

Towards a common 5G strategy: the case for UK-Germany collaboration

Introduction

Over the last four years, the world has seen the United States withdraw from international leadership, turning away from its role as a defender of the international liberal order and as a reliable partner to allies in Europe. At the same time, Washington has escalated tensions with Beijing, forcing European partners who value the transatlantic alliance but who are increasingly reliant on their economic relationships with China to navigate an increasingly difficult path. Nowhere is the fallout from the US-China trade war more acutely felt than in the emerging technologies industry, especially 5G. In Europe – currently preoccupied with Brexit negotiations and responding to Covid-19 – a unique opportunity in 5G exists for the United Kingdom and Germany.



“... the United Kingdom can offer its considerable intelligence capabilities and tech industry to a 5G partnership with Germany”

In cooperating on 5G, the United Kingdom can offer its considerable intelligence capabilities and tech industry to a 5G partnership with Germany, whereas Berlin's leadership in the European Union can help keep Brussels and London in step as the UK adjusts to new trade policies and security guarantees in a post-Brexit world. As economically strong leaders within Europe and on the global stage, the UK and Germany should cooperate around 5G to ensure the security of their domestic critical infrastructures and to develop a set of international standards to create a safer, more resilient global 5G network.

The 5G landscape

The opportunities allowed by 5G technology will enhance data-driven industries and fields ranging from autonomous vehicles to smart-city development and other innovations not yet apparent. 5G will allow for increased data transfer speeds, lower latency between connected devices and greater digital connectivity across global networks. The capabilities offered by 5G stem from the virtualisation of network functions which traditionally take place on existing hardware in the current 4G and 3G environments.¹ 5G networks will still require physical components known as masts

or base stations to interface with mobile devices, but advances in cloud computing will allow many network functions to occur virtually in the network's core. Enhanced physical and cyber security measures will be paramount for network safety, and network vendors will play a far more significant role in contributing to 5G security as they will be responsible for running software updates and patches necessary to keep 5G networks operational.

The question of Huawei

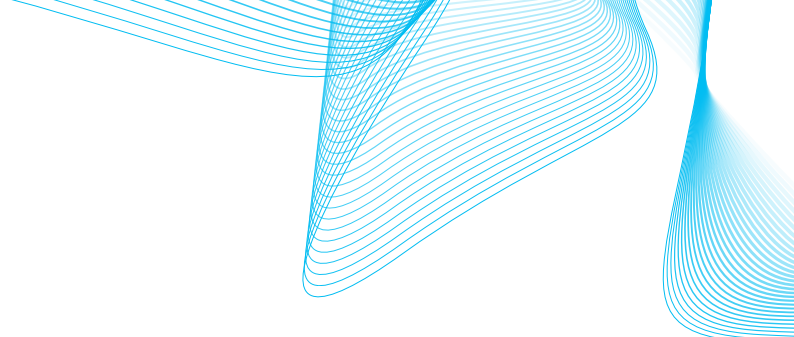
There are currently three leading companies operating in Europe that are capable of producing the components required for a 5G network rollout: Ericsson of Sweden, Nokia of Finland and Huawei of China. All three of these vendors are present in telecommunications networks around the world and have provided countries throughout Europe with the technology needed for 3G, 4G, and now 5G coverage. Huawei in particular has enjoyed widespread deployment due to its state-of-the-art technology offered at lower prices than competitors, a trade practice made possible through state subsidies and financing provided by Beijing. Despite its long partnership with European telecom operators, Huawei's trustworthiness and reliability have recently come under increased scrutiny.

Over the last three years, the United States has engaged in a campaign against Huawei, citing risks to national security. These concerns are due to Article 14 of China's 2017 National Intelligence Law, which requires any privately-owned entity within China to provide the state with support, assistance and cooperation on work related to China's national intelligence.² Western security experts interpret this law to mean that Beijing has the legal authority to compel private organisations to give Beijing access to their commercial networks or to otherwise share secure information contained within these networks.

Huawei has a long history of working with European telecommunications networks and is estimated to operate between 50 and 100 per cent of existing networks in some EU member states.³ For most European policymakers, the primary concerns surrounding 5G are economic. Governments are weighing the quickest route to 5G network deployment against an acceptable financial cost to avoid missing out on the economic opportunities stemming from 5G. Internationally, Australia became the first country to bar Huawei from its 5G rollout in July 2018. The United States followed suit amidst an escalating trade war with China, calling on European allies to ban the company from their 5G networks. To varying degrees, countries around the world are now reconsidering the risks of using Chinese tech in their 5G networks. The international community has watched the Huawei debate in Germany and the UK, two of the United States' closest European allies, with particular interest. Although the UK recently reached a decision regarding Huawei's presence in its 5G networks, Germany has yet to find a resolution to the Huawei problem.

