Written evidence submitted by BT Group

SECURITY OF 5G

Overview

1. The security and resilience of the UK's digital infrastructure is of paramount importance – something thrown into even sharper relief at present as the country responds to the Covid-19 outbreak and reliance on fixed and mobile telecommunications increases to support mass working and schooling from home. BT's networks continue to manage this increase in demand and a reshaping of internet traffic well, keeping our customers connected at this vital time.

2. As our 5G deployment continues, with EE coverage now across seventy towns and cities, the security and resilience of the network will remain our top priority. The technology, which has been developed with security right at its heart, also provides in-built improvements over and above those available in older generations. 5G is also increasingly important to deliver the capacity required in the network as demand for mobile connectivity continues to grow.

3. 5G leadership offers significant economic advantages[1] and the continued success of the UK's digital economy requires a balanced, risk-based policy approach, that ensures access to the best global innovation and greater vendor competition, whilst keeping critical national infrastructure secure. The conclusions of the Government's Telecoms Supply Chain Review, published in summer 2019 and in January 2020, were proportionate and evidence-based – and so broadly achieved this goal. In particular:
   - New Telecoms Security Requirements (TSRs) will be important in further strengthening the UK's approach to cyber security, setting a higher bar for all operators in their network design, management and use of vendors.
   - The distinction the Review makes in its approach to the 5G core network and the 5G access network is valid. We see no change in risk with the introduction of 5G relative to earlier generations due to the ongoing protections around the core network (which will expand as 'edge computing' is introduced), with High Risk Vendors (HRVs) only present in the 'dumb' functions of the access network.
   - Whilst over the medium term, we expect an ongoing reliance on major global vendors, the Government's approach will allow time for exploring new approaches to supply chain diversification, including progressing initiatives that may allow smaller companies and new technology to play a greater role.

4. The three-year transition to a maximum of 35% of a HRV's equipment in the 5G access network is challenging, however, and will not come without significant disruption and cost – up to £500m for BT alone.

5. We want to work with the Government, the security services and Parliament to develop the detail of the approach set out by the Review to ensure the transition to new HRV requirements is manageable, the industry can progress with certainty and we can continue to make significant investment in upgrading the UK's digital infrastructure.

The availability and integrity of our networks and the confidentiality of the data we process is at the heart of our ability to serve our customers – cyber security is a top priority for BT

[1] See, for example, DCMS (2018) Future Telecoms Infrastructure Review.

6. We have adopted robust and long-standing infrastructure security policies based on best practice and work closely with the security services. We have:
   - Invested significantly in developing world-leading capabilities to combat cyber threats.
   - Developed a long-standing partnership with the National Cyber Security Centre (NCSC) focused on improving the resilience of the UK's telecommunications infrastructure. The UK, via the Huawei Cyber Security Evaluation Centre, leads the world in its ability to understand, analyse and assure the quality and integrity of its hardware and software.
   - Established clear and consistent network architecture policies to minimise vendor risk, not permitting HRVs in the sensitive core network.
   - Strong governance arrangements in place, with BT's Security Council providing Executive-level oversight of all cyber security issues, including the use of all external suppliers in the network.

7. We own and operate critical national infrastructure and so we see it as vital to work in lockstep with NCSC on our vendor deployment, sharing full visibility of major procurement decisions. We have established a comprehensive risk mitigation programme, in-line with their guidance and strategy.

8. The Supply Chain Review, as part of its initial conclusions published in summer 2019, proposed new TSRs, which will be underpinned by a robust legislative framework "necessary to safeguard the UK's national security interests". These will undoubtedly provide a higher floor for all operators to meet and we expect that they will represent a significant strengthening in how network security and resilience is regulated. We are working with DCMS and NCSC on their detailed specification. For the TSRs to have the greatest effective, it will be important that all network and service operators follow them.

<u>5G provides for enhanced security features beyond those available in earlier generations</u>

9. With its potential to revolutionise digital communications, there has been significant focus on 5G network resilience and reliability. Security has been, and continues to be, at the heart of 5G development, with an improved set of security features deeply embedded in network design, beyond those available in earlier generations.

10. These include:
    - Improvements to subscriber authentication and privacy.
    - The utilisation of cloud native technology, enabling more rapid patching and upgrading.
    - Network slicing, allowing networks and services to be isolated and logically grouped per customer per deployment.
    - Stronger encryption and integrity protection algorithms to prevent eavesdropping and modification of data.
    - A radio access network that is a full revamp from previous generations, ensuring security from within in its functionality and deployment.
    - Authentication of all elements of data transmission across 5G networks, with authentication protocols being built in from the outset of 5G development, rather than a bolted-on – this mitigates risks of a rogue component conducting reconnaissance or replay attacks.

