HOUSE OF COMMONS LIBRARY

DEBATE PACK

Number CDP 2020/0045, 3 March 2020

Security implications of including Huawei in 5G

By Georgina Hutton
Nikki Sutherland
Joanna Dawson

This pack has been prepared ahead of the debate to be held in Westminster Hall at 9.30am on Wednesday 4 March 2020 on the security implications of including Huawei in 5G. The debate will be opened by Sir Iain Duncan Smith MP.

Contents

The House of Commons Library prepares a briefing in hard copy and/or online for most non-legislative debates in the Chamber and Westminster Hall other than half-hour debates. Debate Packs are produced quickly after the announcement of parliamentary business. They are intended to provide a summary or overview of the issue being debated and identify relevant briefings and useful documents, including press and parliamentary material. More detailed briefing can be prepared for Members on request to the Library.

1. Background

1.1 What is 5G?

5G is the next generation of wireless communications technology, after 2G, 3G and 4G mobile broadband. It is expected to provide faster connections with much higher capacity and very fast response times. It will allow many more users and devices to access fast internet connections and large amounts of data at the same time.

Mobile networks are the first commercial application of 5G. 5G is also expected to be used in applications beyond mobile networks, for example in healthcare, smart cities, transport and manufacturing.

5G for mobile broadband is being rolled-out by private mobile network operators. There are four Mobile Network Operators in the UK: EE, O2, Vodafone and Three. Ofcom reported in December 2019 that 5G was live in 40 towns and cities across the UK.

5G involves some new approaches to network architecture and design, which raises both new security challenges as well as opportunities. 5G technology will integrate existing security measures developed for 4G networks. Key differences between 4G and 5G networks from a security perspective include:

- 5G is expected to include greater numbers of base stations than previous mobile networks and will connect more user devices. This means there are more potential sites that could be vulnerable to attack.
- 5G will involve new use cases, including potentially supporting critical national infrastructure applications. This has implications for the potential consequences of an attack on the network.
- 5G is more likely to use commodity ("off-the-shelf") hardware and software-based functions to control network traffic. This creates both challenges and opportunities for security.
- "Core" network functions (such as user authentication) may move closer in location to the "edge" of the network (base stations). This is required to support the low-latency (high response times) features of 5G. This aspect is discussed further in Section 1.2 of this pack below.

In the first instance in the UK, 5G is being rolled out on existing 4G infrastructure (called non-standalone 5G). This means that vendors used for 5G roll-out must be compatible with existing 3G/4G infrastructure.

The technical security considerations for 5G network design are explained in a blog post written by the NCSC's technical director (Dr Ian Levy) in January 2020.

The Parliamentary Office of Science and Technology POSTbrief on 5G technology (24 July 2019) provides further background information about 5G technology.

The Library briefing paper on 5G (September 2019) provides information about Government policy on 5G roll-out.

1.2 Concerns about the inclusion of Huawei

Section 2.5 of the Library briefing paper on 5G provides background discussion on the security supply chain concerns about 5G.

During the last parliamentary session, the Intelligence and Security Committee (ISC) was engaged in examining the role of Huawei in the UK's telecommunications infrastructure as part of a wider Inquiry into national security issues relating to China. The ISC published a statement in July 2019 following press coverage concerning the Government's decision on which companies to involve in 5G. It noted that the US and Australia have banned Huawei from their networks on the basis of concerns over the nature of its relationship with the Chinese state and the consequent risk of espionage or sabotage. However it also pointed to statements by the National Cyber Security Centre (NCSC) that the focus should be on building the UK network so as to withstand attacks from any quarter, rather than on potential risks posed by a specific country or company. This could be achieved by diversifying suppliers and through network design.

There are only three potential suppliers of mobile access network equipment in the UK – Nokia, Ericsson and Huawei. The ISC suggested that limiting the field to just two suppliers, on the basis of security concerns about Huawei, could lead to over-dependence and reduce competition. This in turn could result in less resilience and lower security standards.

The ISC went on to acknowledge that the question could not be viewed solely from a technical perspective because of the wider geostrategic ramifications, including in relation to intelligence sharing relationships, and the UK's desire to have closer economic links with China.

The Government's Telecoms Supply Chain Review (discussed in more detail below), also published in July 2019, included a telecoms sector risk assessment, which identified the 'backdoor' threat as one category of risk. This refers to malicious capability added to equipment. A subset of this risk is a link between a supplier and a hostile state actor, and the intent of that State with respect to the UK. The Review identified the 2017 Chinese National Intelligence Law as the most obvious focus for this risk. It has been suggested that this law can require individuals and organisations to cooperate with the Chinese intelligence agencies if requested. However in June 2019 a Huawei representative refuted the suggestion that the law could require the company to do anything to weaken its security in evidence to the Science and Technology Committee.

In a letter to the Secretary of State for Digital, Culture, Media and Sport, in July 2019, the Science and Technology Committee concluded that, from a technical perspective, the complete exclusion of Huawei from the UK's telecommunications network would not be a proportionate response to the potential security threat.

The UK has long standing intelligence sharing arrangements with the US under the 'Five Eyes' agreement between the US, the UK, Canada,

Australia and New Zealand. It has been suggested that the US administration sought to put pressure on the UK Government by threatening to limit intelligence sharing in the event that Huawei was allowed access to the UK's network. However, Andrew Parker, Director General of MI5, has said that he has no reason to think that the decision would have a negative impact on intelligence sharing with the US. And a US intelligence official reportedly told the Munich security conference in February that the decision would not lead to an erosion in the intelligence sharing relationship.