The state of 5G in the UK

Of all European countries currently using Huawei technology in their telecom networks, the United Kingdom has a unique relationship with the Chinese company. In 2010, Huawei and the British government jointly created the Huawei Cyber Security



Evaluation Centre (HCSEC) which allows for closer cooperation between Huawei's UK division and the UK's National Cyber Security Centre (NCSC) to identify and address vulnerabilities stemming from Huawei technology present in British networks.⁴ As the leading cyber authority in the UK, the NCSC can liaise with Huawei through the HCSEC, vetting Huawei products before they enter the UK's telecom market and monitoring any risks that Huawei might pose domestically.⁵ Because of this screening centre and follow-on risk mitigation strategies, Huawei enjoys a deep-seated presence in the UK's domestic networks.



Because of this screening centre and follow-on risk mitigation strategies, Huawei enjoys a deep-seated presence in the UK's domestic networks”

The UK has four telecommunications operators vying for space in Britain's 5G rollout: BT, Vodafone UK, Three UK and O2. Of these four, only O2 operates without Huawei technology in its existing networks.⁶ In earlier generations of telecommunications infrastructure, Huawei has had a substantial role in setting up networks and providing the hardware components necessary for network function. Some estimates indicate that banning Huawei from Britain's 5G networks will result in millions of pounds in additional costs to network operators, delays in 5G rollout ranging between two to three years, and billions of pounds of potential economic revenue lost.⁷ The Huawei question, occurring in conjunction with an economically devastating global pandemic and ongoing Brexit debates that will determine the future of the UK's trade and security relationships, has been heavily debated in Britain.

Concern about the risks associated with Huawei technology and its inclusion in Britain's domestic 5G rollout stems back to a 2018 report released by the HCSEC's Oversight Board which identified vulnerabilities rooted in Huawei's engineering standards.⁸ A follow-on report launched in 2019 acknowledged “no material progress” in remediating the concerns laid out the year prior and ultimately provided only “limited assurance that all risks to UK national security from Huawei's involvement in the UK's critical networks [could] be sufficiently mitigated long-term.”⁹ Facing pressure from the United States and China to address the Huawei question, the NCSC released guidance in January 2020 which established practices for governing the role of high-risk vendors in UK networks: high-risk vendors were banned from the network core and could have only a limited presence, totalling no more than 35 per cent, in the tech required for the network periphery.¹⁰ This 35 per cent cap was designed to mitigate the inherent security concern stemming from a high-risk vendor's enhanced network presence without overly reducing supplier diversity within the network.¹¹

In an unusual about-face, a July 2020 decision from the NCSC and Government Communications Headquarters (GCHQ) reversed the initial decision to allow Huawei a place in the UK's domestic 5G rollout. Prohibitive US sanctions called into question Huawei's ability to source key parts needed for 5G infrastructure, forcing Huawei to use components that might not meet acceptable technical or security standards, and potentially resulting in vulnerabilities that could slip through screening mechanisms in place at the HCSEC and NCSC. In response, Downing Street issued a ban on purchasing Huawei 5G equipment beginning in 2021 and will require all telecom companies in the UK to remove existing Huawei tech from their 5G networks by the end of 2027.¹²

With the Huawei decision taken, Ericsson and Nokia remain the primary vendor options for the initial stage of the UK's 5G rollout, and British telecom operators are

struggling to guarantee multi-vendor security going forward. A notable exception to its peers, Vodafone UK has announced its intention to replace part of its existing Huawei kit with Open RAN technology, which allows operators to mix hardware components and integrate them within their networks regardless of component manufacturer.¹³ However, tech experts remain divided regarding Open RAN's security and performance when compared to single-vendor kit, and Vodafone's success in using Open RAN for 5G is far from guaranteed. In addition, the British government has also invited Tokyo-based NEC Corp to participate in the UK's 5G rollout, viewing NEC's involvement as a way to diversify the pool of suppliers working in UK networks.¹⁴ However, all four British operators already use Ericsson and Nokia in earlier generations of their networks, and it remains to be seen if NEC will receive any contracts for 5G.

