experimental design suited to isolating causality.

Moreover, this selection of cases serves the purpose of concept development since the three countries arguably function as "hard cases" for the proposition that Huawei's equipment presents middle powers with a genuine dilemma. After the United States and China, they are the world's third (Japan), fourth (Germany), and fifth (UK) largest economies in nominal gross domestic product. Their economies are large, diversified, and in general less trade-reliant than those of many other middle powers and small states. This economic heft should provide the selected three with a measure of insulation from the PRC's economic coercion. The selected countries also have their own independent intelligence capabilities and domestic agencies prepared to independently assess the risks presented by Huawei gear, making them in principle less vulnerable to U.S. pressure. In sum, if Japan, the UK, and Germany face a Huawei policy dilemma structured by competing pressures from the two superpowers, then so do most other middle powers and small states. In this sense, the selected cases establish that our findings could plausibly extend to other countries.

A preliminary survey of other comparable cases bears out this contention. For instance, while France does not formally prohibit the installation of Huawei's 5G kit, measures adopted by the

French government have been characterized as a "de facto ban."[6] India has also been described as "sidelining" Huawei and likely to "quietly push" its equipment out of its networks, rather than risking China's rebuke with an overt ban.[7] One notable exception to this pattern, however, is Australia ,which moved early on to explicitly ban Huawei's participation in its 5G networks. The result, among others, is that it has experienced strident denunciations and economic retaliation from the PRC in the form of reduced Chinese imports of Australian goods.[8] Certainly the other states examined here were aware of Australia's experience, possibly shaping their own calculations.

In addition, the three selected countries provide ideal empirical terrain for this conceptual exploration since their policy outcomes are uncomplicated by protectionist forces. As a substantial literature on political economy has long recognized, domestic interest groups' demands for protection from foreign competition are a factor shaping regulatory choices, including bans on specific imports. In all three selected countries, however, Huawei has not been a competitor to domestic suppliers of 5G equipment. At the time that their governments were deliberating Huawei's role in their networks, neither Japan, nor the UK, nor Germany were home to any domestic companies capable of supplying the needed 5G equipment.[9] Their operators' choices came down to importing gear from Huawei or other foreign companies, such as Ericsson of Sweden, Nokia of Finland, or Samsung of South Korea. It also bears noting that no U.S. company has been a credible direct competitor to Huawei in Europe's 5G markets either,[10] suggesting that U.S. demands were rooted in security concerns, rather than disguised economic interests that the middle powers could placate in another way. Unmuddied by protectionist influences, the structure of the Huawei dilemma in the selected countries consists of a stark tension between trade and security considerations.

Our second goal is to illustrate the distinct forms that non-decision decisions can take across national settings. To this end, our selected cases each typify a variant of the phenomenon. The Japanese case depicts a policy decision obscured, unannounced formally but nonetheless having its intended effect of excluding Huawei equipment from domestic networks. The UK, in contrast,

---

[6] Mathieu Rosemain and Gwénaëlle Barzic, "Exclusive: French Limits on Huawei 5G Equipment Amount to de Facto Ban by 2028," *Reuters*, July 22, 2020, sec. Media and Telecoms, https://www.reuters.com/article/us-france-huawei-5g-security-exclusive-idUSKCN24N26R.

[7] Justin Sherman, "Don't Underestimate India's Sidelining of Huawei," The Diplomat, September 17, 2020, https://thediplomat.com/2020/09/dont-underestimate-indias-sidelining-of-huawei/.

[8] Jason Scott, Dan Murtaugh, and Bloomberg, "China Restricts Australian Coal Imports in Likely Retaliation to Huawei 5G Ban," Fortune, February 21, 2019, https://fortune.com/2019/02/21/china-australia-coal-imports/.

[9] Japan's NEC and Fujitsu would later enter the market.

[10] In the period preceding the non-decision decisions under study, the leading U.S. company in this space was Cisco, a company that itself did not supply comprehensive 5G network solutions. Moreover, Cisco commanded a far smaller share of global sales of 5G equipment than leaders Ericsson and Nokia and was widely regarded as an implausible alternative to Huawei in European markets.

presents a policy decision deflected. Policymakers dissembled and denied having the agency to decide on a ban, representing their policy reversal as the inevitable consequence of a change in U.S. export restrictions over which they had no control. Germany, meanwhile, presents a policy decision divided. Policymakers carved a single difficult policy decision into a series of smaller choices, each of which has been less conspicuous, but which together form a thicket of regulatory measures that approximates an eventual ban. As the case studies demonstrate, the form of the non-decision reflects the unique configuration of interests and institutions in each country. The concept of the non-decision decision thus captures a range of policy behaviors that reflect a fundamental logic of a government coping with competing demands and muddling through divided expert communities' positions by evading a traditional policy choice.

## Japan's swift but unstated comprehensive ban

In Japan, the office of the prime minister made the relatively early determination to exclude Huawei from national infrastructure. From the outset, even without a formal policy action, Japanese political elites interpreted the Huawei decision as hinging on intelligence and security priorities. Without public debate or disagreement, the swift de facto ban drew no significant reaction from China. A condition enabling this course of action was the Japanese government's power to unilaterally allocate spectrum to network providers, a prerogative that afforded it influence over the operators' conduct. In the UK and Germany, where companies compete for spectrum at auction, the state lacked this crucial lever.

Following the choices of Australia and the United States to exclude Huawei from their future 5G networks in the summer or 2018, reports began appearing in the news that Japan was also deliberating what position it should take.[11] At the time, among the major Japanese carriers that would be involved in 5G rollout—NTT Docomo, KDDI (au), Rakuten, and Softbank—only Softbank already had Huawei equipment already in use in its 4G base stations.[12] Both Softbank and NTT Docomo had partnered with Huawei in trials of 5G technology.[13]

On 7 December 2018, Yomiuri Shinbun first broke the news of a possible ban on Huawei and ZTE from Japanese government procurement.[14] At a meeting of various ministry officials in the Prime Minister's residence (*kantei*) on the 10th, the government indeed announced that in future

[11] "日本政府、華為とＺＴＥの規制検討か[Japanese government, Huawei and ZTE regulatory review?]" Jiji Press, 4 September 2018; "日本もファーウェイ禁止？" Record China, 28 August 2018.

[12] Mathieu Duchâtel, "Japan's 5G: a Mirror for Europe," Institut Montaigne, 26 February 2020, accessed 13 August 2020 at: https://www.institutmontaigne.org/en/blog/japans-5g-mirror-europe

[13] "SoftBank and Huawei Demonstrate 5G Use Cases," Huawei, 8 September 2017, accessed 13 August 2020 at: https://www.huawei.com/en/news/2017/9/Huawei-SoftBank-5G-Use-Cases; "中国通信２社「排除」確認　政府調達 [Confirmed. Exclusion of two Chinese telecommunications firms from government procurement]," Yomiuri Shinbun, 11 December 2018, 01.

[14] "中国通信２社を排除　ファーウェイ・ＺＴＥ省庁使用機器 [2 Chinese telecommunications companies Huawei, ZTE excluded from equipment used by ministries], Yomiuri Shinbun, 7 December 2018, 1.

procurement it would "not just take into consideration price, but also security risks."[15] While not mentioning Huawei or ZTE explicitly, this amounted to a de facto prohibition levelled at both. All the same, at a press meeting that same day, Japanese Prime Minister Shinzo Abe claimed that it is "important not to procure equipment carrying malicious capabilities… The goal is not to exclude any specific firm or equipment."[16]

Despite not facing any public demands to do so, the major carriers soon followed suit, with all, including Softbank, declaring that they would not use Huawei equipment for their 5G networks.[17] This came just days before the Ministry of Internal Affairs and Communications announced its criteria for companies to receive an allocation of frequencies for 5G development. On 14 December, the ministry sought last minute approval from the Radio Frequency Control Council for a clause that called for carriers to "pay attention to" (ryūi) government stipulations, including it's recent decision on procurement as well as to "adopt sufficient cyber-security measures including a response to supply-chain risk."[18] It quickly received the council's assent and made the guidelines public on the same day. The result was that Huawei and ZTE were now, for all intents and purposes, barred from participating in Japan's 5G network.