1.3 Telecoms Supply Chain Review

DCMS led a cross-government review of UK telecommunications supply chains, in November 2018. The review involved an assessment of the supply chain arrangements for UK telecoms networks, focusing on full-fibre and 5G networks.[1]

The Review Report was published on 22 July 2019. It set out plans to develop a new statutory Telecoms Security Requirement (TSR) that telecommunications providers and vendors will be required to comply with. The new legislative framework will include new powers for Ofcom to enforce the security requirements. The Report states that legislation will be pursued "at the earliest opportunity" and in the meantime it would work with telecoms operators to ensure they adhere to new guidance on a cooperative basis.[2] The Report also states that the Government will pursue a diversification strategy to support the development and growth of new market players.

The July 2019 review report did not include a decision on whether "high risk vendors" such as Huawei would be allowed to supply to UK 5G networks. The Government stated that this was because it is still considering the implications of the steps taken by the US to place restrictions on exports of US products and services to Huawei.[3]

1.4 Decision on high risk vendors (January 2020)

On 28 January 2020 the Government announced its decision on "high risk vendors", including (but not limited to) Huawei, in UK telecoms networks.[4] The decision applies to UK telecoms networks generally, not just 5G.

The Government, on advice from the NCSC, decided that:

- High-risk vendors are to be excluded from sensitive "core" parts of 5G and gigabit-capable networks
- High-risk vendors are to be excluded from sensitive and safety/critical locations such as Critical National Infrastructure

1 DCMS, Telecoms Supply Chain Review Terms of Reference, 8 November 2018.
2 DCMS, Telecoms Supply Chain Review Report, 22 July 2019, page 6.
3 DCMS, Telecoms Supply Chain Review Report, 22 July 2019, para 5.23 and 5.24.
4 HC Deb 28 Januaruy 2020

- High-risk vendor access to non-sensitive parts of the network is to be limited to 35%[5]

The NCSC stated that any use of high-risk vendors should be accompanied by a "bespoke mitigation strategy" tailored to each vendor. For Huawei, this would be an "evolution" of the Government's existing Huawei Cyber Security Evaluation Centre (HCSEC).

The Government's decision was accompanied by technical reports and a blog post from the NCSC explaining its security analysis and advice, including:

1. A security analysis for the UK telecoms sector
2. A blog explaining the work that went into the analysis
3. Guidance to UK Telecoms operators on the use of high risk vendors

The Government stated it would "seek to legislate at the earliest opportunity" to put this decision on a statutory footing and provide powers necessary to enforce/implement this decision. Implementation of the decision by operators is currently voluntary.

What is a high-risk vendor?

The Government describes "high risk vendors" (HRVs) as those that "pose greater security and resilience risks to UK telecoms networks". The NCSC has published advice to telecoms companies that includes a list of non-exhaustive criteria for identifying high risk vendors.[6] Factors include the strategic position and scale of the vendor in the UK and other telecoms markets, the quality and transparency of the vendors engineering, and factors relating to the ownership and operating location of the vendor (such as domestic security laws).

Huawei is considered a high-risk vendor.

The 35% cap

The 35% cap is roughly equivalent to Huawei's existing UK market share for the 4G mobile access network; Huawei's market share is higher (45%) for fixed-access networks (full-fibre).[7]

On the 35% cap the NCSC explains:

> The cap balances two different security and resiliency risks; the first is the risk associated with high risk vendors and the second is the need for diversity of supply. The cap at 35% ensures the UK will not become nationally dependent on a high risk vendor while retaining competition in the market and allowing operators to continue to use two Radio Access Network (RAN) vendors. The calculation of 35% is also interesting. We've been quite subtle about how we calculate that – it's important to make sure it can't

5 DCMS, New plans to safeguard country's telecoms network and pave way for fast, reliable and secure connectivity, 28 January 2020
6 NCSC, NCSC advice on the use of equipment from high risk vendors in UK telecoms networks, 28 January 2020
7 HC Deb 28 January 2020, c721; DCMS, Telecoms Supply Chain Review, 22 July 2019, page 30.

> be easily gamed, for example by using an HRV's basestations in all the cities and a non-HRV's products in the countryside.[8]

The Government's press release stated that the "recommended cap of 35 per cent will be kept under review to determine whether it should be further reduced as the market diversifies".[9] Some MPs have called on the Government to outline a plan for reducing the 35% cap to zero over time.[10][11]

Core vs edge functions in 5G networks

5G networks are likely to see core functions move closer in location to edge sites. This is needed to support the low-latency (high signal response rates) for 5G networks. The security protections for core functions would also need to be pushed out closer to the edge to keep those sites secure.

It is often stated that 5G networks "blur" the distinction between the security-critical "core" network functions and the access network "edge" functions (the part of the network that users interact with, such as mobile base stations). This has raised concerns about the inclusion of high risk vendors in "edge" functions for 5G networks. For example, the Head of the Australian Signals Directorate stated in a speech in October 2018 that "the distinction between core and edge collapses in 5G networks" and has advised the Australian Government to exclude high risk vendors from 5G networks entirely.[12]

The NCSC expects that in the UK, it is likely that core functions will be located in each metropolitan area for example, but not on every base station. The NCSC's advice is that the core and edge functions in 5G networks can distinguished in the 5G technical standards:

> In 5G networks, core functions can be relocated nearer the 'edge' of the network. This has been described as blurring the line between core and edge. This is technically inaccurate as the 'core' is defined by a set of functions, standardised within [5; the technical 5G standards], rather than a location. Consequently, the distinction between the two remains clear, as does the advice above. Our advice remains that HRVs are excluded from performing core functions, and this applies whether these functions are deployed centrally or towards the 'edge'. Our understanding is that this clarification is unlikely to be consequential in the UK, as we are informed that core functions may run near the edge, but not actually on edge access equipment (such as base stations).[13]

---

8 NCSC, The future of telecoms in the UK, Dr Ian Levy, 28 January 2020

9 DCMS, New plans to safeguard country's telecoms network and pave way for fast, reliable and secure connectivity, 28 January 2020

10 Huawei: Senior Tories want Huawei 'ruled out' of 5G plans, *BBC News*, 8 February 2020; Senior Tories sound alarm over Huawei role in UK 5G network, Sebastian Payne, *Financial Times*, 8 February 2020.

