Written evidence submitted by techUK

The Security of 5G

About techUK

techUK is a membership organisation that brings together people, companies and organisations to realise the positive outcomes of what digital technology can achieve. We collaborate across business, government and stakeholders to fulfil the potential of technology to deliver a stronger society and more sustainable future. By providing expertise and insight, we support our members, partners and stakeholders as they prepare the UK for what comes next in a constantly changing world.

techUK is working with our members, telecom operators, vendors and regulators on how to continue to improve the security and resilience of our digital infrastructure.

Executive Summary

5G is the next generation of mobile communications technology, it will offer faster mobile broadband connections and the ability to connect a greater number of devices online. The UK Government has said it wants to be a global leader in 5G and the rollout of 5G has already began in many areas. 5G will be a key part of the digital fabric that underpins the next industrial revolution.

5G is an evolution of networks that have come before although we will see more and more critical services make use of it. Therefore, the security and resilience of our telecommunication networks must remain the top priority. Indeed, security and resilience are the primary priorities for the UK's four main mobile network operators (MNOs). It is their reputation and financial position on the line if they suffer a network outage – for any reason.

The UK's MNOs all adopt a layered approach to cyber-security which is in line with best practice. This includes subjecting their suppliers to the highest levels of assurance, network design and ongoing monitoring. There are currently only 3 scale suppliers of 5G access equipment in the UK market; this is already sub-optimal and so new entrants should be encouraged.

The majority of the investment burden into our 5G networks will be made by the private sector; through our MNOs and potential new players as the technology continues to develop.

Given the importance of 5G networks, the Government published a Telecoms Supply Chain Review in 2019 and in January 2020 further guidance on, and definitions of High-Risk Vendors. Together these set out new Telecoms Security Requirements, an enhanced legislative framework for security in the sector and bespoke management of High-Risk Vendors. Part of this management of High-Risk Vendors excludes them from sensitive 'core' parts of 5G and gigabit-capable networks. It was also imposed a 35% cap on high risk vendor supplying peripheral components such as mobile phone masts and antennae.

techUK believes that the Government's current approach, based on a strong evidence base, strike the correct balance between ensuring the security of our telecommunication networks and providing certainty to our mobile network operators (MNOs) who are investing and building out these networks. These measures build on practices our operators already deploy – with their number one priority being to keep customers and the UK safe.

At the same time, we believe the Government must also examine other policy levers that can contribute to securing 5G networks and the applications and services that ride on those networks. A singular focus on the supply chain question and "High-Risk Vendors" risks ignoring other important considerations for securing 5G overall. We recommend the Government initiate future work in this area.

Response

1) What are the risks to the UK's 5G infrastructure? How can these be mitigated?

Why should there be more focus on resilience and security for 5G

Digital communications are becoming ever more important, with the deployment of 5G and full-fibre broadband underpinning the economic transformation of the UK over the next decade.

All networks pose risks to some degree. All vendors have potential vulnerabilities which is why operators deploy defence in depth approaches. High-Risk Vendors (HRVs) require additional and bespoke mitigation strategies. The challenge for operators and society as a whole is about how to manage these risks in order to take advantage of the benefits that they can deliver.

5G is designed to support multiple, specific use cases. Whilst it is an evolution of 20 years of telecommunications development and iterations its value adds over 4G are principally for the enterprise market, where 5G will enable optimisation of manufacturing, autonomous unloading at container ports, real time inventory, and much more. Indeed, as the UK recovers from the economic crisis caused by COVID-19, 5G will necessary more than ever to supercharge the economy[1].

Due to this increased utilisation, it is right that questions are asked about its resilience and security. This is because down-time for the network for whatever reason – from faults to the recent arson attacks due to theories linking 5G to COVID-19 – or due to increased cyber-attacks from hostile actors, will have greater consequences.

We believe the key questions to be:

- How should we ensure that telecoms operators standardise security practices throughout their supply chain?

