Norwegian Institute of International Affairs

Policy Brief
[ 5 / 2019 ]

# Finding a European response to Huawei's 5G ambitions

*Valentin Weber*

**Summary**

This policy brief suggests that European countries should institute national reviewing boards overseen by intelligence agencies to vet Huawei equipment. If that is not feasible due to a lack of resources or capabilities especially among smaller countries, European governments should consider pooling resources and create a common reviewing board. This would also prevent duplication of efforts on national levels. European authorities should also demand from Huawei to clearly separate its international from its domestic business operations in order to further reduce the risk to the confidentiality, integrity, and availability of European mobile networks.

During recent months Huawei has appeared on headlines of international newspapers almost on a daily basis. The US, Australia and New Zealand have publicly stated that they will take a harsher line in restricting Huawei from government contracts and building their 5G networks. Huawei on the other hand has stated that it poses no risk to foreign governments and that any allegations are politically motivated.[1]

The following paragraphs examine the security risk posed by Huawei building European 5G networks. Based on the assessment of the company's cyber security record, the legal environment in China, and cases where Huawei was associated with espionage this policy brief proposes recommendations for European governments that could potentially reduce the risk of buying gear from risky vendors.

**Huawei's cyber security**

Besides assurances from Huawei's side that its equipment is secure, as well as announcements that it will increase cyber security, information is scarce as to whether Huawei equipment poses a cyber security risk.

One of the rare sources on this matter is the UK's Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board. This board is overseen by the UK's National Cyber Security Centre, which is part of GCHQ (Government Communications Headquarters), the UK's signals intelligence agency. The Oversight Board has repeatedly reported on Huawei's cyber security. An annual report released in July 2018 raised two concerns. The Oversight Board maintained that Huawei's source code can cause systems to behave differently in various environments and "security critical third-party software used in a variety of products was not subject to sufficient control."[2]

While the Board did not report any malicious activity from the company's side, Huawei's reply is sobering. It states that it may need three to five years to mitigate the two flaws pointed out by the NCSC.[3] By then, most decisions about 5G contracts will have been taken and construction of 5G networks will already be underway.

**Domestic legal environment**

While Huawei claims that there is no Chinese law that requires it to install backdoors, the company is compelled by Article 7 of the 2017 National

Intelligence Law to support China's intelligence activities and stay quiet about its involvement.[4] This means that even if Huawei was implicated in intelligence endeavours it is prohibited by law to say so publicly. Even if the law was amended, revoked, or Huawei exempt from the law, it is still highly likely that the government would get access to any data it wanted. As Huawei is heavily reliant on government subsidies and the goodwill of the party it has little leverage to resist government demand for access.[5] This may include requests for European data. In a letter to the UK parliament Huawei claims that "relevant provisions of China's National Intelligence Law *do not appear* [emphasis added] to have extraterritorial effect…"[6] Huawei's interpretation of the law is not reassuring and rather indicates that requests for data by the Chinese government could also apply extraterritorially.

The law also requires Huawei to have a Communist Party Committee within its structures, which is usually based at a decision-making level.[7] [8] The Committee ensures that the company's daily operations are aligned with the Communist party's goals.[9] A potential counterargument could be made claiming that Huawei is a privately held company, which ensures independence vis-à-vis authorities. However, as Milhaupt and Zheng have demonstrated there is little difference between state-owned companies and private companies in terms of party control over these entities. *"Many large, successful Chinese firms [both SOEs and POEs] exhibit substantial similarities in terms of market dominance, receipt of state subsidies, proximity to state power, and execution of the state's developmental policy objectives, …"*[10] In short, ownership is not a good indicator of party influence over Chinese economic actors.



**Cases of espionage**

The following two cases show that European governments need to be cautious when entrusting the construction of core internet infrastructure to Huawei. It is unlikely that Huawei has been unaware if not complicit in the Chinese government's previous attempts to develop and deploy backdoors geared towards its systems.