The state of 5G in Germany


In contrast to the UK, Germany has not made a final decision on the Huawei debate and lawmakers remain divided on the issue. On the regulatory side, Germany has two main agencies responsible for its telecommunications industry and for preparing German networks for 5G capability. The Federal Office for Information Security (BSI) is the leading authority responsible for ensuring domestic cyber security.¹⁵ The Bundesnetzagentur (BNetzA) is Germany's regulatory authority that ensures compliance with German law governing the telecommunications sector.¹⁶ Both the BSI and the BNetzA are limited to making technical security assessments and providing the regulatory framework for 5G.¹⁷ In Berlin, the political debate about an exclusion of Chinese vendors continues to be hotly debated between the relevant ministries and will eventually have to be decided by the parliament.

Despite a keen sensitivity to foreign spying in their domestic networks, decision makers in Germany are divided on the risks of including Huawei in their 5G networks. On one hand, Chancellor Angela Merkel, supported by the Ministry of Economy and the heads of Germany's leading telecommunications companies, are against an outright ban on any tech vendor, including Huawei.¹⁸ Their concerns stem from the economic threat China can levy against German companies doing business in China should Berlin ban Huawei from its 5G rollout.¹⁹ On the other hand, members of the parliamentary Green Party and the Social Democrats are led by Foreign Minister Heiko Mass and German intelligence services in citing Huawei's risk to national security as grounds for exclusion from Germany's 5G networks.²⁰ The Christian Democratic Union (CDU), Chancellor Merkel's own party, is notably split on the issue.

This divide has resulted in a delay in Berlin's decision-making for over a year. Even now, a final ruling on allowing Huawei tech into Germany's 5G networks has yet to be reached. Recent reports from the Chancellery indicate that Chancellor Merkel and her ministers have outlined an initial approach foregoing a ban on any specific vendors from Germany's telecommunications networks. Instead, Berlin is considering a two-part approval procedure that would determine vendor participation in Germany's 5G networks. The first half of this proposal requires components to pass certification by the BSI prior to their use in German networks. The second half requires vendors to issue a "declaration of trustworthiness" to any equipment earmarked for use in Germany. Such declarations of trustworthiness will be assessed by the federal ministries of the Interior, Foreign Affairs, and Economy, and by the Chancellery.²¹ Although there is no specific



In Berlin, the political debate about an exclusion of Chinese vendors continues to be hotly debated between the relevant ministries and will eventually have to be decided by the parliament”



mention of Huawei in this initial legislation, experts expect that the proposed regulatory hurdles will be too high for Huawei to overcome and could result in Huawei's de facto ban from Germany's 5G networks.

Operationally, the telecommunications landscape is dominated by three primary companies vying for 5G: Deutsche Telekom, Telefónica Deutschland and Vodafone.²² A fourth company, 1&1 Drillisch, is likewise active in 5G but does not operate its own network infrastructure and will instead contract with an existing vendor to offer 5G services. Germany's telecom operators have decades-long histories of using Huawei technology in their networks and view the Chinese company as a quick, cost-effective way to reach 5G capability. Some have already begun replacing Huawei equipment as part of their 5G rollouts even as the debate surrounding Huawei continues.²³ With national elections on the horizon in 2021 and no clear indicators as to who will succeed Chancellor Merkel as head of the CDU, operators risk heavy financial losses and significant delays in achieving full 5G capability should the Bundestag's eventual decision on Huawei ban the vendor from Germany's 5G networks.²⁴

Recommendations for collaboration

To date, there has not been a great degree of collaboration between the UK and Germany around 5G. While Britain initially believed any risk from Huawei could be sufficiently managed, UK government officials walked back from this position and have since eliminated Huawei as a potential 5G network vendor. By contrast, Berlin has refused to take such a step and cannot seem to find a way forward on the issue. Despite their differences in approaching the Huawei problem, the United Kingdom and Germany can collaborate on critical 5G technology and network infrastructure in the following ways:

