Written evidence submitted by The Scotland 5G Centre

The Security of 5G

Summary:

- The use of high-risk vendors presents several key risks to our mobile infrastructure. We believe that the most important of these, which is **the ability for an adversary to turn off our networks**, is often missed, with much more focus on threats to confidentiality.
- 5G network vendor decisions are **influenced by 4G equipment vendors** – there is insufficient interoperability, meaning that UK Government was pressured by mobile operators to allow high-risk 5G vendor equipment, since they already used high-risk vendor 4G equipment.
- The lack of technical interoperability in **standards** meant that UK Government had effectively no choice. The Committee should liaise with DCMS and recommend it properly focuses its efforts on standards, and **ensuring the UK sufficiently funds standardisation initiatives** to take international leadership on key strategic areas of benefit.
- A short-term approach focused on cost minimisation appears to have driven the UK Government to accept the mobile operators' arguments that 5G would be held back without certain high-risk vendors. Despite this, the UK's long-delayed **Emergency Services Network** (by EE) now looks like it will have **Huawei equipment in its security-sensitive core until 2023**.
- The UK Government has stated its intention to cultivate a thriving and diverse ecosystem of alternative vendors, to drive a more competitive marketplace for radio equipment. However this laudable goal contrasts with policies that allow one vendor which has received **an estimated $75bn in "state aid"** [1]to dominate the UK market, and has benefited from state-bank loans[2] to fund purchases of their equipment?

[1] https://www.wsj.com/articles/state-support-helped-fuel-huaweis-global-rise-11577280736

[2] Huawei looks to state-backed vendor financing, 22 April 2009, https://www.ft.com/content/3f1fd67e-2f56-11de-a8f6-00144feabdc0

Government's Role in 5G Cyber Security

The role of Government in 5G security is central – industry and others look to Government for guidance, both in hard policy, as well as in general approach and outlook. Government is expected to provide leadership on this area.

Clearly in mobile networks, the commercial models of a competitive market have led to a wide range of levels of security available, as a result of decisions taken by mobile operators. At present, Government is being expected by industry to provide clarity as to permitted vendor choices, by virtue of designations of "high-risk" vendors, and then imposing restrictions on these high-risk vendors.

It would seem that while this is clearly important, it would be more beneficial for **Government to work with technical experts across a wider range of stakeholders, including those outside of Government and its advisors**, to form **high-quality technical guidance** that is broader, and more **principles-focused**, rather than based on specific concerns around certain vendors, as current guidance is. While both approaches are important, the industry needs clearer guidance on the principles expected, in order to result in the desired security posture being seen throughout the industry. These activities should be aligned with our worldwide allies, as the UK telecoms market alone is not large enough to be able to drive significant alternative provision, as Government is currently seeing with the limited choices available.

The extent to which it is possible to exclude Huawei from the most sensitive parts of the network, while allowing it to supply peripheral components

This question clearly requires a clear understanding of the meaning of "peripheral", in the context of a mobile network. The current Government/NCSC advice appears to suggest that anything outside the "core" of a mobile network would be viewed as peripheral. The shortcoming of this approach, however, is that the radio access network, and radios themselves, are both equally important to a network's security. Mobile networks are inherently used to inter-connect equipment, and this means connecting the radios, and corresponding access network, to the core.

With the move towards 5G networks, the **distinction between "core" and "edge"** will become problematic – for some of the most important potential applications of 5G (for safety, enhanced productivity, etc.) will be around **ultra-low latency communication**s – for example, connected vehicles. Both Scottish and UK Government are keen to see advances in **connected and autonomous vehicles**, but these require very low latencies for communications between vehicles. **These communications will therefore have to take place at the edge of the network** (i.e. out in the "peripheral" areas of the network) to avoid the increase in latency from sending all traffic back to a network core in another city.

Another area for the Committee to consider is around the likely need **for interoperability and interconnectivity between mobile networks**, in order to facilitate and enable connected vehicles, and other transport-based applications. For example, 5G Vehicle-to-Vehicle connectivity could be used to alert other vehicles to a breakdown in the carriageway ahead, or to coordinate a smart low-carbon goods convoy's movements, allowing goods vehicles to safely drive in the slipstream of the vehicle in front. These applications will require **connectivity between different mobile networks, again at the edge of networks**, in order to enable the low latencies required. This further erodes the distinction between the "most sensitive parts" of the network and its periphery.

Credible Alternatives to Huawei Systems

There are limited credible tier-1 vendors of mobile radio equipment, due to market consolidation and the high-volume, "lower-margin nature of the 5G infrastructure market"[3]. The main two alternatives are Nokia and Ericsson, with Samsung and ZTE having some market share in Asia.