12 Director-General ASD speech to ASPI National Security Dinner, Mike Burgess, Director-General ASD speaking at Australian Security Policy Institute, Canberra, 29 October 2019

12 Director-General ASD speech to ASPI National Security Dinner, Mike Burgess, Director-General ASD speaking at Australian Security Policy Institute, Canberra, 29 October 2019

13 NCSC, Summary of NCSC's security analysis for the UK telecoms sector, Section 8.3.1, 28 January 2020.

The House of Commons Science and Technology Committee came to the same conclusion following an evidence session on UK telecommunications networks. The Committee pointed to statements from the NCSC's technical director on the difference between the UK and Australia's geography (see full text for underlying references):

> Although the Australian Government has concluded that the distinction between the 'core' and 'non-core' elements of 5G networks will be less clear than for previous technology generations, we heard unanimously and clearly that a distinction between the 'core' and 'non-core' parts of a 5G network will still exist. Dr Ian Levy, Technical Director of the National Cyber Security Centre, has explained that "for a purely technical point of view, geography matters in 5G:
>
> > UK and Australia have very different geographies – so our laydowns will be very different to Australia's laydowns. So, we may have exactly the same technical understanding, but come to very different conclusions.[14]

The Intelligence and Security Committee in their July 2019 statement also emphasised that the focus should be on the sensitivity of the functions rather than where in the network they are located:

> In so doing, some parts of the network will require greater protection: critical functions cannot be put at risk. But there are less sensitive functions where more risk can be carried. (It is this distinction - between the sensitivity of the functions - that must determine security, rather than where in the network those functions are located: notions of 'core' and 'edge' are therefore misleading in this context.) We should therefore be thinking of different levels of security, rather than a one size fits all approach, within a network that has been built to be resilient to attack, such that no single action could disable the system.[15]

[14] Letter from House of Commons Science and Technology Committee Chair to Secretary of State for DCMS, dated 10 July 2019.

[15] Intelligence and Security Committee of Parliament, Statement on 5G suppliers (pdf), 19 July 2019

2. News and blogs

BBC Science Focus Magazine

5G and the Huawei controversy: is it about more than just security?

21 February 2020

https://www.sciencefocus.com/news/5g-and-the-huawei-controversy-is-it-about-more-than-just-security/

Guardian

US defence secretary warns Huawei 5G will put alliances at risk

15 February 2020

https://www.theguardian.com/us-news/2020/feb/15/us-defence-secretary-warns-us-alliances-at-risk-from-huawei-5g

BBC News

Huawei: Senior Tories want Huawei 'ruled out' of 5G plans

8 February 2020

https://www.bbc.co.uk/news/uk-51424133

Dr Leslie Vinjamuri, Chatham House

Britain Walks Post-Brexit Tightrope With Huawei Decision

4 February 2020

https://www.chathamhouse.org/expert/comment/britain-walks-post-brexit-tightrope-huawei-decision

Guardian

Huawei ruling will cost us £500m, says BT

30 January 2020

https://www.theguardian.com/business/2020/jan/30/huawei-ruling-will-cost-us-500m-says-bt

FT

EU draws up 5G plan to screen security risks amid Huawei fears

29 January 2020

https://www.ft.com/content/ee3f0764-41fc-11ea-bdb5-169ba7be433d

National Cyber Security Centre

The future of telecoms in the UK

NCSC Technical Director Dr Ian Levy explains how the security analysis behind the DCMS supply chain review will ensure the UK's telecoms networks are secure – regardless of the vendors used

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

28 January 2020

BBC News

Huawei 5G verdict is a decision 'with few good options'

28 January 2020

https://www.bbc.co.uk/news/technology-51263799

FT

US attacks UK's decision on Huawei

28 January 2020

https://www.ft.com/content/e3d38d0e-41c5-11ea-a047-eae9bd51ceba

James Sullivan, Royal United Services Institute (RUSI)

Huawei, Not All the Way

27 January 2020

https://rusi.org/commentary/huawei-not-all-way

3. Press releases

Department for Digital, Culture, Media & Sport, National Cyber Security Centre

New plans to safeguard country's telecoms network and pave way for fast, reliable and secure connectivity

28 January 2020

NEW restrictions should be placed on the use of high risk vendors in the UK's 5G and gigabit-capable networks, the government has announced at the conclusion of its Telecoms Supply Chain Review.

- High risk vendors to be excluded from sensitive 'core' parts of 5G and gigabit-capable networks
- 35 per cent cap on high risk vendor access to non-sensitive parts of the network
- NCSC issues guidance to operators on implementing decision with legislation introduced at the earliest opportunity

Ministers today determined that UK operators should put in place additional safeguards and exclude high risk vendors from parts of the telecoms network that are critical to security.

High risk vendors are those who pose greater security and resilience risks to UK telecoms networks.

The Prime Minister chaired a meeting of the National Security Council (NSC), where it was agreed that the National Cyber Security Centre (NCSC) should issue guidance to UK Telecoms operators on high risk vendors following the conclusions of the Telecoms Supply Chain Review.