[1] https://home.barclays/news/press-releases/2019/04/5g-technology-boost-to-uk-economy/

- How can we create sustainable diversity in the telecoms supply chain?
- How do we address the challenges posed by higher risk vendors?
- How can we validate that products and solutions from other vendors do not introduce risk through poor software quality?
- Do technologies exist that can provide a layer of security on telecom networks regardless of vendor?

Is 5G less secure than 4G?

Delivering on 5G will require networks to be extensively automated. Manual processes will be no match for high demands such as deploying automated cars during a busy period. The priority of 5G networks will, therefore, be the ability to define and control every aspect of the network in software, from the core to edge. This will obviously increase the surface for potential attacks.

However, 5G has been designed with security as a key priority on its control plane. This, along with the extensive virtualisation both in the core and Radio Access Network (RAN), 5G arguably offers increased resilience over previous iterations of comms technology. However, the security design of 5G does not take into account the potential increased risk presented due to the increased capacity and capabilities of a 5G network on the user plane. The increased risk to the network for a rogue or malicious device is a lot larger due to the capacity and capabilities of a 5G network.

Despite this work, cyber security is dynamic – hostile actors are also constantly working to find vulnerabilities to exploit. Cyber attacks on mobile networks' infrastructure and their users continue to grow. Criminals consistently introduce and update new attack tools, using automation, exploit toolkits, and cloud technology to attack mobile operators' network infrastructure, applications, and services, and the operators' customers/end-users (consumers and enterprises). This is a threat that we see across all digital networks today and is independent of the underlying vendor. Therefore, to continue to protect our 5G networks in an effective manner, a new ecosystem of vendors, researchers, cyber security assessors and operators need to emerge to drive the cyber security agenda for 5G.

How can we mitigate risks?

One of the risks to 5G networks in the UK is the existing reliance on a very small number of equipment vendors. It is encouraging that the Government has stated that it wants to diversify the market and increase competition but this will only be achieved if the Government and mobile network operators work with a wider range of low risk vendors and create an environment where there are practical measures, like better interoperability of equipment – this is explored further below.

The Government has sought to provide greater clarity to how we can mitigate supply-chain related risks through its Telecoms Supply Chain Review and follow-up report on High Risk Vendors. These proposals set out:

- New Telecoms Security Requirements (TSR). These will provide clarity and guidance to operators, and their supply chains, on what is expected and required of them in terms of network security.

- Establishes an enhanced legislative framework for security in telecoms. This will put the TSRs on a statutory footing and provide Ofcom with greater enforcement measures – including independent testing of networks.

- Manage the risk posed by high risk vendors. They are prohibited from the core of the network, with a 35% cap on their use in other areas. These measures build upon the already best in class approach that the UK has taken with regards to potentially high-risk vendors where network security.

techUK is not a technical cyber security body, but we and our members know that the UK benefits from having a world-leading independent authority in the National Cyber Security Centre (NCSC). The NCSC are at the heart of the Government's work on security and 5G, as well as providing their technical expertise in the Huawei Cyber Security Evaluation Centre (HCSEC) – another UK innovation which is a model that other countries have replicated.

A body such as NCSC are be well placed to undertake wider testing of equipment to identify issues of poor-quality software and vulnerabilities.

2) What is the role of government in 5G cyber security?

The Government has a crucial role, as it does elsewhere in cyber security and wider resilience of other Critical National Infrastructure. In the National Cyber Security Centre (NCSC), the UK has an internationally recognised centre of excellence which has a deep understanding of the UK's mobile networks.

We believe that Government's role is setting the legislation and regulatory framework for the telecoms sector, providing guidance to actors in this sector regarding the range of risks (supply chain and beyond) and suggested mitigation steps, and encouraging a wider diversification of suppliers to the telecoms sector. These three roles must all be undertaken with meaningful dialogue with the sector.

