Science and Technology Committee
House of Commons London SW1A 0AA
Tel 020 7219 7126
http://www.parliament.uk/science

From Rt Hon Norman Lamb MP, Chair

Rt Hon Jeremy Wright MP
Secretary of State for Digital, Culture, Media and Sport
Department for Digital, Culture, Media and Sport
100 Parliament Street
London, SW1A 2BQ

10th July 2019

Dear Jeremy,

Telecoms Supply Chain Review

Thank you for your letter of 6 March regarding the security of the UK's communications infrastructure and the Government's 'Telecoms Supply Chain Review'. My Committee has since held a public evidence session and approached relevant stakeholders to explore the evidence on this topic further.[1]

Huawei's involvement in the UK telecommunications infrastructure

The National Cyber Security Centre has made clear that "there's no such thing as a 100% secure system" and that "in the end, cyber security is all about risk management".[2] **We have found no evidence from our work to suggest that the complete exclusion of Huawei from the UK's telecommunications networks would, from a technical point of view, constitute a proportionate response to the potential security threat posed by foreign suppliers.**

The mobile network operators, which are legally responsible for managing risks to their networks, expressed a similar view.[3] Regardless of the actual security risk posed by equipment from Huawei or any other vendor, telecommunications networks are designed such that they are secure even if their individual components are not.[4]

Supply chains for telecommunications networks have become global and complex. Many vendors use equipment that has been manufactured in China, so a ban on Huawei equipment would not remove potential Chinese influence from the supply chain.[5] Banning Huawei would also reduce market competition, giving network operators less leverage on equipment vendors to demand high security standards—although we note that Huawei, due to its assumed state subsidy, is not operating on a level playing field, which could in itself distort market competition.[6]

---

[1] Oral evidence taken before the Science and Technology Committee on 10 June 2019, HC 2200—references in this letter to oral evidence gathered in this session are referred to by the relevant question number

[2] 'Security, complexity and Huawei; protecting the UK's telecoms networks', National Cyber Security Centre, accessed 25 June 2019

[3] Q215

[4] Qq185–186

[5] Qq35–36, 43 and 172–173

[6] Q242

Although it is no guarantee of future security, the operators also noted that there has not yet been any evidence of an increased security risk from the use of Huawei equipment.[7] Huawei itself argued that it is a "closely watched company" and that "were Huawei ever to engage in malicious behaviour, it would not go unnoticed—and would certainly destroy [its] business".[8]

Nevertheless, we acknowledge that the security of the UK's telecommunications infrastructure is critical, and that all steps must be taken to ensure that the risks are as low as reasonably possible. In particular, the advent of 5G networks helps to enable the potential deployment of technologies such as driverless cars, smart cities and wearable health monitors.

Our witnesses made clear that these and any other essential services that will make use of 5G networks must be able to operate safely even if their connection to the network is disrupted.[9] This is not just to guard against any attack from a nation state or other third party, but also to protect against disruption caused by flooding, power cuts or other comparable events. **The Government must ensure that it has the measures in place to guarantee that all essential services that make use of communications networks are able to operate safely in the event of network disruption.**

Core vs non-core

Our witnesses also acknowledged that Huawei's particular circumstances mean that it presents a different risk profile to other vendors.[10] They indicated that they have mostly kept Huawei equipment out of the 'core' of their existing networks,[11] to reduce the impact that any potential threat could pose.[12] They also told us that they intended to continue this exclusion for their 5G networks. Although the Australian Government has concluded that the distinction between the 'core' and 'non-core' elements of 5G networks will be less clear than for previous technology generations,[13] we heard unanimously and clearly that a distinction between the 'core' and 'non-core' parts of a 5G network will still exist.[14] Dr Ian Levy, Technical Director of the National Cyber Security Centre, has explained that "from a purely technical point of view, geography matters in 5G":

> UK and Australia have very different geographies—so our laydowns will be very different to Australia's laydowns. So, we may have exactly the same technical understanding, but come to very different conclusions.[15]

The network operators' decision to exclude Huawei from the 'core' of their future 5G networks is, however, voluntary. **The Government should mandate the exclusion of Huawei from the core of UK telecommunications networks.** If such an exclusion were to be made mandatory, the Government must make clear the grounds on which

---

[7] Q210
[8] Letter from Ryan Ding to Rt Hon Norman Lamb MP, 29 January 2019
[9] Qq48, 186
[10] Qq192 and 210
[11] Qq216–224
[12] Q181
[13] 'Government Provides 5G Security Guidance To Australian Carriers', Australian Government, accessed 26 June 2019
[14] Qq15–19 and 229
[15] 'Huawei: Why UK is at odds with its cyber-allies', BBC News, 24 April 2019

Huawei were being excluded, to provide clear criteria that could be applied to another organisation in the future.