This advice is that high risk vendors should be:

- Excluded from all safety related and safety critical networks in Critical National Infrastructure
- Excluded from security critical 'core' functions, the sensitive part of the network
- Excluded from sensitive geographic locations, such as nuclear sites and military bases
- Limited to a minority presence of no more than 35 per cent in the periphery of the network, known as the access network, which connect devices and equipment to mobile phone masts

As part of the Review, the NCSC carried out a technical and security analysis that offers the most detailed assessment in the world of what is needed to protect the UK's digital infrastructure.

The guidance sets out the practical steps operators should take to implement the government's decision on how to best mitigate the risks of high risk vendors in 5G and gigabit-capable networks.

The government will now seek to legislate at the earliest opportunity to put in place the powers necessary to implement this tough new telecoms security framework.

The government is certain that these measures, taken together, will allow us to mitigate the potential risk posed by the supply chain and to combat the range of threats, whether cyber criminals, or state sponsored attacks.

The Review also highlighted the need for the UK to improve the diversity in the supply of equipment to telecoms networks.

The government is now developing an ambitious strategy to help diversify the supply chain. This will seek to attract established vendors who are not present in the UK, supporting the emergence of new, disruptive entrants to the supply chain, and promoting the adoption of open, interoperable standards that will reduce barriers to entry.

The recommended cap of 35 per cent will be kept under review to determine whether it should be further reduced as the market diversifies.

Today's decision marks a major change in the UK's approach that will substantially improve the security and resilience of our critical telecoms networks. It will see the government roll out the most stringent set of controls ever - including new standards with tough underpinning legislation to raise the security and quality of the entire 5G and gigabit-capable networks.

Digital Secretary Baroness Morgan said:

> We want world-class connectivity as soon as possible but this must not be at the expense of our national security. High risk vendors never have been and never will be in our most sensitive networks.
>
> The government has reviewed the supply chain for telecoms networks and concluded today it is necessary to have tight restrictions on the presence of high risk vendors.
>
> This is a UK-specific solution for UK-specific reasons and the decision deals with the challenges we face right now.
>
> It not only paves the way for secure and resilient networks, with our sovereignty over data protected, but it also builds on our strategy to develop a diversity of suppliers.
>
> We can now move forward and seize the huge opportunities of 21st century technology.

Ciaran Martin, the Chief Executive of the National Cyber Security Centre, said:

> This package will ensure that the UK has a very strong, practical and technically sound framework for digital security in the years ahead.
>
> The National Cyber Security Centre has issued advice to telecoms network operators to help with the industry rollout of 5G and full fibre networks in line with the government's objectives.
>
> High risk vendors have never been – and never will be – in our most sensitive networks.

> Taken together these measures add up to a very strong framework for digital security.

Further background

The decision today concludes the Telecoms Supply Chain Review, first published in July 2019. The review was a comprehensive, evidence-based review, designed to ensure the security and resilience of the UK's networks.

It recommended new Telecoms Security Requirements (TSR) to provide clarity to the telecoms industry on what is expected in terms of network security.

The TSRs will raise the height of the security bar by setting out to telecoms operators - overseen by Ofcom and the government - the way to design and manage their networks to meet tough new standards.

Another area covered by the Review was how to treat those vendors which pose greater security and resilience risks to UK telecoms.

The Review also highlighted the need for the UK to improve the diversity in the supply of equipment to telecoms networks.

Today the government has announced the final conclusions of the Telecoms Supply Chain Review in relation to high risk vendors. The government, through the National Security Council, asked the NCSC to consider issuing guidance to UK Telecoms operators in relation to high risk vendors. That guidance has been published alongside the final conclusions of the Review.

The NCSC has published a number of documents. These are:

- A security analysis for the UK telecoms sector
- A blog explaining the work that went into the analysis
- Guidance to UK Telecoms operators on the use of high risk vendors
- An explanation of 5G

Mobile UK

Mobile UK Statement on Huawei

28 January 2020

Hamish MacLeod, Director at Mobile UK, comments on the Government's decision to let Huawei continue to be used in the UK's 5G networks:

> The mobile industry continues to believe that it is in the interests of customers and the UK's desire to be a global leader in 5G that it must have access to a diverse supply chain that is open to the latest and most innovative technologies.
>
> Mobile UK welcomes the clarity provided by the Government and the certainty it provides going forward.

techUK

techUK comments on the conclusion of the Telecoms Supply Chain Review

28 January 2020

techUK CEO Julian David responds to the Government's announcement on the conclusion of its Telecoms Supply Chain Review.

Commenting on today's Government announcement on the conclusion of its Telecoms Supply Chain Review, Julian David CEO of techUK said:

> The deployment of 5G and full-fibre broadband will underpin the economic transformation of the UK over the next decade.
>
> Today's decision sets out how 5G can be rolled out quickly and securely. It gives businesses deploying that infrastructure more of the clarity that they need to get on and build their networks.
>
> To drive innovation in the long-term we need a diverse and competitive supply chain and we encourage Government to lower barriers to entry for new vendors. techUK, with members from across the telecoms sector, will continue to work with DCMS and Ofcom to determine how the security and resilience needed for tomorrow's telecoms networks is assured.

Intelligence and Security Committee of Parliament

Statement on 5G suppliers

19 July 2019

There has been a great deal of public and parliamentary debate recently as to whether the Chinese technology company Huawei should be allowed to supply equipment for the United Kingdom's 5G telecommunications network. Despite the Government's announcement in 2017 that the UK would be a global leader in 5G, the Government has yet to make a decision as to which companies will be involved.