Firstly, Huawei has had closer ties to the Chinese intelligence apparatus than it wants to admit. Huawei was a partner to Boyusec, a company that was working for the Chinese Ministry of State Security (MSS). [11] Boyusec was integral to APT3, an aggressive espionage group of the MSS that has been linked to cyberattacks on telecommunications, defence industry, and government departments in Hong Kong and the US. An internal intelligence Pentagon report further maintained that Huawei and Boyusec were jointly developing products that contained backdoors. These would "allow Chinese intelligence to capture data and control computer and telecommunications equipment."[12] Until Boyusec's closure in 2017, its only other partner besides Huawei was the Guangdong Information Technology Security Evaluation Center (Guangdong ITSEC), which "is a field site for a branch of the MSS."[13]

Huawei's closeness to the Ministry of State Security was also highlighted in a CIA report which showed that Huawei's former chairwoman, Sun Yafang, had worked for the MSS's communications department.[14]

Secondly, a more widely reported spying activity that Huawei was involved in is the snooping on the African Union's headquarters in Addis Ababa. The building was financed by the Chinese government and the telecommunications equipment provided by Huawei.[15] The gist of the story is that data was flowing from Addis Ababa to unknown servers in Shanghai for five years (2012-2017). Once *Le Monde* broke the story the African Union changed their servers and declined help from the Chinese government to configure them.[16] One could imagine the following scenario where data was flowing for five years from Europe to Shanghai. Huawei would most likely state that it had no knowledge of such an occurrence. But how much of a comfort would Huawei's statement be to European authorities?

**Recommendations**

Considering all of the above, European authorities have several options for managing Huawei's risk.

***Option 1: leave it as it is.*** This entails keeping current security screenings, which occur without an institutionalised assistance from national intelligence agencies. This option is not recommended, since it would neither address Huawei's cyber security risk, nor China's domestic legal environment that gives the Chinese government major control over a company's decisions.

***Option 2: ban Huawei and ZTE.*** This option would decrease the attack surface for Chinese spying. China would have to exploit foreign equipment, which is

much harder than if one has intrinsic knowledge of the hardware as well as software. Furthermore, this option would also make it ineffective for China to pressure companies into accessing their systems.

However, despite the security reducing benefits of this option, the consequences remain large. Shutting out Huawei and ZTE (a company raising similar security concerns), would mean that European governments excluded 41% of the market which would in turn strongly reduce competition.[17] Moreover, China has threatened with trade retaliation if governments decide to ban Chinese equipment makers.[18] Retaliation could arguably be reduced if Europe acted unitedly, thereby reducing the impact and likelihood of Chinese sanctions imposed on individual countries.

***Option 3: enhanced security coupled with corporate reform.*** This choice would entail the creation of national Huawei reviewing boards, where intelligence agencies vet software and hardware. The UK has adopted this approach and Germany has followed suit.[19] The advantages of this option are that cyber security risks can be reduced. However, other concerns remain, because Chinese domestic and foreign policy are inextricably linked with each other.[20] Huawei could still collaborate with the Chinese government and give it access to their systems.[21] Then even the best cyber security has no effect. In order to increase trust Huawei needs to separate its domestic from its international corporate structure. *The Economist* has proposed several actions. Huawei ought to "appoint foreign directors, recruit Western investors and set up subsidiaries overseas that have their own boards and indigenous managers."[22]

If both these conditions are met (enhanced security and corporate reform), then a mix of Chinese and other international suppliers can be envisaged. This mix would allow for an isolation of Huawei equipment and hence reduce risks.[23] In addition to this, Huawei should be entirely excluded from providing critical parts that are needed to run the virtualisation layer of the 5G network.[24]

There are several challenges to this solution. Smaller countries' intelligence agencies for instance may not be able to ensure a proper vetting of Huawei gear. Reviewing equipment requires womanpower, resources, and advanced capabilities in cyber security. If one does not trust the supplier, continuously vetting a system becomes a sizeable investment. The question then becomes: does the security risk and the steady deployment of staff and resources to vetting make Huawei's equipment cheaper in the long-term? Are there hidden costs that have not been considered? European governments that decide to allow Chinese companies to compete for the construction of the 5G network should consider pooling their resources to mitigate these costs and institute a common European reviewing board.

