

The Cold Wind of Exclusion

Rachael Falk, CEO Cyber Security Cooperative Research Centre

An earlier version of this article has been published in condensed form as “Can the ‘core’ and ‘edge’ of a 5G network really be separated?” on the ASPI Strategist’.

January 2020

About the Author

Ms Rachael Falk is the Chief Executive Officer of the Cyber Security Cooperative Research Centre (Cyber Security CRC). Ms Falk comes to the Cyber CRC with a strong commercial and cyber security background having practiced as a lawyer for 15 years

both in leading law firms in Australia and the UK and also in-house at Telstra Corporation Limited. Ms Falk became Telstra’s first General Manager of Cyber Influence. Ms Falk is a regular commentator on topical cyber security issues in Australia.

There can be no doubt that the Australian government's decision to ban 'high risk vendors' from its 5G network build caused ripples not just through the Five Eyes community but in key markets where these 'high risk vendors' already has key customers. One of those such customers was Germany.

No specific 'high risk vendor' was named by the Australian government¹, however, the media swiftly named Huawei after the then director-general of the Australian Signals Directorate (ASD) noted in a public speech in October 2018:

"It would be naive to think we can manage these strategic and technology risks by holding back change. Like everything, it is a question of finding the right balance between leveraging all the advantages that these new shifts bring – and protecting Australians, our values and our way of life.

*These twin themes of technological and strategic economic shifts can be seen in the government's recent decision to prohibit telecommunications carriers from using high-risk vendors in 5G networks."*²

In a visit to Germany in June 2019, it became apparent that this was a country that was grappling with a multitude of tensions when it came to opening the door to a potential 5G vendor that other key countries had considered to be a risk. The Five Eyes' decisions (or deliberations, at least) have also slowly become public.

Australia's position with respect to Huawei was hardly new. And risk based decisions when it came to network operators were not new.

In 2012, the Australian government famously banned Huawei from taking part in the National Broadband Network (NBN)

build. However, 2012 was a long time ago and the public narrative (from government, at least) around restriction of such vendors was quite different: there was none. No public statement, no intelligence official publicly talking about it. Nothing. The news dribbled out and was confirmed by the then National Security Advisor, Dr Margot McCarthy before a Senate Estimates Committee hearing in 2013. Importantly, she noted that 'it was a risk based decision to exclude Huawei from the National Broadband Network.'³

Trust and trading partners are also a huge influence in when or if decisions like excluding a vendor from building a piece of critical infrastructure should be made public. In 2012, Australia's largest trading partner was China. The lack of public narrative could be explained away in the context of a trade relationship. Or it could be explained in the context of a different time. A time when the public narrative tended to be less direct.

The 2012 NBN decision also didn't really spook our Allies and certainly not Germany. The only 'spooking' (if there were such a thing) came from the US House Intelligence Committee which had issued a damning report on Chinese vendors and trustworthiness. The wave of distrust may have been quiet here in Australia but it was building up in the United States of America. The arguments of trust were often

interwoven with theft of intellectual property and several indictments for the arrest of Chinese nationals accused of spiriting out highly sensitive US secrets and / or of commercial espionage.

However, the NBN decision was 7 years ago and even then there were questions in the US about Chinese law compelling its citizens to cooperate with requests from the Chinese government.

*"..under Chinese law, ZTE and Huawei would be obligated to cooperate with any request by the Chinese government to use their systems or access them for malicious purposes under the guise of state security."*⁴

Chinese law and how it operates is important when it comes to extraterritoriality. According to the Australian Strategic Policy Institute summary of Chinese law:

'For Chinese citizens and companies alike, participation in 'intelligence work' is a legal responsibility and obligation, regardless of geographic boundaries.

This requirement is consistent across several laws on the protection of China's state security. For instance, Article 7 of the National Intelligence Law (国家情报法) declares:

*Any organisation and citizen shall, in accordance with the law, support, provide assistance, and cooperate in national intelligence work, and guard the secrecy of any national intelligence work that they are aware of. The state shall protect individuals and organisations that support, cooperate with, and collaborate in national intelligence work.*⁵

This can be summarised by *'For Chinese citizens and companies alike, participation in 'intelligence work' is a legal responsibility and obligation, regardless of geographic boundaries.'*⁶ In short, that can mean the ability for the Chinese government to influence/

interfere with/ have access to key assets of national interest and in this case, it would mean Australia's 5G network.