As addressed above, we believe that Government has launched supply-chain related work in an appropriate and proportionate way although we do have some suggestions for improvement in this regard.

The upcoming Telecommunications Security Bill is an appropriate vehicle to embed the Telecoms Security Requirements – currently being

developed in detail with industry input and the wider measures outlined in the Government's evidence-based Telecoms Supply Chain Review. We understand that both the NCSC and the BSI will have a role in developing the TSRs and that activity now is taking place in the NCSC. Once the TSRs are finalized, the upcoming Telecommunications Security Bill is an appropriate vehicle to embed them into the existing legislative framework.

The UK's security services, along with the cyber security functions of our telco operators, have been operating with bespoke mitigation strategy for High-Risk Vendors for over a decade. No two countries have exactly the same telecoms networks, shaped as they are by legacy decisions, geography and population.

We welcome the January 2020 guidance that the NCSC has set out with regard to 5G and gigabit capable networks. This provides the sector with a greater understanding of the threat-matrix, the mitigating actions that are necessary and greater clarity on potential future developments. However, we note that the guidance does not address threats to the user/data plane and mitigation steps, and we suggest the NCSC round out its analysis in this regard.

techUK also believe that Government has a role to encourage additional vendors to enter the market for operators to choose from, so that there is a diverse range of vendors, for example, those that can help operators embrace open interfaces.

Diversification of suppliers into the telecoms market is, to some degree, the heart of the current problem with regards to resilience and security. In particular, the trends for a single Radio Access Network (RAN) and the transfer of operational capabilities to network vendors have made network operators more reliant on a limited number of vendors, making it costly to change direction or, at the very least, disincentivising change. This is different in other parts of the world that are successfully deploying 5G without a reliance on previous network generations, although as noted below there are reasons for different approaches to network deployment.

The Government should act to address this lack of vendor competition and to encourage and facilitate new entrants, leading to greater diversity and reduced reliance on high-risk vendors. Network equipment vendors should be more involved in the discussions with the Government to make sure that they contribute to and follow recommendations, have the right expertise and provide secure products. We discuss in more detail how this can be achieved below.

The NCSC's Technical Director, Ian Levy, commenting on the Government's proposals in its Telecoms Supply Chain Review and for higher risk vendors, stated that "We believe the totality of the measures announced today will ensure the UK's telecoms networks are appropriately secure into the future regardless of the vendors used"[2].

[2] https://www.ncsc.gov.uk/blog-post/the-future-of-telecoms-in-the-uk

techUK believes that the proposals strike the correct balance between ensuring the supply-chain related security of our telecommunication networks and providing certainty to our mobile network operators (MNOs) who are investing and building out these networks. We appreciate Dr Levy's stated desire to secure the UK's telecoms networks regardless of vendors. To expand on this, we suggest the Government separately examine in the future what new, leading-edge technologies exist or are under development to contribute to this goal.

3) 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?

N/A

4) What credible alternatives are available to Huawei systems?

Both mobile and fixed-line networks are broadly made up of the access network and the core. Across both networks there are varying degrees of competition in each part of the network.

The Government's proposals for High-Risk Vendors, such as Huawei, is to prohibit them from the core and put in place a 35% cap for the access networks.

In the UK mobile market, the scale providers of cellular base station equipment are Ericsson, Huawei and Nokia. Additionally, Samsung also supply 5G network equipment in other countries. As noted above, this is already considered to be sub-optimal by the operator community as a resilience issue in one vendor is likely to have a large impact.

Some countries are moving away from their incumbent providers with new suppliers emerging as they are build-out their 5G networks. When considering this it is important to understand the UK market.

The UK is deploying what is known as Non-Standalone (NSA) 5G New Radio. This means that 5G antennae make use of existing base stations that already have 2G/3G/4G on them. This approach has the benefit of an accelerated rollout and lower cost to end-users compared to other markets such as the USA which has pursued a Standalone approach[3]. NSA does however limit new entrants coming into the market and using equipment in the UK, therefore other alternatives should be considered.