This turn of events hit Softbank particularly hard, as its mobile unit was launching an initial public offering; among other things, concerns about the costs of replacing Huawei kit in Softbank's 4G base stations hurt its share pricing.[19] Subsequently, the various carriers announced agreements with Nokia, Ericsson, Samsung, and the Japanese domestic firms NEC and Fujitsu, to cooperate in the rollout of 5G infrastructure in Japan.

That said, the Huawei ban has come as a boon to the Japanese corporations NEC and Fujitsu. NTT has purchased a 5% stake in NEC with the explicit goal of investing in its development of 5G technologies, and Rakuten has also chosen NEC as its 5G partner.[20] Fujitsu has partnered with Ericsson to develop end-to-end 5G services that would compete with Huawei.[21] The Japanese

[15] "中国通信機器-「排除」申し合わせ　省庁調達で日本政府 [Agreement to exclude Chinese telecommunications equipment in ministerial procurement, government of Japan], Mainichi, 10 December 2018.
[16] "中国通信２社「排除」確認　政府調達 [Confirmed. Exclusion of two Chinese telecommunications firms from government procurement]," Yomiuri Shinbun, 11 December 2018, 01.
[17] "携帯３社- 中国機器排除　来秋参入楽天も　５Ｇ基地局などで"[3 mobile companies exclude Chinese equipment, also Rakuten participating next fall, from 5G base stations, etc.] Mainichi, 12 December 2018.
[18] "第 5 世代移動通信システム(5G)の今と将来展望 [Present and future outlook of 5G systems]," Japanese Ministry of Internal Affairs and Communications, 27 June 2019, accessed 13 August 2020 at: https://www.soumu.go.jp/main_content/000633132.pdf; "５Ｇ- 中国製排除求める　総務省、電波割り当て指針 [Ministry of Internal Affairs and Communications radio spectrum allocation guidelines require excluding Chinese-made 5G]," Mainichi, 15 December 201
[19] Leo Lewis and Kana Inagaki, "SoftBank mobile unit falls 15% in Tokyo trading debut," Financial Times, 19 December 2018.
[20] Kana Inagaki and Nic Fildes, "NEC sees Huawei's woes as chance to crack 5G market," Financial Times, 1 July 2020.
[21] "Fujitsu and Ericsson team up on 5G partnership," Telefonaktiebolaget LM Ericsson, 26 October 2018, accessed 14 August 2020 at: https://www.ericsson.com/en/press-releases/2018/10/fujitsu-and-ericsson-team-up-on-5g-partnership

government has assisted as well, offering a 15% tax cut for firms investing in Japan's 5g infrastructure.[22]

Speaking in October of 2019, Japanese Prime Minister Shinzo Abe continued to maintain that Japan's policies "did not target any specific firm or equipment, or any specific country," and "moreover, are not based on any demand from the United States of America."[23] In reality, the Japanese government moved quite quickly and decisively at the end of 2018 to exclude Huawei from supplying equipment to the government or being involved in its 5G networks. All the same, the government has carefully avoided publicly naming Huawei as a target of its measures. It has additionally bolstered this with efforts to support its own indigenous capability—NEC and Fujitsu in particular—which previously had been minor players in terms of producing 5G equipment.

What emerges is a portrait of a state making a relatively rapid move to treat Huawei as a security threat and using the opportunity to advance indigenous alternatives. All this happened with very little open debate, and not without some cost to its carriers. Japan has consequently managed to ban Huawei without this becoming a major issue in Sino-Japanese relations and may see its own companies benefitting as other states look for alternatives to Huawei as well. Most recently, the UK was reported to have approached Japan for help in building its 5G network.[24]

## The UK's U-turn to a comprehensive ban

In the UK, the office of the prime minister was poised to adopt only a partial ban on Huawei equipment in domestic 5G networks as late as 2019. However, a domestic split soon emerged, intensified by U.S. pressure to adopt a complete ban and amid PRC warnings that excluding Huawei would harm economic ties. Opposition mounted in Parliament, demands for a complete ban growing across the political spectrum. Facing intensifying resistance from even within its own ranks, the Johnson government reversed itself. After a separate action by the U.S. government, the Johnson government adopted a complete ban. The official announcement cited new U.S. restrictions on Huawei that made the company's equipment less secure and verifiable than before, creating a changed circumstance that required a total ban. Rather than an independent policy decision, the UK government characterized its choice as the inevitable consequence of the U.S. rule change.

[22] Tetsushi Kajimoto, "Japan tax revision targets corporate cashpile to spur spending, 5G investment," Reuters, 12 December 2019, accessed 14 August 2020 at: https://www.reuters.com/article/us-japan-economy-tax/cashpile-to-spur-spending-5g-investment-idUSKBN1YG0JI

[23] "第二百回国会参議院議録第三号 [200th Meeting of the Upper House of the Diet, Diet Record Number 3], Kanpō, 9 October 2019.

[24] "UK asks Japan for help with 5G as alternative to Huawei," *Nikkei Asia Review*, 18 July 2020.

By 2007, the large telecommunications group BT had become to the first UK operator to deploy Huawei equipment across its network, following a minimal review by government agencies. [25] As other UK operators sought to use Huawei equipment and the need for a coordinated policy response grew apparent, the company established the Huawei Cyber Security Evaluation Centre (HCSEC), known as the Cell, in 2010. Owned and staffed by Huawei, the facility began to conduct analysis and provide operators with general guidance on how to manage the risks associated with the company's kit. In 2014, an Oversight Board began annual reviews of the Cell's operation. The body is chaired by the head of the National Cyber Security Center (NCSC, a division of the Government Communications Headquarter and responsible for computer security) and deputy chaired by a Huawei executive. [26]

As early as 2008, counter-intelligence agency MI5 had warned that the Chinese state could "exploit vulnerabilities in Huawei's equipment" to access the BT network, presenting an espionage risk.[27] Concerns within the intelligence community then mounted, drawing Parliament's attention. In 2013, the Intelligence and Security Committee reported concerns about the government's response to Huawei.[28]

In contrast, British industry remained confident in Huawei equipment. Starting in 2015, both the carrier Vodafone and BT announced partnerships with Huawei to research and test new 5G technologies and services.[29] Huawei's role in UK markets appeared substantial and entrenched.

However, as Huawei's presence in the UK grew, so did the intelligence community's security concerns. In 2018, the Oversight Board warned of "shortcomings in Huawei's engineering processes" introducing "new risks in the UK telecommunication networks and long-term challenges in mitigation and management."[30] The Board noted for the first time that it could provide "only limited assurance that all risks to UK national security from Huawei's involvement in the UK's critical networks have been sufficiently mitigated." [31]

---

[25] UK Parliament, Intelligence and Security Committee, "Foreign Involvement in the Critical National Infrastructure [Rifkind Report]" (London, UK: UK Parliament, June 2013), 4, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/205680/ISC-Report-Foreign-Investment-in-the-Critical-National-Infrastructure.pdf; Nic Fildes, "O2 to Test Huawei 5G Equipment in London," *Financial Times*, December 21, 2018, https://www.ft.com/content/8fa0ad72-0510-11e9-9d01-cd4d49afbbe3.

[26] "Huawei Cyber Security Evaluation Centre: Review by the National Security Adviser" (London, UK: HM Government, December 2013), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/266487/HCSEC_Review_Executive_Summary_FINAL.PDF.

[27] UK Parliament, Intelligence and Security Committee, "Rifkind Report," 11.

[28] UK Parliament, Intelligence and Security Committee, 4–29.

