

Written evidence submitted by Prof J A McDermid, University of York***Huawei 5G***

- What are the risks to the UK's 5G infrastructure? How can these be mitigated?
 - All new technologies – risks and opportunities (better than 4G for end users)
 - Mitigation done at industry level – and Huawei worked with others including NCSC and advising OfCom, etc. – telecommunications security requirements and standards for the whole industry would be very reasonable (NCSC working with vendors and operators) and this may lead to new legislation
 - Risks – medium and high – Huawei in high risk, but have been working with NCSC over many years – giving assurance about the quality of the code, nothing there that shouldn't be there ... and they oversee it – and stress how competent NCSC are, and what they are doing (UK government has more information than anyone else outside China with access to equipment, software, etc.) MPs need to understand that this is coming from good experience etc.
- What is the role of government in 5G cyber security?
 - Ought to set standards and monitor – see the above ...
 - Also, a good opportunity to push the technology forward – NCSC is the first organisation who has worked with Huawei, looked at source code, etc. and other countries are following this (but Germany is also expanding this to other vendors; why doesn't the UK do this for other vendors as well?)
 - UK leading in Europe in terms of publishing 5G policy – so the industry is more ready ... great benefits to the economy especially in innovation and technology
 - There is importance of 5G technology in infrastructure resilience
- To what degree is it possible to exclude Huawei technology from the most sensitive parts of the UK's 5G network while allowing it to supply peripheral components?
 - Entirely possible – but there is misinformation that core and non-core parts are merged – however the standards provide for core and non-core to be separate, so it is a complete myth to say there is no separation – and Ian Levy the Technical Director in the NCSC has said he would refuse a licence to any operator who tried to do otherwise
 - Huawei involved in radio access part of the networks for many years – this will be in legislation, but doesn't really change anything
- What credible alternatives are available to Huawei systems?
 - Ericsson

- Nokia
- Whatever the UK does, it has to deal with overseas suppliers, and needs competition to get good prices
- And you want at least three suppliers (two is too little)
- NB need competition to get the R&D and innovation to get the technology to evolve
- Lowest volume, lowest power consumption, and often fastest – and giving cost savings to end users (OECD tracks this)
- NB quite a lot of the Ericsson and Nokia equipment is made in China!
- CISCO have had some involvement, but not a credible player – they do network switches but not the radio parts (only American company in there are Qualcomm in terms of patents)
- ZTE and Samsung are also possibilities, but no risk mitigation – GTE domestic, and Samsung is a new player, and thus high technology risk (NB many NA standards are different, so would need changes to use in the UK)
- Around 30% of Ericsson's spectrum cannot be used – and the Total Cost of Ownership (TCO) of the Huawei equipment is lower
- To what extent was the UK Government's decision on Huawei driven by political rather than technical factors?
 - So far as I can tell – technical – NB based on conversations with some of the UK's government CSAs
 - Nuances? Need an evidence-based policy, and that seems to have been exactly what has been done (supply chain review, risk matrix, etc. – a lot factual, with some expert judgement, and included a mitigation plan with NCSC support)
 - Intelligence and Security Committee made an assessment – however, intelligence data is not shared over public networks, but there may be some issues in terms of the US willingness to share information with the USA and in Five Eyes
 - NB intelligence community is completely relaxed, so far as I can ascertain – the community gets on and makes the best decisions for the Nation, despite what the politicians might say
- How will the UK Government's decision impact the UK's geopolitical position?
 - See above
- How will the UK's allies, particularly those in Five Eyes, respond to this decision?
 - USA and Australia are making negative decisions towards Huawei – New Zealand and Canada are still thinking ...
 - But global issues, and will carry on working between Nations ...
- How will this decision impact the UK's security and defence capabilities and the UK's interoperability with allies?

- Operationally – not at all, as we don't use this technology for defence
- In R&D – as above (nothing above Official Sensitive goes over public networks)
- And Huawei is not selling directly to the defence community – they only sell to the public service providers
- How important it is for the UK, separately or with allies, to maintain industrial capability in this field?
 - All we can do is be an intelligent customer – this is where we are now, and what we are doing
 - UK gets value with UK-based companies, e.g. ARM, etc. – and can export some elements to China, etc. and get some balance
 - UK couldn't do this "overnight"
 - There are some start-ups with niche products, and they should get some support, but there also needs to be clarity on standards to ensure interoperability

20 April 2020