Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence

The Security of 5G

We write to you in your capacity as Chair of the Defence Select Committee following the launch of the Committee's inquiry into the security of 5G. The Government considers the security and resilience of our telecoms networks to be of paramount importance. We therefore welcome the Committee's interest as another important opportunity to engage with parliamentary colleagues and to set out the detail behind the Government's decision on the use of equipment from high risk vendors in the UK telecoms networks.

The Government conducted a comprehensive, evidence-based review into the telecoms supply chain which was launched in October 2018, with initial conclusions published in July 2019. The Review report set out the Government's priorities for the future of telecommunications as well as our intention to introduce one of the toughest regimes in the world for telecoms security.

The Government announced the final conclusions of the Review in relation to high risk vendors on 28 January. The conclusions set out stringent controls that should be imposed on the use of the equipment from high risk vendors to ensure that we can manage the risk and so that it will not impact on our sensitive networks.

We will:

- exclude high risk vendor equipment from the core of the UK's 5G and full fibre networks;
- limit high risk vendor equipment to a minority presence in other network functions up to a cap of 35 per cent; and
- work with our allies to develop market alternatives so that in time we can cut the need to include any high risk vendor equipment remaining within our telecommunications network.

The Government did not reach this view lightly. This position is based on the comprehensive security advice provided by the cyber security branch of GCHQ, the National Cyber Security Centre. The Government acknowledges that the need for any high risk vendor within our telecommunications network is an example of market failure. That is why we have committed to increasing R&D spending in the manifesto. The Government is committed to working with our Five Eyes and other allies to diversify the market and develop new supply chain capacity in this Parliament. We want to get to a position where we do not have to use a high risk vendor in our telecoms networks at all.

We are grateful once again to the Committee for its interest in this subject, and look forward to presenting evidence verbally to the Committee should an invitation be extended. Please accept this letter and the two attached annexes - the first from the Department for Digital, Culture, Media and Sport and the Ministry of Defence, and the second from the National Cyber Security Centre - as the Government's submission of written evidence to this inquiry.

We look forward to hearing from you as the inquiry progresses.

Rt Hon Oliver Dowden CBE MP
Secretary of State for
Digital, Culture, Media and Sport

Rt Hon Ben Wallace MP
Defence Secretary
MOD

23 April 2020

DEFENCE SELECT COMMITTEE INQUIRY - DCMS & MOD ANNEX
'THE SECURITY OF 5G'

Overview

The security of the UK's telecoms critical national infrastructure is of paramount importance. As new generations of digital communications are adopted and rolled out - from 5G in the mobile network to full fibre in the fixed network - it is vital that we understand and respond to the changing nature of technology in the context of the changing threat and risk landscape. That is why in October 2018 the Government launched a comprehensive, evidence-based review into the telecoms supply chain. The Review sought to answer three key questions:

1. How should we incentivise telecoms operators to improve security standards and practices in 5G and full fibre networks?
2. How should we address the security challenges posed by high risk vendors?
3. How can we create sustainable diversity in the telecoms supply chain?

At the forefront of the Review was the technical and security analysis led by the National Cyber Security Centre (NCSC). This was supplemented with the engagement of the UK telecoms industry, including telecommunications providers and equipment suppliers. The Review was also informed by economic analysis conducted by KPMG.

The initial conclusions of the Telecoms Supply Chain Review were published in a report in July 2019[1]. The final conclusions in relation to high risk vendors were announced in January 2020.

In response to the findings of the Review, the UK is establishing one of the strongest regimes for telecoms security in the world. This will raise security standards across the UK's telecoms operators and the vendors that supply them. At the heart of the new regime will be new security duties, which 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 will also provide Ofcom with the powers to effectively enforce the new framework.

In addition, the Government will establish stronger national security powers, to allow it to impose new controls on high risk vendors taking account of the advice provided by the NCSC and the outcome of the Telecoms Supply Chain Review. High risk vendors are those vendors which pose greater security and resilience risks to UK telecoms. In order to assess a vendor as high risk, the Review recommends a set of objective factors are taken into account including, but not limited to: 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 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 the availability of offensive cyber capability by that domestic state apparatus, or associated actors, that might be used to target UK interests. The Government has said it regards Huawei as a high risk vendor.

[1] https://www.gov.uk/government/publications/telecoms-supply-chain-review-terms-of-reference

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 high risk vendors. The Review's conclusions recommend that high risk vendors should be:

- excluded from security critical 'core' functions of the network;
- excluded from sensitive geographic locations;
- limited to a minority presence of no more than 35 per cent in the periphery of the network, known as the access network, which connects devices and equipment to mobile phone masts; and
- excluded from all safety related and safety critical networks in Critical National Infrastructure.

These new controls are also contingent on an NCSC-approved risk mitigation strategy for any operator who chooses to use such a vendor.