[29] "BT and Huawei Embark on Pioneering 5G Research Partnership," Huawei, December 8, 2016, https://www.huawei.com/us/news/2016/12/bt-huawei-embark-5g-research-partnership.

[30] "Huawei Cyber Security Evaluation Centre Oversight Board (HCSEC): Annual Report 2018" (London, UK: Huawei Cyber Security Evaluation Centre Oversight Board, July 2018), 4, https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2018.

[31] "Huawei Cyber Security Evaluation Centre Oversight Board," 4.

Later that year, scrutiny of Huawei intensified with the arrest of Meng Wanzhou, its chief financial officer and the daughter of its founder, in Canada on U.S. charges related to violating sanctions on Iran.[32] Shortly thereafter, the head of MI6 stated that the UK government faced a decision on whether Huawei should be barred from supplying the country's 5G mobile networks, following a similar ban on Chinese company ZTE.[33] Two days later, the government announced a review of its telecoms supply chains, cautioning that it could yield recommendations to industry. [34]

In response, UK telecommunications executives warned that a move to ban Huawei would set back the rollout of 5G networks by up to a year. [35] Like BT, the operator O2 had invested heavily in Huawei gear and it announced it would press ahead with trials of 5G networks using Huawei gear.[36] BT had already begun removing Huawei equipment from core areas of its 4G network, but sought to use Huawei technology in less sensitive parts of its system.[37] Operator Three also used Huawei equipment in its 5G network.[38]

When the government's supply chain review report came in early 2019, it announced tighter security requirements for operators.[39] That spring, sources in the National Security Council leaked that the government intended to allow Huawei access to "noncore" elements of 5G mobile infrastructure, such as antennas, in spite of opposition from the intelligence community.[40]

In May, U.S. Secretary of State Mike Pompeo warned that Huawei's involvement in the UK's 5G network could compromise U.S. intelligence sharing.[41] The Chinese Ambassador to the UK in turn warned that excluding Huawei from 5G networks would send a "bad signal," intimating that "China's investment in the UK might suffer."[42] A UK government decision remained pending when

[32] Fildes, "O2 to Test Huawei 5G Equipment in London."
[33] Alex Hern and Press Association, "BT Removing Huawei Equipment from Parts of 4G Network," *The Guardian*, December 6, 2018, sec. Technology, https://www.theguardian.com/technology/2018/dec/05/bt-removing-huawei-equipment-from-parts-of-4g-network.
[34] Fildes, "O2 to Test Huawei 5G Equipment in London"; "The Backlash to Huawei's Global 5G Expansion," Carnegie Endowment for International Peace, July 22, 2020, https://carnegieendowment.org/publications/interactive/huawei-timeline.
[35] Fildes, "O2 to Test Huawei 5G Equipment in London."
[36] Fildes; Mike Moore, "O2 Confirms 5G Tests Will Use Huawei Kit," TechRadar, December 21, 2018, https://www.techradar.com/news/o2-confirms-5g-tests-will-use-huawei-kit.
[37] Hern and Press Association, "BT Removing Huawei Equipment from Parts of 4G Network"; Nic Fildes, "BT to Strip Huawei Equipment from Its Core 4G Network," *Financial Times*, December 5, 2018, https://www.ft.com/content/c639aaf4-f7c9-11e8-8b7c-6fa24bd5409c.
[38] Hern and Press Association, "BT Removing Huawei Equipment from Parts of 4G Network."
[39] "UK Telecoms Supply Chain Review Report" (London, UK: UK Department for Digital, Culture, Media, and Sport, July 2019), https://www.gov.uk/government/publications/telecoms-supply-chain-review-terms-of-reference.
[40] Andy Bruce, "UK to Allow Huawei Limited Access to 5G Networks: Telegraph," *Reuters*, April 23, 2019, https://www.reuters.com/article/us-britain-huawei-tech-idUSKCN1RZ2HD.
[41] Castle, "Pompeo Attacks China and Warns Britain Over Huawei Security Risks."
[42] Sean Keane, "Chinese Ambassador Warns UK That Huawei Exclusion from 5G Sends a 'Bad Signal,'" CNET, accessed August 20, 2020, https://www.cnet.com/news/chinese-ambassador-warns-britain-huawei-exclusion-from-5g-sends-bad-signal/.

Parliament's Science and Technology Select Committee stated there were "no technological grounds for banning Huawei."[43]

In early 2020, the new Johnson government appeared to solidify the decision to allow Huawei partial access.[44] A NCSC report recommended restricting high-risk vendors, including Huawei, to 35 percent of total network capacity, keeping it out of "core" network functions, and proposed other mitigation measures, but stopped short of an outright ban.[45] Operators indicated they would comply.[46]

Beyond industry, however, the government's decision to allow Huawei partial access met opposition, both foreign and domestic. Pompeo urged Johnson to adopt a total ban, a message President Donald Trump reportedly reiterated to him in a phone call.[47] Later that spring, the government faced an unprecedented rebellion on the matter from the conservative government's own members. Thirty-eight conservative members backed a legislative amendment to altogether exclude Huawei from the country's 5G network by 2023, forcing a vote.[48]

The initial amendment was defeated, but set in motion a larger effort in Parliament that grew as bilateral relations deteriorated. The Chinese government's handling of the coronavirus pandemic, along with the UK's reliance on China for essential goods exposed by the crisis, intensified security concerns within Parliament.[49] Beijing's threat to impose a new national security law on Hong Kong increased tensions further.[50]

---

[43] Science and Technology Select Committee, "No Technological Grounds for Banning Huawei, but Ethical Concerns Must Be Taken into Account," UK Parliament, July 15, 2019, https://www.parliament.uk/business/committees/committees-a-z/commons-select/science-and-technology-committee/news-parliament-2017/chairs-comments-huawei-5g-network-17-19/; Norman Lamb, "Letter by Chair of Science and Technology Committee to Jeremy Wright Regarding Huawei [190710]" (UK Parliament Science and Technology Select Committee, July 10, 2019), https://www.parliament.uk/documents/commons-committees/science-technology/Correspondence/190710-Chair-to-Jeremy-Wright-re-Huawei.pdf.

[44] "Security Analysis for the UK Telecoms Sector: Summary of Findings" (London, UK: UK National Cyber Security Centre, January 2020), https://www.ncsc.gov.uk/files/Summary%20of%20the%20NCSCs%20security%20analysis%20for%20the%20UK%20telecoms%20sector.pdf.

[45] "Security Analysis for the UK Telecoms Sector: Summary of Findings."

[46] "BT Delays Removal of Huawei from EE's Core Network," *BBC News*, April 15, 2020, sec. Technology, https://www.bbc.com/news/technology-52296666; Mark Sweney, "Vodafone to Remove Huawei from Core European Networks," *The Guardian*, February 5, 2020, sec. Business, https://www.theguardian.com/business/2020/feb/05/vodafone-to-remove-huawei-from-core-european-networks.

[47] "Trump 'apoplectic' with UK's Johnson over Huawei Decision: FT," *Reuters*, February 6, 2020, https://www.reuters.com/article/us-britain-usa-huawei-trump-idUSKBN2002R2.

[48] "Huawei: Government Wins Vote after Backbench Rebellion," *BBC News*, March 10, 2020, sec. UK Politics, https://www.bbc.com/news/uk-politics-51806704.

[49] Dan Sabbagh, "Boris Johnson Forced to Reduce Huawei's Role in UK's 5G Networks," *The Guardian*, May 22, 2020, sec. Technology, https://www.theguardian.com/technology/2020/may/22/boris-johnson-forced-to-reduce-huaweis-role-in-uks-5g-networks.

[50] Sabbagh.