In a sense, this is not surprising. 5G will transform our day to day lives - if it meets its full potential - and it could be key to our future prosperity. Such an important decision therefore requires careful consideration. However, the extent of the delay is now causing serious damage to our international relationships: a decision must be made as a matter of urgency.

At the heart of the public debate has been suspicion around Huawei as a Chinese company. The US and Australia have banned the company from their networks - despite it being a world leader in the development of 5G technology - voicing concern over the nature of Huawei's relationship with the Chinese state and therefore the potential risk of espionage or sabotage.

However the National Cyber Security Centre (NCSC) - which, as part of GCHQ, provides cyber security advice - has been clear that the security of the UK's telecommunications network is not about one company or one country: the 'flag of origin' for telecommunications equipment is not the critical element in determining cyber security. This is logical: we

know, for example, that Russia has carried out significant hostile cyber activity against UK telecommunications networks, and yet there is no Russian equipment in the UK's networks.

The point being made in NCSC's statements thus far appears to be that this is not about whether or not Huawei - or indeed any company - might wish to, or be instructed to, sabotage the UK network or use it to spy on the UK. It is that the UK network has to be built in such a way that it can withstand attack from any quarter - whether that be malicious action from someone within the network, a cyber attack from actors outside, or simple human error. Their approach, in effect, is to assume all worst case scenarios and protect the network accordingly.

In so doing, some parts of the network will require greater protection: critical functions cannot be put at risk. But there are less sensitive functions where more risk can be carried. (It is this distinction - between the sensitivity of the functions - that must determine security, rather than where in the network those functions are located: notions of ‘core' and 'edge' are therefore misleading in this context.) We should therefore be thinking of different levels of security, rather than a one size fits all approach, within a network that has been built to be resilient to attack, such that no single action could disable the system.

NCSC have said that this can best be achieved by diversifying suppliers. The arguments for this are two-fold: reducing over-dependence and increasing competition. First, the network should not be dependent on just one vendor, as this would render it less resilient. Secondly, requiring Mobile Network Operators to use equipment from more than one vendor increases competition between those vendors which will force them to improve their security standards. And it is this raising of the bar on cyber security standards across the board that is needed - together with a requirement for more stringent regulation and enforcement of those standards.

However the telecoms market has been consolidated down to just a few players: in the case of 5G there are only three potential suppliers to the UK - Nokia, Ericsson and Huawei. Limiting the field to just two, on the basis of the above arguments, would increase over-dependence and reduce competition, resulting in less resilience and lower security standards. Therefore including a third company - even if you may have some security concerns about them and will have to set a higher bar for security measures within the system - will, counter-intuitively, result in higher overall security.

NCSC's position is eminently sensible: the UK must have a secure 5G network that is protected against the wide range of threats rather than focussing on just one potential threat. However, this issue cannot be viewed solely through a technical lens – because it is not simply a decision about telecommunications equipment. This is a geostrategic decision, the ramifications of which may be felt for decades to come.

First, there is the question of our intelligence-sharing relationship with our closest allies. From amongst our Five Eyes partners, the United States and Australia have already been vocal in their concern that the

UK might employ Huawei within its 5G network. We should emphasise that this is not about any risk to the communication channels which are used for intelligence exchange - these would always be kept entirely separate. It is about perception as much as anything: our Five Eyes partners need to be able to trust the IJK and we must not do anything which puts that at risk - the value of the partnership cannot be overstated.

And there is a question as to whether other countries might follow the UK's decision. The UK is a world leader in cyber security: therefore if we allow Huawei into our 5G network we must be careful that that is not seen as an endorsement for others to follow.

Such a decision can only happen where the network itself will be constructed securely and with stringent regulation.

Then there is the UK's well-publicised desire for a strong economic relationship with China, and questions have been raised as to whether that is colouring our judgement on this issue. The public debate implies that we have to choose between good economic links with China and our own national security, on the basis that if Huawei were not included in our 5G network that would irretrievably damage our relationship with China. This is a simplistic viewpoint, and those promoting it do a disservice to China.

As a pragmatic global power, China clearly recognises the importance of reciprocity and mutual respect in international relations: the Chinese government would not allow a British company to play a similarly significant role in China's critical national infrastructure - and they will understand if the UK decides to follow their example. There are, after all, many other important areas on which we can collaborate to our mutual benefit.

This debate must not therefore be characterised as one between those who are 'pro- China', and those who are 'anti-China'. China, with its dynamic economy and growing global influence, is - and will continue to be - a key economic and diplomatic partner for the UK, and one with which we must continue to deal with respect. Huawei itself is a remarkable company which has achieved extraordinary technological advances, and brought radical innovation and competition to a sectorthat, without Huawei, might lack these attributes.

Indeed one of the lessons the UK Government must learn from the current debate over 5G is that with the technology sector now monopolised by such a few key players, we are over-reliant on Chinese technology - and we are not alone in this, this is a global issue. We need to consider how we can create greater diversity in the market. This will require us to take a long term view - but we need to start now.

In terms of the immediate issue, restricting those companies who may be involved in our 5G network will have consequences: both in terms of time and cost. And the Government must weigh these, together with the security advice that any risk posed could be managed in a secure system, against the geostrategic issues outlined above. It is important to take the right decision, and take it we must: this debate has been

unnecessarily protracted and this has damaged our international relationships. The new Prime Minister will no doubt have many issues to deal with in his first days in office.

Nevertheless, this Committee urges him to take a decision on which companies will be involved in our 5G network, so that all concerned can move forward.

House of Commons Science and Technology Committee

No technological grounds for banning Huawei, but ethical concerns must be taken into account

15 July 2019

The Science and Technology Select Committee today publishes a letter to the Secretary of State for Digital, Culture, Media and Sport about Huawei's involvement in the UK's 5G network.