At the same October 2018 National Security Dinner, ASD's Director-General spoke publicly about the risk assessment that ASD carried out as part of their risk assessment for government. In short, according to ASD, once a vendor was embedded in the actual network, then for a high risk vendor, it then just becomes a matter of capability and intent⁷. The ability to interfere with or cause harm (at the direction of their government) exists irrespective of the wishes of that company's leadership. Since then, there has been much talk of the 'core' and 'edge' in a 5G network.

In contrast, ASD's UK equivalent, the General Communications Head Quarters (GCHQ) seemed to form a different view⁸ and consequently, the UK government's approach as to 5G vendors was different. And perhaps not surprisingly, the UK also had agreed (many years ago) to having a Huawei 'cell' that assesses Huawei code before it is used⁹. The 5G network build decision is a matter for the UK government and they are perfectly entitled to take a different decision to other Five Eyes partners. It seems, according to news reports, that the 5G decision was subject to heated debate in Cabinet and there was no uniform view as to where the United Kingdom sat with respect to excluding high risk vendors. However, in terms of a public narrative it was the start of the 'core versus edge' narrative. It could be said that Australia was not in this camp.

Was the 'core versus edge' camp looking for convenient nuance in order to justify their decision or to soften the blow for Huawei?

So where did all of this leave Germany in June 2019? It appears somewhat in the middle. Germany did not seem to want to

adopt the direct Australian approach with one organisation we visited saying that “Germany would never directly exclude a company in a procurement process”. Some German organisations labelled the Australian decision as “geopolitical”. Often talk moved to China being regarded as less of a threat because it was not close geographically which is ironic given the conduit of cyber has no borders.

Overwhelming, we heard that Germany wanted to be in a position to ‘trust and verify’ and that it would prefer to be able to ascertain (or perhaps exclude or control?) its vendors on that basis. However, when pressed to explain how an approach of trust and verify when even the best run Chinese company can be subject to its domestic law and no German company would be the wiser, they struggled to articulate how this might actually achieve greater security. Some shifted uncomfortably when we asked why a ban on high risk vendors could not occur. There was also talk of a broader European strategy and that one country could not dictate the procurement process. Although apparently these decisions are made a ‘national level’ and not at the EU level.

The sense was when we left Berlin on a very warm Summer afternoon that they were no closer to a 5G network build procurement decision that enabled the German government to effectively manage the risks of allowing a high risk vendor as part of the 5G build. There was a sense of unease coupled with the tension of knowing they had to act decisively.

Now in early 2020, the leaves have long since fallen and the cold wind of pressure to act would no doubt have been felt in the Bundestag. While the situation with respect to the build of the 5G network remains very fluid at the moment - and there

are dissenting factions within the party on this matter - it appears the CDU would lean towards deciding to allow Huawei to take part in Germany’s 5G bidding¹⁰. Such a move has been labelled a ‘Faustian bargain’ in that it is suggested the Chancellor can put Germany’s economic interests first but potentially jeopardise international security in the long term¹¹.

It is important to look at the actual ‘decision’ the CDU leadership proposes to make. So far, what we seem to know is that Huawei would be included in the 5G network build procurement process.

According to a document apparently endorsed by the CDU leadership¹², it appears they might advocate for adopting a variant of the ‘core versus edge’ approach. The document notes that *‘the core network must fulfill the highest security requirements... the government should also have increased security requirements for the peripheral 5G network without jeopardising the immediate transition to 5G’* and that *‘...no company should have a presence in the network infrastructure no higher than 50% by 2025. In the case of foreign suppliers, a maximum of 30% of the periphery (edge) of the network.’* It is implied that all core network suppliers should be European.