Several members of Parliament drew on new warnings from the intelligence community to advocate for reducing the UK's reliance on China.[51] They maintained that the core-edge distinction was untenable in practice and warned of the lock-in effect of allowing Huawei even a limited role in 5G. Critics noted that the Cell Oversight Board's 2018 warnings of security risks went unaddressed for over a year, indicating that mechanisms to compel the company to improve product security were ineffective.[52]

A growing chorus of parliamentarians tied these arguments to concerns about the nature of the regime in Beijing and its connections to the company. Proponents of a ban argued that Huawei would not contribute to, but instead undermine, supplier diversity, given its long history of underbidding competitors with likely government support. The company's critics pointed to the National Security Law that empowered the Chinese government to compel Huawei's cooperation in intelligence operations. Ban proponents pointed to the Chinese government's persistent human rights abuses and persecution of Uighurs.

Given these factors, they argued, the proposed 35 per cent threshold was too high and a complete ban required. The way forward was to seek alternative suppliers based in like-minded, democratic countries, such as the firms Ericsson, Nokia, and Samsung. These arguments proved persuasive. By May, the ranks of rebel conservatives and their supporters had swelled to 50 members, sufficient to defeat the government in a vote.[53]

Johnson's chief of staff Eddie Lister summarized part of the government's predicament in a 2020 meeting with a Huawei lobbyist, the minutes of which were later leaked to the press. "We are caught," Lister said.[54] "We want the technology, we want it rolled out. There's an American concern and a parliamentary concern. There are a large number of MPs across the political divide who have a problem with China. Some are Atlanticists, some over Covid, some over Hong Kong, some over human rights," he explained.[55]

As Johnson faced this gathering resistance, the U.S. government announced a regulatory amendment that would limit Huawei's access to U.S. chip technology as of May 15.[56] This development proved pivotal. Johnson's government seized upon it to reverse its earlier position.

---

[51] Sabbagh.

[52] "Huawei Cyber Security Evaluation Centre Oversight Board," July 2018; "Huawei Cyber Security Evaluation Centre Oversight Board (HCSEC): Annual Report 2019" (London, UK: Huawei Cyber Security Evaluation Centre Oversight Board, 2019), https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2018.

[53] Sabbagh, "Boris Johnson Forced to Reduce Huawei's Role in UK's 5G Networks."

[54] Tom Ambrose, "Guto Harri Reportedly Lobbied No 10 Chief of Staff to Stop Ban on Huawei," *The Guardian*, February 7, 2022, sec. Technology, https://www.theguardian.com/technology/2022/feb/07/guto-harri-reportedly-lobbied-no-10-chief-of-staff-to-stop-ban-on-huawei.

[55] Ambrose.

[56] Bureau of Industry and Security U.S. Department of Commerce, "Export Administration Regulations: Amendments to General Prohibition Three (Foreign-Produced Direct Product Rule) and the Entity List," *Federal Register*, May 15, 2020, https://www.federalregister.gov/d/2020-10715.

News media reported that his office was drawing up plans for a complete ban on Huawei 5G gear.[57] Days later, Johnson reportedly approached Washington about forging "an alliance of 10 democracies to create alternative suppliers of 5G equipment and other technologies to avoid relying on China."[58]

An official statement of the policy reversal came in in July, when the NCSC published an analysis of the U.S. rule change determining that the measure "increased the risk to UK networks" arising from Huawei's equipment by making the company's products less secure and less verifiable.[59] The NCSC recommended that operators install no Huawei equipment after the new U.S. rule took effect, a move that amounted to a comprehensive ban.[60] UK firms were required to remove all Huawei gear from 5G networks by 2027.[61] Digital Secretary Oliver Dowden announced that the government would pursue "an irreversible path" to complete removal through new legislation.[62] By November 2021, the Telecommunications (Security) Act creating a legal basis for the total ban had cleared Parliament and received royal assent.[63]

## Germany's postponed partial ban

Within the German government, consensus or even broad agreement on the interests at stake in 5G policy have proven elusive for years, but the direction of travel—through a series of non-decision decisions—appears to be towards a broad exclusion of Huawei. In principle, technical, intelligence, and security experts continue to deliberate policy for Huawei and other high-risk vendors of 5G equipment. In practice, however, new guidelines point to a general trend of significantly reducing, if not eliminating, Huawei from German networks.

Public debates over using Huawei equipment in Germany's 5G networks first emerged to any significant measure in late 2018. Prior to this, the major German carriers—Deutsche Telekom, Vodafone, and Telefonica—had all engaged in strategic partnerships with Huawei in anticipation of building their 5G networks.[64] Each also had significant amounts of Chinese-built equipment

[57] Sabbagh, "Boris Johnson Forced to Reduce Huawei's Role in UK's 5G Networks."
[58] Lucy Fisher, "Downing Street Plans New 5G Club of Democracies," May 29, 2020, sec. news, https://www.thetimes.co.uk/article/downing-street-plans-new-5g-club-of-democracies-bfnd5wj57.
[59] "Summary of the NCSC Analysis of May 2020 US Sanction" (London, UK: UK National Cyber Security Centre, July 14, 2020).
[60] "Summary of the NCSC Analysis of May 2020 US Sanction."
[61] Oliver Dowden, "Digital, Culture, Media and Sport Secretary's Statement on Telecoms" (Statement to Parliament, UK House of Commons, London, UK, July 14, 2020), https://www.gov.uk/government/speeches/digital-culture-media-and-sport-secretarys-statement-on-telecoms.
[62] Dowden.
[63] UK Parliament, "Telecommunications (Security) Bill," UK Parliament, accessed September 15, 2021, https://bills.parliament.uk/bills/2806.
[64] "Huawei and Vodafone announce strategic partnership on 5G Technologies," *Huawei*, 18 February 2016, accessed 19 August 2020 at: https://www.huawei.com/en/news/2016/2/huawei-and-vodafone-announce-strategic-partnership-on-5g-technologies; "Telefonica and Huawei Sign Joint Innovation Agreement on 5G&NG-RAN," *Huawei*,

already in their 4G networks, with the shares being Deutsche Telekom 65%, Vodafone 55%, and Telefonica 50%, respectively.[65] Over the course of 2018, several developments prompted growing attention to turn to the question of Huawei involvement. The first was the increase in warnings coming out of the United States and the subsequent decisions by the United States, Australia, and New Zealand not to use Huawei components in their networks. A second was a desire by the carriers for clarity in the face of an upcoming frequency auction and the need to plan for 5G network construction. All this led to a number of German politicians publicly questioning the wisdom of relying on Huawei components as well as pressure on the German government to take a clear stance.[66]

Behind the scenes, however, there had already been movement. In December 2017, the head of Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik or BSI) had flown to China to meet with the head of Huawei to discuss greater access. The result was that November 2018 Huawei opened a collaborative laboratory in Bonn where BSI staff could examine Huawei equipment and source code for security issues.[67]

Building on this, a cabinet meeting in early February 2019 came to the conclusion that Huawei should not be excluded from participation in the German 5G network—a position apparently strongly held by German Chancellor Angela Merkel—but that the government would compile a new "security catalogue" that would delineate requirements for 5G suppliers and the BSI would be responsible for inspecting and certifying components.[68]

While the frequency auction went forward in March, the security catalogue would not be forthcoming until 15 October. When it came, however, it indeed left the door open for Huawei to take part in building Germany's 5G network. It stipulated a certification process for components defined as critical and required suppliers to provide a written declaration concerning their own trustworthiness.[69] This was quickly criticised as insufficient by various German politicians, even some belonging to Merkel's own party, the CDU/CSU.[70] The United States also expressed its

---

22 June 2016, accessed 19 August 2020 at: https://www.huawei.com/en/news/2016/6/5gng-ran-lianhe-chuangxin-xieyi; "Deutsche Telekom and Huawei Complete World´s First 5G High mmWave Technology over-the-air Field Tests," *Huawei*, 28 February 2018, accessed 19 August 2020 at: https://www.huawei.com/en/news/2018/2/dectschtelckom-5g-high-mmwave-technology

[65] Strand Consult, "Understanding the Market for 4G RAN in Europe: Share of Chinese and Non-Chinese Vendors in 102 Mobile Networks," accessed on 19 August 2020 from: http://www.strandreports.com/sw8772.asp

[66] Dana Heide and Stephan Scheuer, "Mobilfunknetz; 'Wer hat Angst vor Huawei?' - Die Sorge um die Sicherheit von 5G wächst [Mobile Network: Who is afraid of Huawei? Concerns over the security of 5G grow], *Handelsblatt,* 16 January 2019; Noah Barkin, "German officials sound China alarm as 5G auctions loom," *Reuters*, 13 November 2018.