- Letter to the Secretary of State (PDF 420 KB)
- Inquiry: UK telecommunications infrastructure
- Science and Technology Committee

Rt Hon Norman Lamb MP, Chair of the Science and Technology Committee, said:

> Following my Committee's recent evidence session, we have concluded that there are no technical grounds for excluding Huawei entirely from the UK's 5G or other telecommunications networks.
>
> The benefits of 5G are clear and the removal of Huawei from the current or future networks could cause significant delays.
>
> However, as outlined in the letter to the Secretary of State for Digital, Culture, Media and Sport, we feel there may well be geopolitical or ethical considerations that the Government need to take into account when deciding whether they should use Huawei's equipment. The Government also needs to consider whether the use of Huawei's technology would jeopardise this country's ongoing co-operation with our major allies.
>
> Moreover, Huawei has been accused of supplying equipment in Western China that could be enabling serious human rights abuses. The evidence we heard during our evidence session did little to assure us that this is not the case.
>
> I hope the evidence we have gathered helps the Government as it completes its Telecoms Supply Chain Review, which must be published by the end of August 2019."

4. Parliamentary material

Statement

UK Telecommunications

Lords statement on the security of the telecoms supply chain.

HL Deb 28 January 2020 | Vol 801 cc1338-1351

The Secretary of State, Department for Digital, Culture, Media and Sport (Baroness Morgan of Cotes)

My Lords, with the leave of the House, I will make a Statement on the security of the telecoms supply chain.

This Government are committed to securing nationwide coverage of gigabit-capable broadband by 2025, because we know the benefits that world-class connectivity can bring: from empowering rural businesses, to enabling closer relationships for the socially isolated, to new possibilities for our manufacturing and transport industries. We are removing the barriers to faster network deployment and have committed £5 billion of new public funding to ensure that no area is left behind. It is of course essential that these new networks are secure and resilient, which is why the Government have undertaken a comprehensive review of the supply arrangements for 5G and full-fibre networks.

The telecoms supply chain review—laid in the other place in July last year—underlined the range and nature of the risks facing our critical digital infrastructure, from espionage and sabotage to destructive cyberattacks. We have looked at the issue of how to maintain network security and resilience over many months and in great technical detail. We would never take decisions that threaten our national security or the security of our Five Eyes partners. As a result, the technical and security analysis undertaken by GCHQ's National Cyber Security Centre is central to the conclusions of the review. Thanks to its analysis, we have the most detailed study of what is needed to protect 5G, anywhere in the world. It is also because of the work of the Huawei Cyber Security Evaluation Centre Oversight Board, established by the NCSC, that we know more about Huawei and the risks it poses than any other country. We are now taking forward the review's recommendations in three areas.

First, on world-leading regulation, we are establishing one of the strongest regimes for telecoms security in the world—a regime that will raise security standards across the UK's telecoms operators and the vendors that supply them. At the heart of the new regime, the NCSC's new telecoms security requirements guidance will provide clarity to industry on what is expected in terms of network security. The TSRs will raise the height of the security bar and set out tough new standards to be met in the design and operation of the UK's telecoms networks. The Government intend to legislate at the earliest opportunity to introduce a

new comprehensive telecoms security regime, to be overseen by the regulator, Ofcom, and government.

Secondly, the review also underlined the need for the UK to improve diversity in the supply of equipment to telecoms networks. Currently, the UK faces a choice of only three major players to supply key parts of our telecoms networks. This has implications for the security and resilience of these networks, as well as for future innovation and market capacity. It is a "market failure" that needs to be addressed. The Government are developing an ambitious strategy to help diversify that supply chain. This will entail the deployment of all the tools at the Government's disposal, including funding.

We will do three things simultaneously: seek to attract established vendors to our country who are not present in the UK; support the emergence of new, disruptive entrants to the supply chain; and promote the adoption of open, interoperable standards that will reduce barriers to entry.

The UK's operators are leading the world in the adoption of new, innovative approaches to expand the supply chain. The Government will work with industry to seize these opportunities, and we will partner with like-minded countries to diversify the telecoms market. It is essential that we are never again in a position of having limited choices when deploying important new technologies.

The third area covered by the review was how to treat vendors which pose greater security and resilience risks to UK telecoms. As I know the House has a particular interest in this area, I will cover this recommendation in detail. Those risks may arise from technical deficiencies or considerations relating to the ownership and operating location of the vendor. As noble Lords may recall, the Government informed the other place in July that they were not in a position to announce a decision on this aspect of the review. We have now completed our consideration of all the information and analysis from the National Cyber Security Centre, industry and our international partners. Today, I am able to announce the final conclusions of the telecoms supply chain review in relation to high-risk vendors.

In order to assess a vendor as high risk, the review recommends that a set of objective factors be taken into account. These include the strategic position or scale of the vendor in the UK network; the strategic position or scale of the vendor in other telecoms networks, particularly if the vendor is new to the UK market; the quality and transparency of the vendor's engineering practices and cyber security controls; the vendor's resilience, both in technical terms and in relation to the continuity of supply to UK operators; the vendor's domestic security laws in the jurisdiction where the vendor is based and the risk of external direction that conflicts with UK law; the relationship between the vendor and the vendor's domestic state apparatus; and, finally, the availability of offensive cyber capability by that domestic state apparatus, or associated actors, that might be used to target UK interests.

To ensure the security of 5G and full-fibre networks, it is both necessary and proportionate to place tight restrictions on the presence of any companies identified as higher risk. The debate is not just about "the core" and "the edge" of networks; neither is it just about trusted and untrusted vendors. Threats to our networks are many and varied, whether from cyber criminals or state-sponsored malicious cyber activity. The most serious recent attack on UK telecoms has come from Russia, and there is no Russian equipment in our networks.