Establish a multilateral council on 5G security

The UK and Germany should lead the way in establishing a multilateral council on 5G that works towards international standard setting and collaborative practices for ensuring cross-border network security. The UK's existing proposal, a D10 group of democracies cooperating on 5G, focuses primarily on countering Huawei's dominance in 5G and overdependence on China's supply chains for sensitive technologies. The United States' Clean Network Initiative, another attempt at international coordination on 5G, specifically targets China and Huawei as adversaries in the race for 5G. Both organisations fail to recognise that their proposed member states each have distinct acceptable thresholds for Huawei's presence in their 5G rollouts, differing degrees of dependency on Huawei for their existing 3G and 4G networks, varying capacities to independently build or obtain the hardware needed for 5G emplacement, and individual priorities in choosing an alternate vendor to Huawei for their 5G network rollouts and domestic economies.²⁵

Instead, a council on 5G led by the UK and Germany should focus on establishing common standards for minimum security requirements, harmonising spectrum allocation for network connectivity and developing shared approaches to threat or vulnerability detection and response. It should initially focus on intra-European membership with mechanisms in place for the eventual ascension of like-minded countries seeking international collaboration and security on 5G and future tech.

Though the UK would be unlikely to join a European Union-led initiative following its final separation from the EU in January 2021, a council on 5G aimed at a multilateral approach could still be based on the model of an existing EU institution. An idea first suggested by Chancellor Merkel, such a council could be modelled on the European Medicines Agency, which collaborates with national authorities within each member state to provide regulatory oversight for medications dispersed throughout the EU.²⁶ In the same way, members of a council on 5G would benefit from sharing resources and expertise while working within a unifying 5G framework to ensure interoperability and network connectivity across borders. Such a framework could draw in part from the recommendations laid out in the European Commission's Toolbox on 5G Cybersecurity. By integrating input from each stakeholder's relevant authorities, these recommendations could be adapted to form a kind of roadmap for a 5G council with regulatory oversight over members. A council on 5G would also provide the UK, Germany and other European countries with stronger positioning vis-à-vis China not just on 5G technology but on other issues related to critical infrastructure, supply chain vulnerability or economic trade security.

Invest in international digital infrastructure development

A critical and yet sometimes overlooked component of the 5G debate is Europe's continued dependence on other countries for the technological components (such as semi-conductors) needed 1) to emplace 5G in domestic telecommunications networks; and 2) to fully take advantage of the technological advances stemming from 5G that will become available once widespread commercial rollout is underway.²⁷ In effect, the international community continues to be dependent on the same few companies for innovation and advancement stemming from 5G and eventually 6G technology and beyond. As the continent's two leaders in tech innovation and economic might, London and Berlin should lead the effort to overcome this persistent problem. This endeavour can be tackled in two ways:



... the international community continues to be dependent on the same few companies for innovation and advancement stemming from 5G and eventually 6G technology and beyond”

1. Germany and the UK should invest in nascent digital infrastructure enterprises in developing countries around the world.²⁸ Possible options for financial investment in the telecommunications industry include India and Vietnam, both of which are in the process of developing homegrown 5G equipment and networks independent of Huawei.²⁹ Investments such as these will help create a global telecom marketplace that offers a more diverse supply chain and vendor selection, two criteria critical for ensuring domestic network security.
2. Germany and the UK should prioritise investing in European companies working on tech innovation. The funding made available by the European recovery fund should also be used to invest in the bloc's domestic tech industries.³⁰ Although the European recovery fund does not extend to the United Kingdom, London should work closely with Brussels and Berlin to support European tech challengers able to stand up to China and the US. A pan-European approach would grant London access to the EU's single market economy and the burgeoning tech industry found outside the dominant hubs of Berlin and Paris while simultaneously allowing EU-based tech companies to work with counterparts in London, helping to fuel the continued growth of the European tech sector.³¹



Create a role for NATO in 5G

Recent reports out of Washington DC call for NATO to engage in the early stages of 5G network deployment, correctly identifying the importance of NATO's focus on 5G while rightfully acknowledging that NATO cannot be the driver behind nor the enforcer of a nation-wide telecommunications overhaul in allied countries.³² Instead, NATO should adhere to the principle of ensuring collective defence through cooperation and trust-building around 5G. As the two leading European contributors to NATO, the UK and Germany should lead other allies in directing NATO's financial, technical and political resources towards ensuring all member countries can integrate 5G technology in their individual networks in such a way that cross-network communication and joint military capability are assured. In the 5G environment, NATO's continued efficacy will rely heavily on the interoperability of numerous information-sharing and data-transmission systems in order to fully integrate emerging tech capabilities on the battlefield and at the strategic level. As more and more member countries begin their domestic 5G rollouts, NATO leadership must make the consequences of a disjointed approach to network and vendor security clear.