11. Industry forums and international standard-setting bodies[2] continue to define and refine the technical specifications for 5G security, drawing on global collaboration of chipset manufacturers, network equipment vendors, subscriber equipment manufacturers, operators and the suppliers of new technologies such as virtualisation. Every supplier in the 5G ecosystem will be

[2] Including 3GPP, ETSI, IETF, NGNM, CNCF and GSMA

independently audited against these standards and scrutinised during procurement and in-life operations. These provide a baseline line of defence which is then enhanced by operator-specific policies, standards, procedures, periodic auditing, penetration testing and vulnerability scanning.

The Government has taken a proportionate and evidence-based approach to High Risk Vendors in 5G

12. In January 2020, the Government announced its conclusions on the use of HRVs in the UK's 5G and full fibre networks. NCSC guidance published alongside was clear that, within three years, all HRVs, including Huawei, should not be present in the sensitive core networks and only compose 35% of the access networks.[3]

13. We believe that this was a proportionate decision, one based on clear analysis of evidence following the year-long Telecoms Supply Chain Review, broadly in line with BT's existing network architecture policies and with a recognition of the UK's strong foundation on cyber security (to be enhanced further through new TSRs). In particular, the distinction it makes between the 5G core and access networks is appropriate. The Government's approach will also allow time for exploring new approaches to supply chain diversification, including progressing initiatives that may allow smaller companies and new technology to play a greater role.

14. However, the three-year transition to a maximum of 35% is challenging – due in most part to the lack of vendor interoperability across 4G and 5G technologies – and will represent a significant shift over a relatively short period of time. We estimate the cost to BT to be circa £500m.

15. We want to work closely with the Government, the security services and Parliament to ensure that the forthcoming legislation, through the Telecoms Security Bill, continues to represent a proportionate and evidence-based approach to managing the risks of HRVs, enhances the UK's cyber security and provides the opportunity to leverage the economic benefits of 5G as far and as fast as possible.

The core-access distinction remains valid for 5G

16. We are conscious of the potential risks regarding the use of less traditional suppliers and designated HRVs. Where we leverage such equipment (from, for example, Huawei) in our networks and service, we apply constraints to manage risks, including network architecture principles and our procurement strategy, and we work closely with the NCSC. In combination, this provides for effective risk management across all vendors we use in our network.

17. BT has a long-standing and robust network design approach that exclude HRVs from the sensitive core network. The core network handles customer-sensitive data and connects users to each other and other networks. The access network has no decision-making capabilities and just provides access to the core network. Since introducing Huawei into our fixed network in 2006, we have consistently followed a deliberate policy of not using Huawei equipment in the core. This means that the impact of any issue with a single item of Huawei equipment or software is minimised – they have no remote access or meaningful ability to present risk to the core network or access to subscriber data. We have the source codes from Huawei (as we have access to those of all our network suppliers) and check all Huawei code via the Huawei Cyber Security Evaluation Centre.

[3] For 5G, this is defined as both a maximum of 35% of an operator's base stations where HRV equipment can be deployed and a maximum of 35% of network traffic to travel over HRV equipment.

18. In 2016, following the acquisition of EE, we began a process to remove Huawei equipment from the core of our 3G and 4G mobile networks, as part of adhering to our long-standing network architecture principles. We are applying these same principles to our 5G core infrastructure.

19. It is true to say, when 5G reaches a level of maturity, that the core-access configuration will be different than that for 3G and 4G networks. In future 5G architecture, in order to deliver the benefits of, for example, low latency, mission-critical connectivity, some of the core functions will likely move further out, physically, in the network. This is so-called 'edge computing'. However, so too will the security principles we will apply to them in order to maintain a very clear operational and security distinction between the core and access parts of the network.

20. Edge computing will only be deployed where we are confident it will be secure, remaining behind the key security perimeters and firewalls that we have in place today. We therefore see no change in the risk profile for 5G relative to 4G. Indeed, as the core functions become physically more distributed across the network through edge computing, it does mean that any single core network issue can be more easily defined and contained, reducing the wider impact on the infrastructure as a whole. This is in addition to the enhanced security features of 5G, as highlighted above.