The reality is that these are highly complicated networks relying on global supply chains, where some limited measure of vulnerability is inevitable. The critical security question is: how to mitigate such vulnerabilities and stop them damaging the British people and our economy.

For 5G and full-fibre networks, the review concluded that, based on the current position of the UK market, high-risk vendors should be excluded from all safety-related and safety-critical networks in critical national infrastructure; excluded from security-critical network functions; limited to a minority presence in other network functions up to a cap of 35%; and be subjected to tight restrictions, including exclusions from sensitive geographic locations.

These new controls are also contingent on an NCSC-approved risk mitigation strategy for any operator who uses such a vendor. We will legislate at the earliest opportunity to limit and control the presence of high-risk vendors in the UK network and to allow us to respond as technology changes.

Over time, our intention is for the market share of high-risk vendors to reduce as market diversification takes place. I also want to be clear that nothing in the review affects this country's ability to share highly sensitive intelligence data over highly secure networks, both within the UK and with our partners, including the Five Eyes. GCHQ has categorically confirmed that how we construct our 5G and full-fibre public telecoms networks has nothing to do with how we share classified data. The UK's technical security experts have agreed that the new controls on high-risk vendors are completely consistent with the UK's security needs.

In response to the review's conclusions on high-risk vendors, the Government have asked the NCSC to produce guidance for industry. This guidance was published earlier today on the NCSC's website. The NCSC has helped operators to manage the use of vendors that pose a greater national security risk, such as Huawei and ZTE, for many years.

This new guidance will include how it determines whether a vendor is high risk, the precise restrictions it advises should be applied to high-risk vendors in the UK's 5G and full-fibre networks, and what mitigation measures operators should take if using high-risk vendors. As with other advice from the NCSC on cybersecurity matters, this advice will be in the form of guidance. The Government expect UK telecoms operators to give due consideration to this advice, as they do with all their interactions with the NCSC.

I recognise that noble Lords may wish to pursue further the technical details of these proposals, not least with my officials and officials at the National Cyber Security Centre, who will be available to answer questions in Committee Room 11 from 4.30 pm today.

I hope the whole House will agree that if we are to achieve our digital connectivity ambitions, it is imperative that we trust the safety and security of our telecoms networks. Risk cannot be eliminated in telecoms, but it is the job of the Government, Ofcom and industry to work together to ensure that we reduce our vulnerabilities and mitigate the risks. The Government's position on high-risk vendors marks a major change in the UK's approach. When taken together with the tough new security standards that will apply to operators, this approach will substantially improve the security and resilience of the UK's telecoms networks, which are a critical part of our national infrastructure. It reflects the maturity of the UK's market and our world-leading cybersecurity expertise, and it follows a rigorous and evidenced-based review. It is the right decision for the UK's specific circumstances.

The future of our digital economy depends on trust in its safety and security. If we are to encourage the take-up of new technologies that will transform our lives for the better, we need to have the right measures in place. That is what this new framework will deliver, and I commend this Statement to the House.

[followed by questions}

Statement repeated, followed by questions, in the Commons:

UK Telecommunications

Statement on the security of the telecoms supply chain.

HC Deb 28 January 2020 | Vol 670 cc708-727

Urgent Question

5G Network and *Huawei*

Urgent question on Huawei's involvement in the UK's 5G network.

HC Deb 27 January 2020 | Vol 670 cc533-546

Tom Tugendhat (Tonbridge and Malling) (Con)

To ask the Minister to make a statement on Huawei's involvement in the UK's 5G network.

The Parliamentary Under-Secretary of State for Digital, Culture, Media and Sport (Matt Warman)

I thank my hon. Friend the Member for Tonbridge and Malling (Tom Tugendhat) for this question. I know he has a deep interest in this issue, and my right hon. Friend the Secretary of State has corresponded with

him about it over the past few months. She will address this issue herself in the other place later today.

New telecoms technologies and next-generation networks like 5G and full fibre can change our lives for the better. They can give us the freedom to live and work more freely, help rural communities to develop thriving digital economies, and help socially isolated people to maintain relationships, so the security and resilience of the UK's telecoms networks is of paramount importance. The UK has one of the world's most dynamic digital economies, and we welcome open trade and inward investment. However, our economy can prosper and unleash Britain's potential only when we and our international partners are assured that our critical national infrastructure remains safe and secure.

As part of our mission to provide world-class digital connectivity, including 5G, my Department carried out a cross-Whitehall evidence-based review of the telecoms supply chain to ensure a diverse and secure supply base. That review's findings were published in July 2019 and set out the Government's priorities for the future of our telecommunications. Those priorities are strong cyber-security across the entire telecommunications sector, greater resilience in telecommunications networks and diversity across the entire 5G supply chain. It considered the UK's entire market position, including economic prosperity, the industry and consumer effects, and the quality, resilience and security of equipment.

However, in July, the review did not take a decision on the controls to be placed on high-risk vendors in the UK's telecoms network. Despite the inevitable focus on Huawei, that review was not about one company or even one country. We would never take a decision that threatens our national security or the security of our allies. The Government's telecoms supply chain review is a thorough review into a complex area that made use of the best available expert advice and evidence, and its conclusions on high-risk vendors will be reported once ministerial decisions have been taken.

The National Security Council will meet tomorrow to discuss these issues. This work is an important step in strengthening the UK's security frameworks for telecoms and ensuring the roll-out of 5G and full-fibre networks. I know that Members on both sides of the House feel strongly about this issue, and the Government will make a statement to the House to communicate final decisions on high-risk vendors at the appropriate time. We will always put national security at the top of our agenda.