[67] Holger Stark, "Konzern unter Verdacht [Corporation under suspicion]" *Die Zeit*, 21 February 2019, 19-20.

[68] Daniel Delhaes, Moritz Kock, and Dana Heide, " Neue Sicherheitsmaßnahmen; Huawei darf das 5G-Netz ausrüsten [New security measures, Huawei is allowed to equip the 5G network], *Handelsblatt*, 7 February 2019; Melanie Amann, "Spion an der Milchkanne [Spy on the Milk Jug]," *Der Spiegel*, 9 February 2019, 28.

[69] Bundesnetzagentur, "Katalog von Sicherheitsanforderungen, [Catalogue of security requirements]," 9 October 2019.

[70] Moritz Koch, "5G-Ausbau; Aufstand gegen Huawei: Abgeordnete rebellieren gegen Merkels Politik [5G-expansion, revolt against Huawei: representatives rebel against Merkel's policy], *Handelsblatt*, 22 October 2019.

disapproval.[71] For its part, the Chinese Chamber of Commerce in Germany warned that an exclusion of Huawei for political reasons or due to foreign pressure would have "highly negative effects on future economic cooperation between Germany and China."[72]

Over the following months, opposition within the Social Democrats (SPD), the Liberals (FDP), the Greens, and even the CDU/CSU itself continued to grow. In December 2019, the SPD parliamentary group put forward a position paper calling for the exclusion of untrustworthy suppliers—which given their definition thereof would include Huawei.[73] Two months later the CDU/CSU parliamentary group put forward its own position. While not calling for an outright ban on Huawei or any specific supplier, it did state that the "deployment of components from a supplier can be prohibited when it is confirmed that it contradicts the overriding public interest, especially the security needs of the Federal Republic of Germany."[74]

The various carriers sought to move forward with 5G rollout, but each reacted differently to the legal uncertainty involved. Telefonica, in December of 2019, publicly announced it would be using Huawei antennae for its 5G network.[75] Subsequently, however, in response to the U.S. "Clean Network" initiative, it has declared itself a "5G Clean Path company" that in the "near future" would not use any equipment from "untrusted vendors."[76] In February 2020, Vodafone stated that it would remove Huawei from its core network at a cost of two hundred million euros, but still is proceeding with plans to use Huawei equipment in its radio access network (RAN).[77] Deutsche Telekom (DT) also stated it would not use Huawei in its network core, but remained committed to using Huawei equipment for its RAN. In June 2020, it made the news when leaked documents revealed DT officers describing a Huawei ban as "Armageddon," estimating a replacement of existing Huawei kit in its network to require five years and cost three billion Euros.[78] DT has subsequently announced that its reliance on Huawei is decreasing, but it continues to advocate

[71] Matthias Nass, "»Praktisch nicht zu schützen«; Soll die chinesische Firma Huawei an der Zukunft der Telekommunikation in Deutschland beteiligt werden? Der US-Diplomat Christopher Ford warnt vor Naivität ["Practically impossible to protect"; should the Chinese company Huawei participate in the future of telecommunications in Germany? The US diplomat Christopher Ford warns against naivety], *Die Zeit*, 7 November 2019, 6.

[72] Thorsten Mumme, "Huawei: Chinesische Handelskammer warnt vor Bann, [Huawei: Chinese chamber of commerce warns against a ban]" *Tagesspiegel Background*, 11 November 2019, accessed 19 August 2020 at: https://background.tagesspiegel.de/digitalisierung/huawei-chinesische-handelskammer-warnt-vor-bann

[73] SPD Fraktion in Bundestag, "Ein digital souveränes Europa mit sicheren 5G-Netzen," 17 December 2019, accessed 19 August 2020 at: https://www.spdfraktion.de/system/files/documents/positionspapier-ein-digital-souveraenes-europa-mit-sicheren-5g-netzen-20191217.pdf

[74] CDU/CSU-Fraktion im Deutschen Bundestag, "Deutschlands digitale Souveränität sichern – Maßstäbe für sichere 5G-Netze setzen [Securing Germany's digital sovereignty—setting standards for secure 5G-networks]" 10 February 2020, accessed 19 August 2020 at: https://www.cducsu.de/sites/default/files/2020-02/Positionspapier%205G-Netzaufbau-100220.pdf

[75] Sara Germano, "Huawei Strikes German 5G Deal Despite Political Pushback," *Wall Street Journal*, 11 December 2019.

[76] U.S. Department of State, "The Clean Network," 5 August 2020, accessed 20 August 2020 at: https://www.state.gov/the-clean-network/

[77] Paul Sandle, "Vodafone to remove Huawei from core of European network," *Reuters*, 5 February 2020.

[78] Moritz Koch and Stephan Scheuer, "Szenario des Schreckens [Terror scenario]," *Handelsblatt*, 17 June 2020, 16.

using a variety of vendors including Huawei.[79] A newcomer also emerged—1&1 Drillisch—but sought partnerships with Japan's Rakuten of building its network.[80]

Given that both Vodafone and DT desired to proceed with using Huawei in their RAN, both actively lobbied against a ban within Germany. Politically, those most strongly supporting their position were Merkel, the German Minister for Economic Affairs and Energy, Peter Altmaier, and the German Minister of the Interior, Horst Seehofer, all of whom belong to the CDU/CSU.[81] They have also been supported by the head of the BSI, Arne Schönbohm, who argues that his office can control the risk of using Huawei.[82] Arguments in favour of allowing Huawei to participate in Germany's 5G networks included the fact that its equipment is cheaper, it is seen as more advanced in some areas as compared to its competition, and its participation increases the diversity of suppliers so as to avoid the dangers of a technological monoculture. A further concern was a potential backlash from Beijing that would harm German market access in China, particularly the automotive industry—"Audi and Mercedes of late sell approximately every third car in the People's Republic."[83] Indeed, the Chinese ambassador was not above making threats of retaliation should Huawei be excluded from the German market.[84]

Rallying against Huawei were the Foreign Ministry under the SPD politician, Heiko Maas, the Federal Intelligence Service (Bundesnachrichtendienst or BND), the SPD, all opposition parties, and even key members of the CDU/CSU, such as the Chair of the Parliamentary Foreign Affairs Committee Norbert Röttgen.[85] The concerns critics raised in debates over Huawei were multiple: the possibility of network sabotage, whether through a "kill-switch," a network slowdown, or re-routing of traffic; the possibility of espionage, be it targeted at specific communications or in the form of meta-data concerning general activity; broader intelligence cooperation with Beijing, be it in terms of allowing Beijing head-start access to zero-day flaws or providing information on the structure and composition of German networks; overdependence, leaving Germany subject to

[79] Stephan Broszio, "Vielfalt statt Abhängigkeit [Diversity instead of dependence]," Deutsche Telekom, 7 July 2020, accessed 20 August 2020 at: https://www.telekom.com/de/blog/konzern/artikel/telekom-setzt-auf-multi-vendor-strategie-603466

[80] Stephan Scheuer, "Japanischer Netzbetreiber Rakuten soll 1&1 mit 5G in Deutschland helfen" [Japanese network provided Rakuten will help 1&1 with 5G in Germany], Handelsblatt, 15 March 2021.