If intergovernmental relations between Europe and China were to deteriorate the latter would be in the best position to exploit the former. The Chinese government will always be in a position of influence towards domestic companies. China could be demanding access to Huawei equipment or intercepting hardware before it is exported to Europe. Being one of the main suppliers of European mobile infrastructure will also give China the advantage of having intrinsic knowledge of the workings of the system, further easing potential for exploitation.

Moreover, 5G infrastructure is very complex. Consequently, it is hard to vet current systems to a sufficient level, some would say almost impossible.[25] Many countries are conducting supply chain attacks and they are difficult to detect due to the various possibilities of tampering with devices in the process of "design to manufacturing to storage to shipment."[26]

## Conclusion

No matter what European governments decide in the short-term, the dependency on China for core equipment that is used in critical internet infrastructure needs to be reduced in the long-term. For the moment vetting and corporate infrastructure reform should be taken into consideration to reduce risks. However, further restriction of equipment should not be taken off the table.

## Endnotes

1[1] Huawei Enterprise, 'Media Statement: Huawei Technologies Global HQ – Huawei Australia Hub', accessed 22 February 2019, https://huaweihub.com.au/media-statement-huawei-technologies-global-hq/.
2 Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board, 'Annual Report', July 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/727415/20180717_HCSEC_Oversight_Board_Report_2018_-_FINAL.pdf.
3 BBC, 'Huawei: Tackling Security Concerns May Take Five Years', *BBC*, 7 February 2019, https://www.bbc.com/news/business-47145685.
4 People's Republic of China, 'National Intelligence Law of the People's Republic of China', 27 June 2017, http://www.npc.gov.cn/npc/xinwen/2017-06/27/content_2024529.htm.
5 European Parliament, 'EU - China Trade Relations' (Directorate-General for External Policies, 2011), http://www.europarl.europa.eu/RegData/etudes/etudes/join/2011/433861/EXPO-INTA_ET(2011)433861_EN.pdf.
6 Huawei Enterprise, 'Re: Security of the UK's Communications Infrastructure', 29 January 2019, https://www.parliament.uk/documents/commons-committees/science-technology/Correspondence/190129-Correspondence-from-Huawei.pdf.
7 BBC, 'The US Cannot Crush Us, Says Huawei Boss', 18 February 2019, sec. Business, https://www.bbc.com/news/business-47274679.
8 Sebastian Heilmann, 'How the CCP Embraces and Co-Opts China's Private Sector |', Mercator Institute for China Studies, 21 November 2017, https://www.merics.org/en/blog/how-ccp-embraces-and-co-opts-chinas-private-sector.
9 Emily Feng, 'Chinese Tech Groups Display Closer Ties with Communist Party', Financial Times, 10 October 2017, https://www.ft.com/content/6bc839c0-ace6-11e7-aab9-abaa44b1e130.
10 Curtis Milhaupt and Wentong Zheng, 'Beyond Ownership: State Capitalism and the Chinese Firm', *UF Law Faculty Publications* 103, no. 665 (2015), https://scholarship.law.ufl.edu/facultypub/696.
11 Recorded Future, 'Recorded Future Research Concludes Chinese Ministry of State Security Behind APT3', Recorded Future, 17 May 2017, https://www.recordedfuture.com/chinese-mss-behind-apt3/.
12 Bill Gertz, 'Pentagon Links Chinese Cyber Security Firm to Beijing Spy Service', *Washington Free Beacon* (blog), 29 November 2016, https://freebeacon.com/national-security/pentagon-links-chinese-cyber-security-firm-beijing-spy-service/.