NATO should adhere to the principle of ensuring collective defence through cooperation and trust-building around 5G”

Beyond ensuring more harmonised telecommunications networks throughout the alliance, tackling the issue of 5G and the associated geopolitical security concerns can also help NATO establish a unified, transatlantic approach to China's growing influence in NATO's backyard and dominance in the cybersecurity realm.³³ NATO membership does not dictate an individual country's relationship with China, and the wide range of economic and political ties to Beijing found throughout member countries can make it difficult to coordinate an effect response to China's increasing presence in NATO's traditional security spheres. A common approach to 5G technology, led by Germany and the UK and in close collaboration with the United States, can strengthen NATO's resolve in standing up to China's encroachment.

Expand the HCSEC model to Germany and other European allies

In Germany, Berlin's still-unfinalised response to the Huawei question lays out a security evaluation strategy requiring not only the testing of components for technical vulnerabilities but a political assessment of the trustworthiness of any vendor operating in Germany's telecom networks.³⁴ In setting up these evaluation mechanisms, Germany should look to the UK's HCSEC model for inspiration, which allows government-led evaluation of Huawei technology and components prior to signing off on operator use of Huawei's equipment. The HCSEC model allows the equipment to be tested for vulnerabilities at an arguably higher standard (ie at the government level) rather than at the standards of individual network operators which must consider cost in their assessment protocol.

Rather than tasking the BSI with sole responsibility for technical evaluation and allocating responsibility for the trustworthiness assessment among the Foreign Ministry, Ministry of Economy, and Interior Ministry – all of which have competing priorities and varying degrees of support for Chinese investment in Germany's networks – a collaborative HCSEC-like entity would allow a greater degree of localised government cooperation, technical expertise and improved oversight for any foreign vendor seeking access to Germany's networks. These centres would also allow Berlin to test for vulnerabilities that might exist in telecom equipment and components already in place in Germany's older generation of networks, many of which have a significant Huawei

presence embedded in their operations. The establishment of these centres could be codified in the Bundestag's forthcoming IT Security law 2.0, and cooperation from the vendor in building the centres could be a criterion of the proposed verification of trustworthiness vendors must receive prior to participating in Germany's 5G network rollout.

Continue research on Open RAN technology

As a final recommendation, Berlin and London should continue research on Open RAN technology. For many telecom operators and government officials concerned with the national security implications of a commercial 5G rollout, Open RAN is thought to be an umbrella solution for increasing vendor-diversity within networks and ensuring operational redundancy and robustness should a hardware component or piece of coding fail. The idea behind Open RAN allows for a more diverse 5G ecosystem as it further disaggregates the hardware and software architecture available for use in building 5G networks, offering more opportunities for network diversity than single-vendor equipment.³⁵

However, increased variety also means increased vulnerability, and experts are divided as to whether Open RAN offers the same degree of security as single-origin 5G kit. Experts also question if the one-size-fits-all solutions available through Open RAN can offer the same higher speeds and reduced latency as a single-vendor operation. When viewed through a security lens, further research into Open RAN is a necessary and worthwhile endeavour. The UK and Germany should collaborate around Open RAN, throwing the might of their respective tech facilities into the research and working collaboratively to ensure high international standards of security at the outset.

Conclusion

Dealing with the outbreak of the coronavirus pandemic has delayed 5G rollouts around the world, diverting attention from the issue but also providing enough of a delay for the international community to realise the importance of a joint approach to 5G security. Now however, with countries in the later stages of Covid-19 management and with promising vaccine trials underway, countries are again looking to the economic opportunities of 5G as a way to boost their domestic economies post-pandemic. The United Kingdom and Germany would do well to take advantage of this common threat perception to shape the way 5G is deployed around the world

References

1. Connor Craven, "What Is 5G Network Infrastructure? Definition," SDxCentral, last modified January 4 2020, <https://www.sdxcentral.com/5g/definitions/5g-network-infrastructure/>
2. Bonnie Girard, "The Real Danger of China's National Intelligence Law," The Diplomat, last modified February 23 2019, <https://thediplomat.com/2019/02/the-real-danger-of-chinas-national-intelligence-law/>
3. *The Chinese View of Strategic Competition with the United States: Testimony before the US-China Economic and Security Review Commission*, June 24 2020, Statement of Dr Janka Oertel, Director, Asia Programme, European Council on Foreign Relations
4. *Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board Annual Report 2020*, (2020), <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attach->