[81] Moritz Koch and Stephan Scheuer, "Huawei-Technik; 5G-Offensive von Vodafone und Telekom stößt in der Politik auf Widerstand [Huawei Technic: 5G-offensive from Vodafone and Telekom runs up against political resistance]," *Handelsblatt*, 26 April 2020.

[82] Marcel Rosenbach, "Nur Vorsorge hilft [Only precaution helps]," *Der Spiegel*, 20 July 2019, 36.

[83] Tim Bartz, "Ewiger Kniefall [Eternal Kneeling]," *Der Spiegel*, 24 August 2019, 60;

[84] Katrin Bennhold and Jack Ewing, "German Call on Huawei and 5G May Hinge on Vital Automakers," *The New York Times*, 17 January 2020, A1.

[85] Moritz Koch and Stephan Scheuer, "Huawei-Technik; 5G-Offensive von Vodafone und Telekom stößt in der Politik auf Widerstand [Huawei Technic: 5G-offensive from Vodafone and Telekom runs up against political resistance]," *Handelsblatt*, 26 April 2020.

potential economic coercion or disruptions; and the further weakening of European technological capabilities and capacities.[86]

It is important to note that the United States also played a role in these debates. On the one hand, it was seen as an important ally, and its threats to withhold intelligence cooperation should German 5G networks use Huawei equipment were taken seriously. What is more, it has also been the source of intelligence on Huawei that has raised concerns in Germany.[87] On the other hand, the intervention of the U.S. ambassador in German domestic debates over Huawei has been perceived as heavy-handed.[88] The fact that the Washington had used its technological position to spy on German officials in the past also means that its stance is easily perceived in Germany as cynical and hypocritical.

These debates came to a head at the end of April 2021, when the Bundestag passed the new IT Security Law 2.0 (IT-Sicherheitsgesetz 2.0). The law did not explicitly forbid the use of Huawei kit—as CDU representative Christoph Bernsteil put it, it is not a "Lex Huawei" (law specifically for Huawei)—but it did raise significant hurdles for its deployment.[89] Under the new law, carriers are required to notify the Federal Ministry of the Interior of the components they intend to use when building critical infrastructure. These components are then not just to be subjected to technical testing for security vulnerabilities, their producers will also be evaluated on the basis of political-security (sicherheitspolitischen) criteria.[90] To these belong questions of whether "the producer directly or indirectly is controlled by the government… of a third state"; "the producer had already been or is involved in activities that have a disadvantageous effect on the public order or security of the Federal Republic of Germany or another member state of the European Union, the European Free Trade Association, or the North Atlantic Treaty or their facilities"; and whether or not "the deployment of critical components is in harmony with the political-security goals of the Federal Republic of Germany, the European Union, or the North Atlantic Treaty."[91] Also added were a variety of requirements for stipulating the trustworthiness of a producer, including false

[86] For thorough discussion of these issues, see: "Öffentliche Anhörung des Auswärtigen Ausschusses zum Thema: Einführung des Mobilfunkstandards 5G [Public Hearing of the Foreign Affairs Committee on the topic: Introduction of the 5G mobile communications standard]," Deutscher Bundestag, 11 November 2019, accessed 20 August 2020 at: https://dbtg.tv/cvid/7398783

[87] Moritz Koch, "5G-Debatte; 'Smoking gun': Bundesregierung hat Beweise gegen Huawei [5G-Debate: smoking gun: the federal government has evidence against Huawei," *Handelsblatt*, 29 January 2020.

[88] Christian Rothenberg, "5G-Debatte; 'Unreife Ansichten': Deutsche Außenpolitiker greifen US-Botschafter Grenell *scharf* an [5G-Debate, Immature views: German foreign policy makers sharply attack US Ambassador Grenell]," *Handelsblatt*, 17 February 2020.

[89] Der Spiegel, "Bundestag beschließt Hürden-für-Huawei-Gesetz," [The Bundestag passes a 'hurdles-for-Huawei' law], 23 April 2021.

[90] Till Hoppe, Moritz Koch, Christof Kerkmann, "5G-Netz: Bundestag beschließt strikte Sicherheitsprüfung für Huawei,"[5G-Network: Bundestag decides strict security test for Huawei], *Handelsblatt*, 23 April 2021.

[91] Bundesrat, "Gesetzbeschluss des Deutschen Bundestages: Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme," 23 April 2021, accessed 16 May 2021 at: https://www.bundesrat.de/SharedDocs/drucksachen/2021/0301-0400/324-21.pdf?__blob=publicationFile&v=1

statements in its declaration of trustworthiness or not immediately declaring remedying weakness or manipulations of its components upon becoming aware of their existence.[92]

German officials claimed that the new law treated all suppliers as equal—"no supplier is ruled out a priori"[93]—but as the measures become implemented the bar will be raised so as to make it far more difficult for Chinese suppliers to participate than before. Merkel and Altmaier had worked hard to prevent the inclusion of a political test for suppliers, but the Bundestag, including members of their own party, had over-ruled them.[94] Certainly, the law did provide the Ministry of the Interior some leeway in its decision making. But given the existence of explicit PRC national intelligence laws compelling the cooperation of companies and other private actors in China, arguing that Huawei is free from any possibility of such influence would appear be a difficult case to make.[95]

At the point of this writing, Huawei still has not been officially excluded from German 5G networks. That said, over the coming decade it is unlikely to have a significant role going forward, and already the telecoms that bet on cooperation with Huawei are seeking a means to insulate themselves from the costs of using alternatives.[96] The German process was one of significant and fractious public debate—albeit without becoming a major focus of popular media attention—that resulted in the incremental tightening of regulatory criteria. German officials were careful not to ban Huawei outright, but they have continued to raise the bar making Huawei's participation more difficult. By including reference to the goals, the European Union and NATO goals, the German government has also provided itself an external reason for a potential ban.

That being, as many German commentators spoken to off-the-record for this piece have noted, "Papier ist geduldig" (paper is patient), meaning that although the laws are on the books, the oversight apparatus will still require time to realise in practice. There also remain questions as to what components will be classified as "non-critical" in their function, and thus exempt. The combination of these two mean that Huawei components may remain in German networks for some time, although in the long-term—especially given that the new coalition government has taken a more sceptical view towards Huawei—it looks like Huawei's role will decline if not disappear. In short, Germany has avoided an explicit decision to exclude Huawei, but at the same time increasingly raised the regulatory barriers to its continued involvement in its 5G networks.

---

[92] Ibid.

[93] CDU/CSU, "IT-Sicherheitsgesetz 2.0 verabshiedet" [IT security law 2.0 concluded], 22 April 2021, accessed 16 May 2021 at: https://www.cducsu.de/presse/pressemitteilungen/it-sicherheitsgesetz-20-verabschiedet

[94] Till Hoppe, Moritz Koch, Christof Kerkmann, "5G-Netz: Bundestag beschließt strikte Sicherheitsprüfung für Huawei,"[5G-Network: Bundestag decides strict security test for Huawei], *Handelsblatt*, 23 April 2021.

[95] Yuan Yang, "Is Huawei compelled by Chinese law to help with espionage?" *Financial Times,* 5 March 2019.

[96] Moritz Koch, "Drohender Huawei-Ausschluss bei 5G-Netz: Es darf keine Entschädigung für die Telekom geben," [Impending Huawei exclusion from the 5-G Network: There should be no compensation for Telekom], *Handelsblatt*, 24 April 2021.

## The non-decision decision: Middle powers muddle through

Although the three governments arrived at the outcome in distinct ways, all converged on policy measures that obstruct or complicate the installation of Huawei equipment within their domestic 5G infrastructure, while evading explicit, definitive, or singular policy decisions that would have invited objection from one or both superpowers. Japan's ban was undeclared and tacit. The UK's ban was represented as the inevitable consequence of a U.S. action, rather than a policy decision. And Germany has progressively raised barriers to Huawei's participation that make it an increasingly unlikely supplier in the long term.