It has also been suggested that the decision to not exclude Huawei from the 5G German build is based on commercial and trade interests that have prevailed over security interests. According to *Foreign Policy*, Germany is heavily reliant on the Chinese market and according to unnamed ‘German Officials’ that ‘Merkel was warned by Chinese leaders that an exclusion of the Shenzhen - based group from the German 5G network would have serious consequences for bilateral economic ties’.¹³

What is clear is that Germany wants to pursue a different path, and that is its choice. To let many vendors compete in the procurement process for any critical infrastructure build is inclusive and this is in keeping with the organisations we spoke with in June 2019. The sense that direct exclusion was not seen as the right thing to do. Or possibly, the impact upon German / China trade relations was too great? Another factor could be that Huawei has partnered with Deutsche Telekom and other carriers in Germany for many years so the cost of replacing such equipment would be considerable.¹⁴

Germany's possible decision to let Huawei take part in the 5G procurement process feeds into a broader EU issue about security as a whole (as in, the EU) rather than individual member States deciding what is in their national interests. There does seem to be a tension between the German way, and the EU way and it is unclear whether there can really be a unified approach to building of a 5G network particularly because each EU member state may have different incumbent providers who in turn have relationships with many overseas vendors like Huawei.

It will be interesting to see as Germany moves through the 5G procurement process how it will (or will not) be influenced by the different approaches other nations have taken. Similarly, whether it will be influenced by a broader EU approach to national security.

Will Germany decide that it is neither the 'core' or the 'edge' that matters - and the security risks will be managed by limiting foreign network operators as suggested in the CDU document? Irrespective of which path Germany takes, it is bound to attract attention and be closely watched.

Endnotes

- i See <https://www.aspistrategist.org.au/can-the-core-and-edge-of-a-5g-network-really-be-separated/>
- 1 <https://www.minister.communications.gov.au/minister/mitch-fifield/news/government-provides-5g-security-guidance-australian-carriers>
- 2 <https://www.asd.gov.au/publications/speech-ASPI-national-security-dinner> Speech by the director-general ASD, ASPI National Security Dinner, 29 October 2018
- 3 https://parlinfo.aph.gov.au/parlInfo/download/committees/estimate/bbcd742-8b94-4a59-952b-08a9c3964c43/toc_pdf/Finance%20and%20Public%20Administration%20Legislation%20Committee_2013_02_11_1661_Official.pdf;fileType=application%2Fpdf [pages 149-151]
- 4 US House of Representatives, Investigative Report on the US National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE, https://fas.org/irp/congress/2012_rpt/huawei.pdf, page 3
- 5 Samantha Hoffman and Elsa Kania, ASPI, The Strategist, 'Huawei and the ambiguity of China's intelligence and counter espionage laws' <https://www.aspistrategist.org.au/huawei-and-the-ambiguity-of-chinas-intelligence-and-counter-espionage-laws/>
- 6 *ibid*
- 7 <https://www.asd.gov.au/publications/speech-ASPI-national-security-dinner>
- 8 <https://www.bbc.com/news/technology-48035802>
- 9 Similar offers (or suggestions for a cell) as far back as 2012 had been made by Huawei in Australia which have never been accepted by the Australian government.
- 10 Theresa Fallon, 'Germany's Faustian Bargain with China', The Diplomat, November 8, 2019
- 11 *Ibid*
- 12 Tweet from Noah Barkin, 18 December 2019 noting 'The CDU leadership in parliament adopted this paper on #5G yesterday evening. It is softer in key areas, paving the way (by my reading) for a #Huawei role in the German network...'
- 13 'Europe's Backlash Against Huawei has Arrived, Foreign Policy, November 27 2019
- 14 The Diplomat, Germany's Faustian Bargain with China, Theresa Fallon, November 8, 2019

Copyright

© Konrad Adenauer Stiftung (Australia) Limited, January 2019

Editor

Katja Theodorakis

Publisher

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

11/3 Sydney Avenue

Barton, ACT 2600

Australia

Tel: +61 2 6154 9322

www.kas.de/australia

Disclaimer

All rights reserved. No part of this publication may be reprinted or reproduced or utilised in any form or by any electronic, mechanical or other means, now known or hereafter invented, including photocopying or recording, or in any information storage or retrieval system, without permission from the publisher.

The opinions expressed in this publication rests exclusively with the authors and their interpretations do not necessarily reflect the views or the policy of the Konrad Adenauer Stiftung.

Design, Layout and Typeset

Swell Design Group

Paper



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