13 Recorded Future, 'Recorded Future Research Concludes Chinese Ministry of State Security Behind APT3'.
14 Director of National Intelligence Open Source Center, 'Huawei Annual Report Details Directors, Supervisory Board for First Time' (Reston, VA: Central Intelligence Agency, 5 October 2011), https://fas.org/irp/dni/osc/huawei.pdf.
15 Danielle Cave, 'The African Union Headquarters Hack and Australia's 5G Network', The Strategist, 12 July 2018, https://www.aspistrategist.org.au/the-african-union-headquarters-hack-and-australias-5g-network/.
16 Joan Tilouine and Ghalia Kadiri, 'A Addis-Abeba, le Siège de l'Union Africaine Espionné par Pékin', *Le Monde*, 26 January 2018, http://www.lemonde.fr/afrique/article/2018/01/26/a-addis-abeba-le-siege-de-l-union-africaine-espionne-par-les-chinois_5247521_3212.html.
17 IHS Markit, 'Global Mobile Infrastructure Market down 14 Percent from a Year Ago', 13 March 2018, https://technology.ihs.com/600864/global-mobile-infrastructure-market-down-14-percent-from-a-year-ago.
18 Danielle Cave and Tom Uren, 'Why Australia Banned Huawei from Its 5g Telecoms Network', *Financial Times*, 29 August 2018, https://www.ft.com/content/e90c3800-aad3-11e8-94bd-cba20d67390c.
19 Douglas Busvine, 'Exclusive: China's Huawei Opens up to German Scrutiny Ahead of 5G...', *Reuters*, 23 October 2018, https://uk.reuters.com/article/uk-germany-telecoms-huawei-exclusive-idUKKCN1MX1VE.
20 Niels Nagelhus Schia and Lars Gjesvik, 'China's Cyber Sovereignty' (Norwegian Institute of International Affairs, February 2017), https://brage.bibsys.no/xmlui/bitstream/handle/11250/2434904/NUPI_Policy_Brief_2_17_Schia_Gjesvik.pdf?sequence=4&isAllowed=y.
21 Reuters, 'Merkel Sets out Condition for Huawei's Participation in 5G Network', *Reuters*, 5 February 2019, https://uk.reuters.com/article/us-huwawei-europe-germany-merkel-idUKKCN1PU0GZ.
22 The Economist, 'How to Handle Huawei', *The Economist*, 31 January 2019, https://www.economist.com/leaders/2019/01/31/how-to-handle-huawei.
23 Ian Levy, 'Security, Complexity and Huawei; Protecting the UK's Telecoms Networks', National Cyber Security Centre, 20 February 2019, https://www.ncsc.gov.uk/blog-post/security-complexity-and-huawei-protecting-uks-telecoms-networks.
24 Levy.
25 Olav Lysne, *The Huawei and Snowden Questions: Can Electronic Equipment from Untrusted Vendors Be Verified? Can an Untrusted Vendor Build Trust into Electronic Equipment?*, Simula SpringerBriefs on Computing (Cham, Switzerland: Springer Open, 2018).
26 Micah Lee and Henrik Moltke, 'Everybody Does It: The Messy Truth About Infiltrating Computer Supply Chains', *The Intercept*, 24 January 2019, https://theintercept.com/2019/01/24/computer-supply-chain-attacks/.



Norwegian Institute of International Affairs

NUPI
Norwegian Institute of International Affairs
C.J. Hambros plass 2D
Postboks 7024 St. Olavs Plass,0130 OSLO
www.nupi.no | info@nupi.no

Established in 1959, the Norwegian Institute of International Affairs [NUPI] is a leading independent research institute on international politics and areas of relevance to Norwegian foreign policy. Formally under the Ministry of Education and Research, NUPI nevertheless operates as an independent, non-political instance in all its professional activities. Research undertaken at NUPI ranges from short-term applied research to more long-term basic research.

Valentin Weber is a DPhil Candidate in Cyber Security at the Centre for Doctoral Training in Cyber Security and a Research Affiliate with the Centre for Technology and Global Affairs, University of Oxford. He is also an Open Technology Fund Senior Fellow in Information Controls at the Berkman Klein Center for Internet & Society, Harvard University.