Written evidence submitted by Huawei Technologies (SFG0010)

Overview

The approach taken in the UK will make its 5G networks the most secure in the world; it now needs to focus on delivering the potential economic benefits from 5G networks.

Huawei firmly believes that the rapid and deep rollout of 5G infrastructure is key to delivering the UK's future economic ambitions, leading to improved productivity and driving future growth in industrial sectors. During the Covid-19 lockdown we have also seen how digital communications can keep business running and people connected, even in the most difficult circumstances. Huawei has worked closely with the operators to ensure the continuity and resilience of the UK's networks at this difficult time.

Looking to the future, the UK should set itself high ambitions for 5G as a key pillar of the next generation of digital infrastructure, alongside the government's stretching targets for full fibre.

The reason 5G is so important to the UK is that it provides unique capabilities, including faster mobile broadband connections, the ability to connect a greater number of devices online and support for a new range of industrial applications. A stretching rollout target would help support the UK's development of the Internet of Things, and make sure the UK is well placed to benefit from the Fourth Industrial Revolution. The rapid, deep rollout of 5G networks across the whole of the country would also help support the government's aim of 'levelling up' across the UK by opening new possibilities for businesses in every sector.

Huawei is proud to have played a critical role in the deployment of the UK's existing 4G infrastructure, and we want to be at the forefront of the next generation of communications technology. The recent Government decision to allow Huawei to continue to supply equipment to the UK's network operators has provided some certainty for the communications industry and clarity for Huawei's business in the UK. Within the regulatory framework set out by the Government, and against the backdrop of a competitive three-supplier market, Huawei will now work with operators to help drive the rollout of high quality telecoms infrastructure across the country.

Security of networks is of paramount importance. The threat landscape is continuously evolving: the whole of the industry needs to meet new challenges and ensure that both individual users and the national interest are protected. New 5G networks are no exception. The UK has long had deep capabilities in cybersecurity – but the legislation being proposed by the government will make the UK the most strongly regulated communications market in the world. It is inherently impossible to make any real world network completely risk free, but as a result of the approach proposed by the government UK users will enjoy the most guarded 5G networks.

Within the policy framework set out by the government, some additional protections will be applied to the use of equipment provided by suppliers designated as high risk vendors. Huawei is one such company, and will face very significant additional restrictions on its ability to supply the 5G market:

- No use of HRV equipment in sensitive networks or at sensitive sites – 5G that uses Huawei equipment will not be used for intelligence sharing or other critical state activities for example

- No use of HRV equipment in 'core' networks – all authoritative technical advice states that a distinction between core and non-core will apply to 5G networks

- Use of HRV equipment in non-core networks limited to 35% – given this limit is for each operator, Huawei's national market share is likely to be below 35%

- Full transparency of Huawei equipment used in the UK – scrutiny that at present is applied to no other supplier

Experts at the National Cyber Security Centre (NCSC) have been clear on public record that this package of measures satisfies them that potential risks have been properly mitigated. There are voices that have called for more draconian measures – a total ban on all use of Huawei in 5G networks. We have not seen any evidence that suggests a need to go further than the measures being put in place (which we are already abiding by). Indeed, eliminating Huawei from the UK market might make the UK's networks less secure by reducing the number of suppliers to just two, increasing risks around dependency in the future. Strengthening diversity of suppliers by sustaining a three player market (with one heavily regulated player) or increasing to a four player market is the right approach.

We should also be clear that where the UK government does believe that risks are unmanageable it has acted decisively – potential supplier ZTE has been banned outright from supplying the UK market.

Competition has been a vital part of the UK supplier ecosystem for many years, and Huawei has played an important role since it began as a challenger in the UK over a decade ago. Our growth has been based on technologically advanced solutions and excellent customer service. Contrary to some claims, Huawei does not gain an unfair market advantage through the receipt of state aid or other special funds from the Chinese government. Our annual reports, audited by KPMG, clearly show that Huawei is a private company wholly owned by its employees. The Chinese government does not hold a single share in the company. An independent report by a professor of finance at Columbia University Graduate School of Business concluded that any financial benefits Huawei does receive, such as R&D incentives, are in line with the benefits that global competitors such as Nokia, Ericsson and Cisco receive, and are standard for high tech corporations around the world.

The boom of the global telecoms market across the world has provided firms like Huawei with extraordinary growth opportunities. The reason why Huawei's technology is best in class is because our business model is based on high investment and technical expertise – built through decades of market-leading R&D. We invested over $15 billion in R&D globally last year alone to ensure we can continue to offer the most attractive 5G and fibre network solutions and develop the leading technologies of the future.