We contend that the resort to non-decision decisions on the Huawei 5G matter in these three cases foreshadows a new mode by which middle powers manage competing demands from the two rivalrous superpowers and navigate transnationalized policy questions that lie at the intersection of trade, technology, and security. These cases of non-decision decisions reflect four major trends in international relations. First, in the post-Cold War period, the boundaries between technology, trade, and security policy have blurred, presenting governments with new challenges for which their domestic institutions are unprepared. Second, this intertwining of technology, trade, and security interests has created especially acute challenges for the making of policy in the information-technology (IT) sectors. Third, the new trade-security nexus in IT presents a unique challenge to middle powers who have sought to preserve a privileged security relationship with the United States while reaping the benefits of growing trade with the PRC. This strategy depended on a neat compartmentalization of policy issues into economic and security spheres that is no longer tenable. Fourth, as the U.S.-PRC rivalry now intensifies and extends to new technology issues, middle powers face narrowing options. Their resort to non-decision decisions represents one means of coping with these tightening constraints.

First, the post-Cold War period has seen the gradual blurring of technology, trade, and security policy, a transformation that encompasses a broadening range of technology-intensive products and domestic policy considerations. This change has brought the gradual elevation of technology policy from "low" to "high politics" in a growing number of countries.[97] Once the preserve of obscure specialized bureaucracies, the regulation of trade in high-technology items is now intertwined with new and far-reaching national security considerations. As the Cold War-era compartmentalization of traded goods into "commercial" and "dual-use" products has dissolved in practice, the range of "sensitive" traded high-technology items demanding regulatory attention from security and defense agencies has expanded.[98] Information and communications technology systems, which function as infrastructure that sustains industrial and large-scale consumer activity, sit at this blurred boundary.

At the same time, in many countries regulatory processes for addressing the new security challenges lurking within trade remain in the early stages of their development.[99] The result has

[97] Tai Ming Cheung and Bates Gill, "Trade Versus Security: How Countries Balance Technology Transfers with China," *Journal of East Asian Studies* 13, no. 3 (2013): 448, https://www.jstor.org/stable/26335258.
[98] Cheung and Gill, "Trade Versus Security."
[99] Cheung and Gill.

been the mounting securitization of trade and technology without concomitant growth in regulatory capacity and authority. This tendency toward securitization is illustrated in the redefinition by governments of wireless networks as elements of critical national infrastructure directly presenting national security considerations. National legislatures now play pivotal roles in these issue areas, defining decisions on high-technology trade as hinging on long-term foreign-policy goals and geostrategic considerations. In the UK, Germany, and other parts of Europe, the contentious debate over authority in this policy space between different government agencies and expert constituencies reflects the relative underdevelopment of these regulatory structures.

Second, this intertwining of technology, trade, and security considerations is particularly acute in the making of policy for information-technology (IT) goods and services. The growth of trade specifically in IT-intensive items presents entirely new forms of interdependence and, with it, risks, to which states' security institutions are growing increasingly attuned.[100] While goods and services have long depended on transnational supply chains, the now-unfolding fourth industrial revolution has brought greater and more persistent interconnectedness between supplier and buyer countries, including in data flows. Governments today have begun to wrestle with a trade-security nexus reshaped by these forces.[101] In many cases, policymakers and expert communities have redefined issue-areas once understood as primarily domestic, such as infrastructure, as geopolitical and strategic elements of their digital economies.[102] As concerns over cybersecurity have grown and broadened, telecommunications networks have grown securitized to an unprecedented degree.[103]

While the new trade-security nexus in high technology complicates trade flows in general, nowhere are its effects more striking than in the PRC's trade relations. The PRC is rapidly becoming a world-leading exporter of certain IT-intensive goods and services, from handsets and financial technology applications to 5G network equipment. Moreover, Beijing has adopted a series of policies and measures that underscore its strong political commitment to cultivating and promoting national champions in global IT-intensive industries. Huawei stands out as an emblem of the PRC's transformation from a manufacturer of low-value-added labor-intensive goods to a global high-technology powerhouse, whose homegrown firms operate at the cutting edge of the industries defining the twenty-first century. The enormous importance the PRC attaches to Huawei in particular is apparent in its response to Canadian authorities' arrest of Meng Wanzhou, the company's chief financial officer and its storied founder's daughter, on a U.S. warrant for charges relating to violating sanctions on Iran. As apparent retaliation for Meng's arrest, Beijing resorted to the detention of two Canadian citizens in China and the extraordinary resentencing of

[100] Henry Farrell and Abraham L. Newman, "Weaponized Interdependence: How Global Economic Networks Shape State Coercion," *International Security* 44, no. 1 (July 1, 2019): 42–79, https://doi.org/10.1162/isec_a_00351.

[101] Kello, Lucas. "The meaning of the cyber revolution: Perils to theory and statecraft." *International Security* 38, no. 2 (2013): 7-40.

[102] See, for example, Andrew Stephen Campion, "From CNOOC to Huawei: Securitization, the China Threat, and Critical Infrastructure," *Asian Journal of Political Science* 28, no. 1 (January 2, 2020): 47–66, https://doi.org/10.1080/02185377.2020.1741416; Inkster, "The Huawei Affair and China's Technology Ambitions"; Mascitelli and Chung, "Hue and Cry over Huawei."

[103] Lene Hansen and Helen Nissenbaum, "Digital Disaster, Cyber Security, and the Copenhagen School," *International Studies Quarterly* 53, no. 4 (2009): 1155–75, http://www.jstor.org/stable/27735139.

a third Canadian serving a prison sentence to the death penalty, allowing the release of the first two only after Meng's negotiated return to China three years later.[104] For the PRC's leaders, foreign steps to curb Huawei amount not to the snub of a mere company, but to hostile attempts at thwarting the country's modernization and ascent into the ranks of the world's leading economic powers.

Third, these changes present a distinct challenge to U.S.-allied and U.S.-aligned middle powers. Throughout the post-Cold War, the PRC's rapid economic growth within a U.S.-led global order presented these states with more opportunities than threats. In spite of setbacks in the U.S.-PRC relationship, many of these countries for decades managed to maintain a security relationship with the United States while cultivating a growing trade relationship with the PRC.[105] Virtually every member of NATO, Japan, South Korea, Australia, Singapore, and numerous other allies and security partners of the United States have reaped substantial benefits from trade with the PRC, which for many has become a chief export destination. The crux of these countries' strategies, most apparent for those in East Asia, was to hedge against the PRC by preserving or even developing a security partnership and/or enhanced trade with the United States, while pursuing expanded sales and investment opportunities for their companies in China. Indeed, for a period after the great financial crisis, when the PRC's appetite for imports persisted amidst slowing global demand, the necessity and wisdom of these strategies appeared reaffirmed to leaders of export-reliant middle powers. However, a crucial, if usually unstated, assumption behind such strategies was that trade and security issues could be separated and, it followed, relations with the superpowers could be compartmentalized, a supposition now challenged by the changing nature of global high-technology trade.

Fourth, as a result of these changes, the continued viability of these long-standing middle-power strategies is today in doubt.[106] As the U.S.-PRC rivalry has intensified and broadened into a multi-dimensional competition encompassing technology questions, the options before middle powers have narrowed. Japan, Germany, and the UK now face competing, incompatible demands by the United States and PRC on a range of issues, spanning international governance of pandemics to domestic infrastructure. These issue-areas do not admit of neat compartmentalization into traditional security and economic spheres. As Brian Job and others have explained, the constraints on middle powers are tightening.[107] These countries are now "stuck" between the two great superpowers, enjoying less "space" to maneuver than before.[108] Under the Xi and Trump

[104] Inkster, "The Huawei Affair and China's Technology Ambitions," 106–8; Liu, "Chinese Multinational Enterprises Operating in Western Economies," 378; Rob Gillies, "Canadians, Chinese Executive Return Home in Prisoner Swap," AP NEWS, September 25, 2021, https://apnews.com/article/middle-east-canada-china-arrests-washington-2b6e0977ae93557ad1265869d57838ed.