[followed by questions]

Answer repeated in the Lords, followed by questions:

***Huawei*: UK's 5G Network**

Lords statement on Huawei's involvement in the UK's 5G network.

HL Deb 27 January 2020 | Vol 801 cc1296-1300

PQs

Huawei: 5G

Asked by: Onwurah, Chi

To ask the Secretary of State for Digital, Culture, Media and Sport, whether the Government has made an assessment on the effect of the decision to give Huawei permission to build parts of the UK's 5G network on UK-US digital trade.

Answering member: Matt Warman | Department: Department for Digital, Culture, Media and Sport

The UK has one of the world's largest and most dynamic economies, and we welcome open trade and inward investment in our digital sectors. At the same time, the UK's economy can only prosper when we, and our international partners, are assured that our critical national infrastructure remains safe and secure.

We have announced one of the toughest regimes for telecoms security in the world. This should reassure the US and other partners that we are clear about the security risks we face. We worked closely with the US throughout the course of the Telecoms Supply Chain Review and will continue to work closely with them on telecoms security.

We have not taken these decisions lightly, this Government has underlined its commitment to making the UK a world leader in gigabit capable networks like 5G and full fibre, and have taken the decisions necessary to safeguard the UK's national security interests.

HC Deb 24 February 2020 | PQ 1969

Huawei: 5G

Asked by: Davis, Mr David

To ask the Secretary of State for Digital, Culture, Media and Sport, how much Huawei equipment analysis has been installed by UK 5G carriers since March 2019.

Answering member: Matt Warman | Department: Department for Digital, Culture, Media and Sport

Huawei's presence in the UK is subject to detailed, formal oversight through the Huawei Cyber Security Evaluation Centre and its oversight board. The recent conclusions of the Telecoms Supply Chain Review set

out clear limits on the role of Huawei, as a High Risk Vendor, in the UK telecoms market. The Government examined the full range of threats and risks when making its decision on the use of high risk vendors in the UK telecoms networks.

HC Deb 24 February 2020 | PQ 1865

Huawei: 5G

Asked by: Lord Taylor of Warwick

To ask Her Majesty's Government what steps they have taken to ensure that Huawei's limited role in the UK's 5G network does not present a security risk.

Answering member: Baroness Morgan of Cotes | Department: Department for Digital, Culture, Media and Sport

UK Telecoms operators have been advised by the National Cyber Security Centre - in its guidance published on 29 January - on the steps they need to take in relation to high risk vendors. The guidance also sets out the steps necessary for Huawei, including the important continuing role for the world class Huawei Cyber Security Evaluation Centre and Oversight Board.

In addition, new telecoms security requirements proposed in the Government's Telecoms Supply Chain Review will raise the height of the security bar and require telecoms operators to design and manage their networks to meet new requirements. They will provide clarity to industry on what is expected in terms of network security and, in turn, improve security across vendors.

HL Deb 06 February 2020 | PQ HL881

Huawei: 5G

Asked by: Lord Scriven

To ask Her Majesty's Government what arrangements for interoperability will be put in place for the use of Huawei equipment in the 5G network and any related systems.

Answering member: Baroness Morgan of Cotes | Department: Department for Digital, Culture, Media and Sport

Interoperability will be one of the three strands of the strategy that the Government is developing to help diversify the supply chain. This will entail the deployment of all the tools at the Government's disposal. The strategy has three main strands:

- Attracting established vendors who are not currently present in the UK;
- Supporting the emergence of new, disruptive entrants to the supply chain; and

- Promoting the adoption of open, interoperable standards that will reduce barriers to entry.

In addition, the Government's 5G Testbeds and Trials Programme provides an opportunity to support architectural models that open-up the radio access network, allowing operators to use different vendors for different components of the radio access network.

HL Deb 06 February 2020 | PQ HL1224

Huawei: 5G

Asked by: Lord Taylor of Warwick

To ask Her Majesty's Government what risk assessment they have conducted of the proposed adoption of Huawei technology for the UK's 5G network infrastructure.

Answering member: Baroness Barran | Department: Department for Digital, Culture, Media and Sport

The security of the UK's telecoms networks is of paramount importance. The Government has undertaken a comprehensive review of the telecoms supply chain to ensure the security and resilience of 5G and fibre in the UK. The Review, published in July, set out the Government's priorities for the future of telecommunications and proposed the introduction of a new, strengthened security framework for telecoms

The Review also considered the use of high risk vendors in UK telecoms networks. High risk vendors never have been and never will be in the UK's most sensitive networks. A decision on the use of high risk vendors in the UK telecoms networks will be made in due course following a robust assessment of the risks

The UK is not considering options that would put at risk the UK's national security or intelligence sharing. The Government continues to work closely with the US and other international partners on the issue of telecoms security.

HL Deb 22 January 2020 | PQ HL430

About the Library

The House of Commons Library research service provides MPs and their staff with the impartial briefing and evidence base they need to do their work in scrutinising Government, proposing legislation, and supporting constituents.

As well as providing MPs with a confidential service we publish open briefing papers, which are available on the Parliament website.

Every effort is made to ensure that the information contained in these publicly available research briefings is correct at the time of publication. Readers should be aware however that briefings are not necessarily updated or otherwise amended to reflect subsequent changes.

If you have any comments on our briefings please email papers@parliament.uk. Authors are available to discuss the content of this briefing only with Members and their staff.

If you have any general questions about the work of the House of Commons you can email hcinfo@parliament.uk.

Disclaimer

DEBATE PACK
CDP 2020/0045
3 March 2020