Huawei Cyber Security Evaluation Centre

We also heard the importance of the role played by the Huawei Cyber Security Evaluation Centre.[16] The most recent annual report of this Centre's Oversight Board reported that "significant technical issues have been identified in Huawei's engineering processes" and further that "no material progress has been made by Huawei in the remediation of the issues reported [previously]".[17] Professor Andrew Martin, of the University of Oxford, told us that the details of the report had "shocked" him.[18] BT Group and Vodafone UK indicated that they would be very concerned if Huawei did not act on the issues raised by the Oversight Board, and that they would seek to use commercial pressure to encourage Huawei to do so, if required.[19] John Suffolk, Global Cyber Security and Privacy Officer for Huawei, told us that the company accepted that it must "do better in many areas".[20] Ryan Ding, President of the Carrier Business Group at Huawei, informed us that, in response to the Oversight Board's annual report, Huawei would "initially invest US$2 billion over the next five years to comprehensively improve [its] software engineering capabilities".[21]

During the course of our inquiry, Ofcom informed us that although network operators were subject to legal duties to take appropriate measures to protect the security and availability of communications networks, its enforcement powers in this regard were "limited".[22] Firstly, although Ofcom issues guidance to operators on how they can meet their obligations, the current legislation "does not make provision for [Ofcom] to instruct providers on specific action that they must take in order to meet their [...] duties". Ofcom's powers also apply only to network operators, and do not extend to equipment vendors within the telecoms supply chain. Finally, the fines that Ofcom can levy are capped at £2m, which is lower than the limits that apply under similar EU regulations and other sector-specific UK regulation. Ofcom informed us that "were the Government to conclude [...] that more action was needed on security and resilience (for example, that certain specific requirements should be placed upon providers) then, depending on the details, this might require legislative changes including an extension to [Ofcom's] statutory powers".

It is clear that Huawei must improve the standard of its cybersecurity. While it is reassuring to hear that network operators share this point of view and are ready to use commercial pressure to encourage this, there is currently limited regulatory power to enforce this. **The Government should monitor Huawei's response to the issues raised by the Huawei Cyber Security Centre's Oversight Board and be prepared to act to restrict the use of Huawei equipment if progress is unsatisfactory. The Government should also consult Ofcom on strengthening its powers in order to help to improve cyber security in telecommunications networks, and support any changes that are deemed necessary.**

---

[16] Qq204 and 207

[17] Huawei Cyber Security Evaluation Centre Oversight Board, 'Annual Report 2019' (2019)

[18] Q52

[19] Q213

[20] Q105

[21] Letter from Ryan Ding to Rt Hon Norman Lamb MP, 29 January 2019

[22] Letter from Mansoor Hanif to Rt Hon Norman Lamb MP, 21 June 2019

It is worth noting that an assurance system comparable to the Huawei Cyber Security Evaluation Centre does not exist for other vendors. The shortcomings in Huawei's cyber security reported by the Centre cannot therefore be directly compared to the cyber security of other vendors. Representatives from Vodafone and O2 told us that they would support the establishment of similar arrangements for vendors other than Huawei, for example Nokia and Ericsson.[23] These vendors, unlike Huawei, are expected to be supplying equipment to be used in the 'core' of 5G networks. **The Government should consult the National Cyber Security Centre on the merit of establishing equivalent cyber security evaluation centres for 5G equipment vendors other than Huawei.**

Conclusion

Overall, my Committee concludes that—subject to: restrictions on access to highly sensitive elements of the relevant networks; continued close scrutiny; and satisfactory improvements in Huawei's cyber security in response to the Huawei Cyber Security Centre's Oversight Board—there are no technical grounds for excluding Huawei entirely from the UK's 5G or other telecommunications networks.

This conclusion is restricted to technical considerations. There may well be geopolitical or ethical grounds for the Government to decide to enact a ban on Huawei's equipment.

For example, consideration must be given to the UK's ongoing co-operation with its major allies. In addition, the Australian Strategic Policy Institute has reported allegations that Huawei supplied equipment and support to Xinjiang's Public Security Bureau, which has been accused of the most serious human rights abuses.[24] John Suffolk, Huawei's Global Cyber Security and Privacy Officer, clarified that Huawei's services were provided to Xinjiang's authorities through a third party,[25] but acknowledged that its products were used there. Huawei has since informed us that its Business Conduct Guidelines forbids its employees from engaging in "misuse" of information and communications technology to "conduct surveillance on end users' communications and/or movements".[26] It did not, however, specify what would constitute misuse. John Suffolk indicated that Huawei seeks only to "operate within the law" and "not create any moral judgements on what we think is right or wrong".[27] Unfortunately, this position could permit the appalling treatment of Muslims in Western China.

I hope the evidence we have gathered and summarised will be of use to your department as the Government completes its Telecoms Supply Chain Review. The potential benefits of 5G are clear and, as the Government has identified, the UK should aim to be a world-leader in the deployment and use of 5G networks.[28] The communications network operators estimate that a complete exclusion of Huawei equipment from existing or future networks could delay the rollout of 5G by two or three years.[29] The outcomes of the Government's Telecoms Supply Chain Review will therefore clearly influence the timing of the deployment of 5G in the UK, as does the

---

[23] Qq204 and 212

[24] Australian Strategic Policy Institute, 'Mapping China's technology giants' (2019)

[25] Qq63–65

[26] Letter from John Suffolk to Rt Hon Norman Lamb MP, 20 June 2019

[27] Qq62 and 102

[28] Department for Digital, Culture, Media and Sport, 'Future Telecoms Infrastructure Review' (2018)

[29] Qq235–237

delay in its publication.[30] **The Government must publish the outcome of its Telecoms Supply Chain Review by the end of August 2019.**

I would be grateful if you could respond to this letter and my Committee's conclusions and recommendations (indicated in bold text) by Tuesday 3 September.

Rt Hon Norman Lamb MP
Chair

[30] Q245