It is important for the Committee however to note that **there are strong, credible, and viable alternatives to Tier-1 offerings**, and these should not be ignored by the UK. While mobile operators will always advocate for large-scale contracts with limited numbers of vendors (to improve economies of scales, and thus pricing), **this approach is what led us to the near-monopoly scenario of market failure** we see currently.

Mobile networks are inherently built around international standards, and there is a growing industry of "Tier-2" suppliers of compatible radio equipment, which is fully standards-compliant, and performs as well as, or better than, Tier-1 equipment. The University of Strathclyde, one of the founding partners of the Scotland 5G Centre, has demonstrated that it is **credible, possible, and feasible to build a mobile network using Tier-2 equipment**, with radios and other equipment **sourced exclusively from within Europe, on a lower cost basis** than Tier-1 vendors' offerings.

Mobile Network Operators are not keen to adopt these technologies, as **they are the victims of "vendor lock-in"**, with non-standardised and different orchestration and network management systems used by each Tier-1 vendor. Therefore, a mobile operator will find the lowest cost solution is to use equipment from their existing radio vendor, as it will integrate with their existing network management systems.

This challenge of interoperability is an **area of key opportunity** for the UK to innovate in, and work with its allies and partners to develop domestic solutions to this problem. Initiatives like Open RAN have been heralded as the solution, but are generally widely reported as not being ready yet. Our response here is simple and straightforward – this problem will not go away, and will come back again and again for Government, unless it acts to address the underlying problem. That underlying issue is around **technical standards, the interoperability of equipment, and a need for strong representation of Government and public interests at international standards committees**.

Consumers do not benefit from vendor lock-in at a network equipment level (but nor do they realise it exists). **Government in particular do not benefit from vendor lock-in at the equipment level either**, and are in a position to drive progress at addressing it, by **selecting suitable delegates to the standards bodies on behalf of the UK, who can prioritise and advance this work**.

[3] Cisco rules out approach for Nokia or Ericsson. 13 February 2020. https://www.ft.com/content/536d28c8-4e87-11ea-95a0-43d18ec715f5

Extent to which decision was driven by political rather than technical factors

The UK Government decision appears to have been driven heavily by economic factors, steered by the mobile operators concerned – mobile operators publicly[4] warned of increases to costs of deploying 5G were they not allowed to proceed as planned, with Huawei equipment.

This contrasts with the technical advice from the UK Government's security services, specifically the Huawei Cyber Security Evaluation Centre (HCSEC), whose oversight board reports to the National Security Adviser. The most recent reports from this board are available online for 2017[5], 2018[6] and 2019[7].

In 2018's report, the **National Cyber Security Centre (NCSC) advised** the HCSEC Oversight Board that "**it is less confident that NCSC and HCSEC can provide long term technical assurance** of sufficient scope and quality around Huawei in the UK". Reasons for this included "repeated discovery of **critical shortfalls … in the Huawei engineering practice**s and processes that will cause **long term increased risk in the UK**".

2019's report identified that "**HCSEC's work has continued to identify concerning issues in Huawei's approach to software development,** bringing significantly increased risk to UK operators" and that "Huawei **continues to use an old and soon-to-be out of mainstream support version** of a well-known and widely used real time operating system supplied by a third party", and that "NCSC believes **there is currently no credible plan to reduce the risk in the UK** of the use of this real time operating system", in light of the "**time elapsed since discovery** of this issue without a credible plan being presented".

Additionally, the 2019 report identified that a plan prepared by Huawei to "remediate the software engineering and cyber security issues in the LTE eNodeB product" (i.e. their 4G base stations), "was **unacceptable to NCSC and UK operators**", with "**NCSC currently not confident that Huawei is able to remediate the significant problems it faces**".

In light of these findings, it is unclear why Government and NCSC's latest advice has since only sought to exclude Huawei from certain core network functions[8], given the above issues reported by HCSEC related to their base station products, which are not be banned, and subject only to the more general restrictions on market share and similar.

Finally, the Committee should note that the Government's own approach around use of high-risk vendors' equipment "near certain sites that are significant to national security" appears to **acknowledge and accept a level of risk that is undesirable** and may "**cause an unmitigable security issue**", according to NCSC.

17 April 2020

---

[4] https://www.theguardian.com/technology/2020/jan/17/uk-officials-frustrated-us-huawei-plan-b

[5] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/626110/20170413_HCSEC_Oversight_Board_Report_2017_-_FINAL.pdf

[6] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/727415/20180717_HCSEC_Oversight_Board_Report_2018_-_FINAL.pdf

[7] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf

[8] https://www.ncsc.gov.uk/files/Advice-on-use-equipment-from-high-risk-vendors-in-UK-telecoms.pdf