There are also compatibility challenges when deploying 5G antennae that are different from a different vendor to the 4G equipment being used for Non-Standalone deployments. If the Government was to overly restrict a vendor's market share of 5G this would mean the operators would need to spend capital and time replacing their 4G equipment rather than driving 5G coverage out.

[3] https://home.kpmg/uk/en/home/insights/2019/07/the-5g-launch-conundrum-how-to-cost-it.html

There are high barriers to entry in the telecoms market beyond these issues. There are steps that Government can and should take however which will help use reduce these barriers:

- OpenRAN: This technology standardises the design and functionality of RAN hardware and software. OpenRAN allows operators to buy equipment from different vendors as certain elements of telecom networks are separated out. This then opens the door for smaller vendors. Industry is actively exploring this type of technology, but the Government can spur this market by prioritising OpenRAN and similar initiatives in Government funded testbeds (such as its 5G Testbeds Programme) or subsidised rollouts.

  Implementing OpenRAN would introduce potential suppliers of base station equipment such as Dense Air, Parallel Wireless, Altiostar, Gigatera Supermicro, Xilinx etc. The current implementation of 5G wireless networks, in contrast, are still built using proprietary systems developed by individual vendors. If telecommunications networks used open standards equipment, high-risk vendors would not have such a dominance on wireless infrastructure.

- Adopt practices that make 5G open like most of the rest of the digital world. Such a capability has been under development for several years by a group called the O-RAN Alliance[4] (replacing traditional network vendors' proprietary technology with software-driven technology that will run on any off-the-shelf hardware). Nokia and Ericsson have already joined the effort to create an open and interoperable RAN.

- Wider diversification measures including target R&D support, the creation of a test lab between the NCSC and Government to de-risk new entrants and attracting globally significant players who are not yet present in the UK market.

A complimentary action to focusing on such diversification measures, is to promote scalable security controls and tools that can overlay a telecom ecosystem and serve to secure all traffic traversing the network infrastructure, services, and applications. It is important to keep in mind that today's telecom networks are decentralized and consist of multiple physical, virtual (software-defined), and cloud-delivered technologies that are supplied by dozens of vendors from all over the world. More work needs to be done to explore this area, bringing together cyber security researchers and industry.

In addition, because all telecom network elements in the core and edge, whether hardware, software, or cloud, must communicate to perform the various functions and provide the services the telecom operator seeks to

[4] https://www.o-ran.org/

provide, security of the communications traffic is imperative (in addition to the security of each underlying technology element). Telecom operators need to have constant real-time visibility across traffic passing through their networks and be able to detect and stop in real time cybersecurity threats within that traffic. Technology exists today to enable operators to do this - monitor and control traffic interactions between and among diverse and virtualized network elements.

5) To what extent was the UK Government's decision on Huawei driven by political rather than technical factors?

N/A

6) How will the UK Government's decision impact the UK's geopolitical position?

N/A

7) How will the UK's allies, particularly those in Five Eyes, respond to this decision?

N/A

8) How will this decision impact the UK's security and defence capabilities and the UK's interoperability with allies?

N/A

9) How important it is for the UK, separately or with allies, to maintain industrial capability in this field?

The UK, like the other Five Eyes countries, does not manufacture base station equipment or devices. Samsung, Ericsson and Nokia are independently contributing to the 5G rollout (with some multi-industry companies particularly focused on rollout across the US, Korea and Japan and beginning rollout in Canada and New Zealand) – although as noted above some of these countries are pursuing different 5G network rollouts to the UK.

The UK does have world-leading capabilities in designing crucial *chip* architectures (including those licensed to Huawei, Samsung and Qualcomm), as well as in AI and developing applications.

The UK has a number of highly respected companies with deep cyber security expertise which can and should be used to maintain and develop independent 5G capability for the UK, working alongside specialists like NCSC.

17 April 2020