[105] G. John Ikenberry, "Between the Eagle and the Dragon: America, China, and Middle State Strategies in East Asia," *Political Science Quarterly* 131, no. 1 (2016): 9–43, https://doi.org/10.1002/polq.12430.

[106] Sung Chul Jung, Jaehyon Lee, and Ji-Yong Lee, "The Indo-Pacific Strategy and US Alliance Network Expandability: Asian Middle Powers' Positions on Sino-US Geostrategic Competition in Indo-Pacific Region," *Journal of Contemporary China* 30, no. 127 (2021): 53–68, https://doi.org/10.1080/10670564.2020.1766909.

[107] Brian Job, "Between a Rock and a Hard Place: The Dilemmas of Middle Powers," *Issues and Studies* 56, no. 2 (2020): 1–24, https://doi.org/10.1142/S10132.51120400081.

[108] Job, 1–4.

administrations, both the United States and PRC have used "coercive economic tactics to threaten or punish middle powers and small states" for transgressions.[109] The growing rivalry, increasingly characterized by hawks on both sides "as a confrontation of 'existential threats'" – across a range of policy areas that straddle trade and security considerations – reduces the options available to middle powers and forces them into dilemmatic choices between sides.[110]

The Huawei policy dilemma is illustrative of the broader tensions between commercial and security interests that governments face in making contemporary foreign and technology policy. While such trade-offs are perennial, they arguably arise in a more pronounced form with digital technologies and the tightly integrated supply chains in which they are embedded, virtually all of which run through China. For instance, export controls today are not only as difficult as ever to implement, but also more challenging to design effectively, since so many sensitive technologies have important or even primary commercial applications. Many defense systems depend on commercial IT inputs whose export cannot be restricted except at great opportunity cost to the industries that produce them. And many commercial inputs are assembled or produced in China, the very target of the export controls applied to the finished systems that will contain them.

Foreign direct investment into high-technology industries presents a similar dilemma.[111] Several governments have contemplated limiting foreign ownership of domestic companies possessing significant proprietary technology. Some are developing investment-screening mechanisms intended to curb Chinese control of their national champions.[112] While inbound capital is often needed to develop these industries, governments perceive it as carrying intolerably high risks, both directly to the target companies and downstream to the client firms with whom they exchange privileged technical information.

As with critical communications infrastructure, in policy decisions about export controls and investment screening, middle powers and certain small states face countervailing pressures from the superpowers. A supplier of capital to these middle powers and purchaser of their high-technology goods, China insists on access to investment opportunities and products, while the United States, ever the staunch guardian of security interests, demands restrictions on Chinese involvement and influence. In this sense, the Huawei policy dilemma is far from a discrete and specialized problem, but a manifestation of a more fundamental challenge that will outlast any specific choices on 5G suppliers.

---

[109] Job, 9.

[110] Job, 1.

[111] We thank an anonymous reviewer for raising this point.

[112] Sarah Bauerle Danzman and Sophie Meunier, "The Big Screen: Mapping the Diffusion of Foreign Investment Screening Mechanisms," SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, August 28, 2021), https://doi.org/10.2139/ssrn.3913248; Ashley Thomas Lenihan, "How Can the Effectiveness of Western FDI Regulations Be Ensured with Respect to the National Security Risks Posed by Strategic Inbound Investment from China?," in *Protect, Constrain, Contest: Approaches for Coordinated Transatlantic Economic and Technological Competition with China* (London, UK: LSE Ideas, 2021), 11–16, https://www.lse.ac.uk/ideas/publications/reports.

The resort to non-decision decisions represents one means for middle powers to cope, however imperfectly, with these tightening constraints. The non-decision decision affords governments room to negotiate the superpowers' competing demands in several ways, not least by undermining the latter's basis for retaliation against an unfavorable move. First, the non-decision decision may bring the middle power some plausible deniability, since the offending choice goes unstated. Without a formal announcement, no obvious target exists to attract either a superpower's ire or its demands for redress. Japan's undeclared ban on Huawei illustrates this significant advantage at work, since it was the only one of the three countries not to experience major pressures from the Chinese government in connection with the decision. Second, the non-decision decision can allow for a deflection of responsibility by the middle power. In some instances, a skillful non-decision decision can dissimulate the agency behind an offending policy outcome. The UK's reframing of its complete ban on Huawei as the inevitable consequence of a U.S. action that rendered Huawei equipment less secure and verifiable illustrates this feature. Third, a non-decision approach can allow a government to fragment a single high-stakes policy decision into several less conspicuous maneuvers. Each of these is individually less likely to invite retaliation or even notice by a superpower. Germany's layering of measures that gradually made Huawei's participation in its 5G networks less feasible illustrates this approach.

In certain respects, the non-decision decision shares similarities with the non-tariff barrier, a protectionist trade measure that takes the form of a regulatory obstacle to unwanted imports, often adopted instead of an explicit tariff. Non-tariff barriers grew more common and more effective as international trade organizations restricted governments' capacity to impose outright tariffs.[113] Similarly, non-decision decisions are poised to grow more common as the U.S-China rivalry makes explicit decisions unfavorable to one or the other superpower more costly for middle powers to adopt. An implication of this change may be that middle-power governments systematically shift away from formal, institutionalized policymaking toward more opaque, informal decision making in certain policy areas. For example, as the Japanese case suggests, governments may find it helpful to signal policy intentions to private companies without explicitly codifying or formalizing guidance or regulation in such instances. Such approaches may encounter domestic resistance from the private sector, either because they directly inflict additional costs on companies or because, as a result of their unstated character, they introduce uncertainty and unpredictability into the business environment. Telecommunications providers raised both these complaints in Germany and the UK. Beyond their domestic consequences, such informal measures can become a means to sidestepping a country's nominal commitments to preserving free trade and open markets, either under the World Trade Organization or in bilateral agreements, in high-technology sectors featuring incompletely understood security risks.[114]

[113] Edward D. Mansfield and Marc L. Busch, "The Political Economy of Nontariff Barriers: A Cross-National Analysis," *International Organization* 49, no. 4 (1995): 723–49, http://www.jstor.org/stable/2706924.
[114] Mascitelli and Chung, "Hue and Cry over Huawei," 4–5.

## Conclusion

Faced with a similar policy dilemma presented by Huawei's 5G equipment, the governments of Japan, the UK, and Germany appeared to respond in distinct ways. Japan acted early to restrict Huawei's role in supplying 5G technology without publicly issuing a formal policy. The UK at first allowed Huawei's limited participation, but then reversed itself in response to a U.S. restriction, ultimately adopting a complete ban. Germany continues to deliberate Huawei's partial access, but new regulatory measures have progressively reduced the incentives for operators electing to install the company's equipment. Although variant in form and timing, all three of these national responses share a crucial similarity: they all amount to non-decision decisions that point towards the increasing de facto, if not de jure, exclusion of 5G equipment from the Chinese company. For each government, the non-decision decision proved the least-worse way to extricate itself from a multi-level bind. Negotiating the prospects of either superpower's retaliation for an unfavorable decision, facing domestic operators' resistance to bans on Huawei imports, and, in the cases of the UK and Germany, contending with specialized agencies divided in their assessments of the technology's risk, these governments avoided making decisions that were either explicit, definitive, or singular. Instead, they opted for collections of measures and signals that over the course of two or more years erected barriers to the use of Huawei's equipment by domestic firms. These instances of non-decision decisions highlight the complexities of making policy at the intersection of technology, trade, and infrastructure in the age of digital trade and untenable distinctions between purely commercial products and products with national-security implications. Moreover, as a modality of policymaking, the non-decision decision presents an increasingly likely management strategy to middle powers, whose range of options is shrinking as the U.S.-PRC global contest for influence intensifies and broadens to new issue areas.