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

New technology brings with it remarkable new opportunities. However, it also creates new threats to the safety and security of consumers. It is right that as these threats evolve, the UK's security framework is tested and adapted so that it continues to be fit for purpose. Huawei fully supported the Government's comprehensive security assessment, the Telecoms Supply Chain Review. This Review identified the key security risks to telecoms supply arrangements in the UK. It did this in a forensic, evidence-based way, taking proper time to consider all of the arguments.

It made several conclusions of how best to ensure the security of the telecoms network in the future, including the development of a new, robust security framework for telecoms, supported by the NCSC's existing risk-mitigation model. This framework will be based upon new Telecoms Security Requirements (TSRs) that will provide welcome clarity to industry on what is expected in terms of network security. Huawei welcomes this approach, given security is best considered at a whole network level. Vendors can and must support operators, and a concerted effort is required across the industry to raise security standards.

Alongside this, Huawei understands the desire for some specific restrictions to be placed on the use of equipment provided by high risk vendors to ensure that networks are secure and resilient. However, these restrictions should be evidence based and proportionate to the threat. The criteria for designating high risk vendors should also be transparent and evidence based, and subject to periodic review. It should not be based solely on country of origin.

The proposed additional controls on the use of Huawei's equipment will ensure that it is not found in any sensitive networks nor any sensitive core parts of networks. Much has been made of the claim that 5G will result in a blurring of sensitive and non-sensitive parts of the network. Whilst it is true that core networks will be bigger and closer to the end user for 5G, there will still be a clear distinction between a user accessing the network through a mobile mast or small cell, and the centralised management of the network for different regions of the country. This is a matter of science, not opinion.

The Huawei Cyber Security Centre (HCSEC) provides specific mitigation of risks arising from Huawei's involvement in the UK. HCSEC offers unprecedented levels of scrutiny and oversight on Huawei relative to other vendors. Huawei firmly believes that the security of networks will not be high until all vendors are subject to a proper base level of scrutiny, similar to that placed upon Huawei. This could potentially be exercised through the National Telecommunications Laboratory recently proposed by the Government, so that the performance of all network equipment can be properly assessed.

The Government also rightly identified that maintaining diversity of supply helps make networks more secure. A diverse supply chain promotes innovation and helps to reduce over-dependence that could in turn lead to network weaknesses. There are currently a limited number of vendors capable of providing 5G equipment, and Huawei welcomes the Government's ambition to ensure there is a sustainable and diverse supply chain through pursuing a diversification strategy.

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

The Government is responsible for ensuring that cyber security standards are maintained at a level that can best protect the UK's national security. Operators of networks are responsible for assessing risk and taking appropriate measures to ensure the security and resilience of their networks on a day to day basis. Suppliers should support this activity.

The new TSR, developed by Government in conjunction with NCSC, will form the bedrock of requirements in the sector, and demonstrate a shift away from informal government guidance, towards substantial formal rules and regulations that businesses will have to comply with. Huawei believes that this is the right approach, compelling operators, to take appropriate measures to safeguard the general security and resilience of the UK's networks and to flow down the relevant measures to the vendors that support them.

The UK has always been a global leader on cyber security standards. Once in place, the new TSR will be the toughest regulations of any cyber security regime. It is right that the government has sought expert advice from cyber security officials in NCSC before making decisions that affect these standards, given this is a complex technical issue.

This new regime will involve many tough new requirements. These measures, taken together, will allow the UK to mitigate the potential risk posed by the supply chain and to combat the range of threats, whether cyber criminals or state sponsored attacks.

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?

Operators run networks, not Huawei, and it is operators that determine exactly where a vendor's equipment is placed. The Government's recent decision to place restrictions on the use of equipment provided by high risk vendors excludes the use of Huawei equipment from security critical core functions in sensitive parts of the 5G network. Contrary to claims, this distinction between the periphery of the network, the so-call access network, and the core can be maintained for 5G. Ian Levy, Technical Director of NCSC, has made clear that despite the fact that sensitive functions are more dispersed in 5G networks, it is still possible to group and separate them accurately[1].

Huawei equipment is not currently present in core networks in the UK, with the exception of EE's 4G network where it is in the process of being removed. The Government's recent decision to make this position law for 5G networks has provided much needed certainty for the communications industry and clarity for Huawei's business in the UK. Huawei is now working

[1] https://www.ncsc.gov.uk/blog-post/blog-post-security-complexity-and-huawei-protecting-uks-telecoms-networks

closely with its customers, the government and the NCSC to enable them to ensure continued full compliance with the requirements of this decision.

What credible alternatives are available to Huawei systems?

There are three main 5G vendors in the UK: Nokia, Ericsson and Huawei. The Government's Telecoms Supply Chain Review concluded that the UK telecoms equipment market currently displays sufficient diversity – but that ideally this diversity would be further strengthened in the future. We would support any measures that support strengthened competition and the diversity this brings, and believe that it is competition that has helped the development of a thriving telecoms sector in the UK.