- [ment_data/file/923309/Huawei_Cyber_Security_Evaluation_Centre_HCSEC_Oversight_Board-annual_report_2020.pdf](#)
5. Ibid.
 6. Iain Morris, “Huawei Avoidance Strategy is Paying off for UK’s O2,” Light Reading, last modified June 11 2020, <https://www.lightreading.com/5g/huawei-avoidance-strategy-is-paying-off-for-uks-o2/d/d-id/761639>
 7. Bundesnetzagentur, “Press Release: Spectrum Auction Comes to an End,” issued June 13 2019, https://www.bundesnetzagentur.de/SharedDocs/Downloads/EN/BNetzA/PressSection/PressReleases/2019/20190612_auction.pdf;jsessionid=BA14B617C4AFB7D4DE68EBF-854413CC7?__blob=publicationFile&v=4
 8. United Kingdom House of Commons Committees, Defence Committee, *The Security of 5G* (October 8 2020), p37
 9. Ibid., p37
 10. Ibid., p25
 11. NIS Cooperation Group, *Report on Member States’ Progress in Implementing the EU Toolbox on 5G Cybersecurity* (2020), p7, <https://ec.europa.eu/digital-single-market/en/news/report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity>
 12. Reuters, “Factbox: Huawei’s Involvement in 5G Telecoms Networks Around the World,” last modified October 20 2020, <https://www.reuters.com/article/us-sweden-huawei-global-factbox/factbox-huaweis-involvement-in-5g-telecoms-networks-around-the-world-idUSKB-N2751A1>
 13. Iain Morris, “Vodafone UK to Swap Big Part of Huawei for Open RAN,” Light Reading, last modified November 2 2020, <https://www.lightreading.com/vodafone-uk-to-swap-big-part-of-huawei-for-open-ran/d/d-id/765104>
 14. “NEC to Support 5G Networks in UK as Alternative to Huawei,” Nikkei Asia, last modified October 26 2020, [https://asia.nikkei.com/Spotlight/Huawei-crackdown/NEC-to-support-5G-networks-in-UK-as-alternative-to-Huawei#:~:text=LONDON%20\(Kyodo\)%20%2D%2D%20Major%20Japanese.according%20to%20the%20British%20government](https://asia.nikkei.com/Spotlight/Huawei-crackdown/NEC-to-support-5G-networks-in-UK-as-alternative-to-Huawei#:~:text=LONDON%20(Kyodo)%20%2D%2D%20Major%20Japanese.according%20to%20the%20British%20government)
 15. BSI - Bundesamt für Sicherheit in Der Informationstechnik, “The BSI,” accessed November 13 2020, https://www.bsi.bund.de/EN/TheBSI/thebsi_node.html
 16. Bundesnetzagentur, „The Bundesnetzagentur’s Duties,“ accessed November 13 2020, https://www.bundesnetzagentur.de/EN/General/Bundesnetzagentur/About/Functions/functions_node.html;jsessionid=40BA8B412B1017193115BEF09EF62C0D
 17. Philipp Grill, “Huawei Shouldn’t Be Getting Its Hopes Up for German 5G Expansion Just Yet,” translated by Daniel Eck, Euractiv, last modified February 13 2020, <https://www.euractiv.com/section/5g/news/huawei-shouldnt-be-getting-its-hopes-up-for-german-5g-expansion-just-yet/>
 18. Laurens Cerulus, “How U.S. Restrictions Drove Deutsche Telekom and Huawei Closer Together,” *POLITICO*, last modified July 7 2020, <https://www.politico.com/news/2020/07/07/deutsche-telekom-huawei-us-restrictions-350252>
 19. Katrin Bennhold and Jack Ewing, “In Huawei Battle, China Threatens Germany ‘Where It Hurts’: Automakers,” *The New York Times*, last modified January 16 2020, <https://www.nytimes.com/2020/01/16/world/europe/huawei-germany-china-5g-automakers.html>. <https://www.nytimes.com/2020/01/16/world/europe/huawei-germany-china-5g-automakers.html>
 20. Cerulus, “How U.S. Restrictions Drove Deutsche Telekom and Huawei Closer Together.”
 21. Till Hoppe and Moritz Koch, “Hohe Hürden Für Huawei – „Das Verfahren Kommt Einem Ausschluss Gleich“,” *Handelsblatt*, last modified September 9 2020, translated with DeepL translator, <https://www.handelsblatt.com/politik/international/5g-mobilfunknetz-hohe-huerden-fuer-huawei-das-verfahren-kommt-einem-ausschluss-gleich/26229670.html>
 22. “America’s War on Huawei Nears its Endgame,” *The Economist*, last modified July 16 2020, <https://www.economist.com/briefing/2020/07/16/americas-war-on-huawei-nears-its-endgame>
 23. Moritz Koch, “Ringten Um Huawei-Ausschluss: Kalter Krieg Um Saubere Netze,” *Handelsblatt*, last modified September 24 2020, translated with DeepL translator, <https://>