The three-year transition to a maximum of 35% is challenging and will not come without significant cost and disruption

21. We are developing our plans to meet this requirement, albeit we are currently assessing the likely impact of the Covid-19 outbreak on this and other parts of the business.

22. We estimate that the cost to BT alone in meeting these new restrictions will be circa £500m over a five-year period, with the bulk of the cost being driven through our mobile rather than our fixed access network (run and managed by Openreach).

23. These costs are created by a number of factors. First and most substantially is the expense of swapping out existing Huawei equipment for those of another vendor. BT's 5G deployment is, in this first phase, focused on upgrading our existing 4G cell sites. Due to the current lack of vendor interoperability (which we expect to persist in the medium term), we have to use the same vendor for 5G as the underlying 4G technology – so in the vast majority of cases, we will also have to replace our existing 4G equipment. Second, is the expected increase in unit prices of 5G equipment from other global vendors as they respond to increased demand. And third is the likely cost impact of negotiating access to sites with landlords who will be in a strong position to demand increased payments as our hard deadline for completing the transition is known publicly.

24. Looking to meet this 35% limit more quickly or significantly reducing this limit to be met within a similar timeframe would have significant economic impact. Most immediately it would have material consequences for the pace and scale of 5G deployment across the UK and drive significantly greater swap-out costs than we currently estimate. We would also be concerned that a shorter timescale could create network disruption and lack of coverage as sites need to be taken off air.

25. This comes at a time when BT – and other operators – are in the middle of major programmes to future-proof the UK's digital infrastructure, involving unprecedented levels of change, investment and upgrading. We are seeking to support the Government's ambitions for nationwide gigabit-capable connectivity by 2025 through the scale roll-out of full fibre, world leadership in 5G and improved rural mobile coverage through the £1bn Shared Rural Network initiative. Driving

increased cost and uncertainty through an accelerated Huawei removal programme will put these other priorities at risk through reducing available capital.

The Government's approach will allow time for exploring new approaches to supply chain diversification – albeit reliance on major global vendors will remain over the medium term

26. Currently, UK telecoms operators are heavily reliant on a small number of global organisations for their mobile radio access network – Huawei, Ericsson and Nokia. The ability to modulate radio waves efficiently to enable scale radio access network (RAN) deployment is challenging – and only three players in the world do that well given the investment and experience needed to build this capability.

27. We source network equipment from multiple suppliers and we will continue to do that as we deploy 5G – our investment is not and will not be monopolised by any one supplier. Huawei has invested significantly in 5G radio access technology and, as such, has taken a leadership position – but we fully anticipate other suppliers to accelerate their development timescales to meet this competitive challenge.

28. A more diverse and competitive supply chain would, however, be beneficial – both economically and in terms of quickening technological advances. New approaches, such as Open RAN, offer the potential for this, although it is as yet unclear whether these will be successful.

29. The backbone of the telecoms industry is open standards, enabling interworking and global economies of scale. An industry response to consolidation in the equipment supply chain has been a drive for the development for open architectures which incorporate telecommunication standards. The objective of Open RAN is to enable a vibrant RAN supply chain. An industry architecture is being specified through live industry groups with standardised functions and interfaces which will enable multiple vendors to produce components which can be integrated into a complete RAN solution.

30. We want to accelerate the progress of these initiatives and BT is heavily involved in the industry forum. However, in the short to medium term, we will rely predominantly on scale global vendors. We need strategic relationships with vendors and cannot allow multiple, smaller scale players into our network without full confidence that they can support the resilience and security of our networks. This will take time.

31. Greater Government action in this space would be valuable in accelerating progress. We believe it should focus on supporting operators in the following ways:
    - Targeting public funding on a number of Open RAN projects based in the UK with industry providing opportunities for commercial deployments e.g. via rural coverage programmes or dense urban small cell roll-out.
    - Encouraging major vendors who do not have a significant presence in the UK, such as Samsung, to invest in UK-focused product development that meets UK operators' specific requirements.
    - Greater funding support, potentially through the DCMS 5G Testbeds and Trials programme, to develop a new Future Network Research Initiative (FNRI) to complement the proposed National Telecoms Lab (which will focus on the testing of security of new equipment for the UK market). The FNRI would provide the infrastructure to enable universities and companies to trial new approaches to network deployment and operation, collaborate to build to prove end-to-end solutions, test hardware and software in a scaled environment. This would help

in overcoming the hurdles smaller vendors face in proving their products in the UK telecoms environment.

BT Group
17 April 2020