Huawei is a global business, as are our competitors, both in their ownership and the nature of their product development and production. Huawei is a Chinese company, but it has globally integrated supply chains and R&D partnerships all over the world. Nokia and Ericsson also have significant R&D and manufacturing operations in China. All three firms also supply parts of China's own telecoms networks. The UK has benefitted from the strong competitive forces present in the global market. Significant investments in R&D that would not be possible in a world of national champions have resulted in rapid technological innovation.

It is important that restrictions on the use of equipment provided by high risk vendors do not unintentionally weaken the security of networks by reducing network diversity, or by causing an overreliance on vendors who are known to have less developed equipment and have unknown security risks due to a lack of transparency. The Intelligence and Security Committee's Statement on 5G Suppliers (July 2019) made clear that maintaining a market of three suppliers – Nokia, Ericsson and Huawei – will result in higher overall security.

Some commentators have questioned whether Samsung could provide an alternative. Samsung currently provides 5G telecoms equipment in South Korea, and some limited services in Japan and the US. However, Samsung is not currently used in the UK or in the rest of Europe. This is an issue that is worthy of further examination by the Committee, as is the lack of domestic supplier in the UK or its main strategic allies such as the US.

There is also currently no alternative that could meet the UK's deployment targets, without a significant impact on the delivery timetable and cost of deployment of 5G. The Supply Chain Review recognised that the high levels of R&D and time taken to develop technically capable products restricts the ability of new entrants to the market. Huawei, for example has invests billions into research and development (more than $15 billion globally last year). The development of its 5G technology required the work of thousands of highly qualified engineers and mathematicians over many years to bring it from the laboratory to the real world.

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

From Huawei's perspective, the UK government ran a methodical, evidence-based process, despite enormous politically motivated pressure for tougher restrictions from the US. The Government's Supply Chain Review placed significant scrutiny on Huawei, which allowed the technical considerations of risk and mitigation to come to the fore. The National Security Council, chaired by the Prime Minister, decided to allow Huawei to continue operating in the UK, with significant restrictions on the use of its equipment. Huawei firmly believes that this decision reinforces the UK's position as a global leader on cyber security.

This decision was taken on the advice of NCSC, which has been on public record stating its firm belief that any risks of Huawei's continued involvement in UK telecoms infrastructure can be adequately mitigated. This mitigation is provided by HCSEC. It was set up to manage potential cyber security risks from the use of Huawei's equipment in UK telecoms networks. HCSEC has provided extensive assurance to its Oversight Board that there are no concerns around malfeasance. We would note that no other vendors open themselves to this level of scrutiny.

Additional mitigations will be provided by the new Telecoms Security Requirements, which will be passed under the Telecoms Security Bill. These are significant additional measures relating to the use of equipment provided by all vendors that the Government itself believes will allow it to mitigate the potential risk posed by the supply chain, as well as stringent enhanced requirements that mean Huawei equipment will not be used in any sensitive networks nor any sensitive parts of networks.

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

The specific restrictions recently announced by the Government mean that equipment from high risk vendors, including Huawei, cannot be used in sensitive networks. This includes the UK's defence and intelligence networks. The Intelligence and Security Committee's Statement on 5G Suppliers made clear that different levels of security should be applied to different parts of the network, and that communication channels which are used for intelligence exchange would always be kept entirely separate.

This has been the case for Huawei since we first started operating in the UK. The Government's new laws will now make sure that Huawei's equipment will never be used in defence and intelligence networks in the future. Given this, it is difficult to see how this decision will have any impact on the UK's security and defence capabilities, or on its interoperability with allies.

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

The UK currently has no sovereign industrial capability in the area of 5G equipment. Indeed, there is no sovereign industrial capability within the Five Eyes group. Industrial capability is focused within the major global players, including Ericsson and Nokia.

It is right that a global, rules-based multilateral system develops in the telecoms sector. Globalisation and trade liberalisation promote innovation and collaboration, allowing all countries to take advantage of rapid improvements in technologies. The UK could play a leading role in this space, drawing on its deep expertise in cybersecurity and the world leading approach it has taken as a result of the Supply Chain Review. A thriving vendor market drives innovation and technological evolutions like 5G, with all the benefits that this technology will bring.

Significant time and investment are required to build sufficient industrial capability to compete on the global stage. Huawei, for example invests roughly 15% of its sales revenue into R&D every year, totalling $71 billion over the last decade. Huawei's commitment to the UK remains strong. Development of domestic industrial capability will require a long-term approach from the government, working closely with industry.

16 April 2020