- www.handelsblatt.com/politik/international/5g-netzausbau-ringen-um-huawei-ausschluss-kalter-krieg-um-saubere-netze/26215640.html?ticket=ST-15486329-jrHLfj0RvZg2h-QLrThji-ap5
24. “Germany’s Ruling Party is Making a Hash of Choosing Its Next Leader,” *The Economist*, last modified October 31 2020, <https://www.economist.com/leaders/2020/10/31/germanys-ruling-party-is-making-a-hash-of-choosing-its-next-leader>
 25. Erik Brattberg and Ben Judah, “Forget the G-7, Build the D-10,” *Foreign Policy*, last modified June 10 2020, <https://foreignpolicy.com/2020/06/10/g7-d10-democracy-trump-europe/>
 26. Arne Delfs, “Angela Merkel Demands European 5G Agency for Joint China Approach,” Bloomberg, last modified November 27 2019, <https://www.bloomberg.com/news/articles/2019-11-27/merkel-demands-european-5g-agency-for-joint-china-approach>
 27. Jan-Peter Kleinhaus, “Europe’s 5G Challenge and Why There is No Easy Way out,” TechNode, last modified June 25 2019, <https://technode.com/2019/06/25/europes-5g-challenge-and-why-there-is-no-easy-way-out/>
 28. Andrew Small, Phone Interview, November 12 2020
 29. Iain Morris, “Vietnam Makes Big Bet on Homegrown 5G,” Light Reading, last modified January 20 2020, <https://www.lightreading.com/asia/vietnam-makes-big-bet-on-homegrown-5g/d/d-id/756939>; Gagandeep Kaur, “India’s Jio Looks to Acquire Firms to Fire Its 5G Ambitions,” Light Reading, last modified September 1 2020, <https://www.lightreading.com/5g/indias-jio-looks-to-acquire-firms-to-fire-its-5g-ambitions/d/d-id/763572>
 30. Jonathan Hachenbroich et al., *Defending Europe’s Economic Sovereignty: New Ways to Resist Economic Coercion*, (European Council on Foreign Relations, 2020), https://ecfr.eu/publication/defending_europe_economic_sovereignty_new_ways_to_resist_economic_coercion/
 31. Joe Schorge, “The Next Silicon Valley Won’t Be in the US,” Quartz, last modified December 11 2019, <https://qz.com/1764868/the-next-silicon-valley-is-in-europe/>
 32. Christopher Skaluba et al., *NATO 20/2020: Twenty Bold Ideas to Reimagine the Alliance After the 2020 US Election*, (Atlantic Council, 2020), <https://www.atlanticcouncil.org/nato20-2020/>
 33. Oertel, *Testimony before the US-China Economic and Security Review Commission*
 34. Hoppe and Koch, “Hohe Hürden Für Huawei”
 35. Rene Summer, “Mobile Radio Access Networks: What Policy Makers Need to Know,” Ericsson.com, last modified September 17 2020, <https://www.ericsson.com/en/blog/2020/9/ran-what-policy-makers-need-to-know>

This report is part of a Policy Institute project investigating defence cooperation between the UK and Germany, funded by the Hanns Seidel Foundation. Visit [our website](#) to find out more about the project.

About the author

Beryl Thomas is an Alexander von Humboldt Foundation German Chancellor Fellow at the European Council on Foreign Relations.



The Policy Institute

The Policy Institute at King's College London works to solve society's challenges with evidence and expertise.

We combine the rigour of academia with the agility of a consultancy and the connectedness of a think tank.

Our research draws on many disciplines and methods, making use of the skills, expertise and resources of not only the institute, but the university and its wider network too.

Connect with us

 [@policyatkings](https://twitter.com/policyatkings)  kcl.ac.uk/policy-institute