The Government will seek to introduce legislation to implement the new telecoms security framework, including the new powers to impose controls on high risk vendors, before the summer recess.

In relation to Huawei in particular, the UK knows more about Huawei and the risks it poses than any other country in the world. The Government has always considered Huawei to present higher risk and we have developed a bespoke risk mitigation strategy to carefully risk-manage their presence since they first came to the UK in 2003; first through the government's National Technical Authority for Information Assurance (CESG), and now through the NCSC, including the Huawei Cyber Security Evaluation Centre. The Huawei Cyber Security Evaluation Centre has access to full product information, including source code, allowing the behaviour of Huawei equipment to be analysed and understood. These arrangements exist specifically for Huawei, and were established to effectively mitigate the higher risk posed.

The Review also identified the lack of competition in the telecoms equipment market and the need to diversify the market. This is a global problem. The Government is therefore developing a targeted diversification strategy for the telecoms supply chain to ensure we have a more robust supply base. Over time our intention is to reduce our reliance on high risk vendors as market diversification takes place. We want to get to a position where we do not have to use high risk vendors in our telecoms networks at all, but to do that, we have to work with our Five Eyes and other partners to develop new supply chain capacity in our critical national infrastructure. The Government has set out that we will do that in this Parliament.

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

The Telecoms Supply Chain Review was informed by security analysis conducted by the NCSC. This security analysis highlighted four key security risks linked to the telecoms supply chain:

- national dependence on any one vendor, in particular those deemed 'high risk';
- faults or vulnerabilities in network equipment;
- the 'backdoor' threat - the embedding of malign functionality in vendor equipment; and
- vendor administrative access to provide equipment support or as part of a managed services contract.

These risks are applicable to all vendors and not just those considered high risk - all vendors carry a level of risk. The framework that the Government is implementing is

designed to address these risks through a combination of technical and regulatory measures. While these measures can mitigate the risks related to faults in network equipment, the 'backdoor' threat, and vendor administrative access, we recognise that national dependence cannot be mitigated through technical measures alone. That is why the Government determined that the risk posed to 5G and full fibre networks by high risk vendors should be reduced by excluding them from the core of the network and restricting them to 35% of the access network.

It is important to make clear that risk cannot be eliminated entirely. There will always be risk regardless of the specific framework or mitigations in place. Therefore the Government's intent is to manage the risk down to an acceptable level in all of the relevant networks, and using all of the different vendors. The new set of controls and the new regulatory framework proposed by the Government will minimise the risk of using a high risk vendor, such as Huawei, and reduce that risk to broadly the same point as using equipment from vendors not considered to be high risk.

The Government further recognises that as networks change and evolve, the security analysis and the subsequent mitigations need to change and evolve with them. In that regard, the security analysis that underpinned the Review, as with all security analysis, is subject to continual review.

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

The first role of government is to protect its citizens and its security interests. Telecommunications sits at the heart of the UK's critical national infrastructure and as such responsibility for the management of the security and resilience of the telecoms network is shared across government, Ofcom and industry.

It is the role of Government, through DCMS and the Cabinet Office, to ensure that we have the right frameworks in place to incentivise, and where necessary, require that appropriate steps are taken to ensure the confidentiality, integrity and availability of the telecoms network, and that Ofcom has the appropriate levers and powers to enforce this where necessary. Through the NCSC the Government ensures that industry has access to world class cyber security technical expertise and advice.

The Telecoms Supply Chain Review found that despite clear roles and responsibilities across Government, the regulator and industry, there can be tensions between operators' commercial priorities and security concerns, particularly when these impact on costs and investment decisions. Furthermore, the business models of vendors also do not always prioritise cyber security sufficiently. That is why, in response to the Review the Government is introducing a robust regulatory framework to safeguard telecoms security. This framework will raise the standard of security across the telecoms sector, principally by applying to telecoms operators and through them to the vendors that supply equipment to their networks. It will further ensure Ofcom has the necessary powers to enforce the new, higher standards and it will provide the Government with the national security powers required to effectively protect our telecoms critical national infrastructure.

But the Government's interests are not limited to the UK's network. The Ministry of Defence (MoD) deploys forces worldwide, and will be able to operate in theatres where there are all types of other networks available, including 5G. The MoD has worked with NCSC to understand what impact 5G will have on how we continue to deploy now and in the future in a safe, efficient, and effective way.

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?

Security has been at the forefront of the Government's decision-making on high risk vendors. The technical and security analysis from the NCSC is clear - it is both possible and desirable to exclude high risk vendors from the most sensitive functions and restrict them to less critical functions.

Telecoms networks have evolved in an organic way over the last 20 years. The introduction of 5G brings technical advantages in terms of capacity, speed and latency (i.e. quicker reaction times), which could support new services, but it does not break all of our current security principles and paradigms.

In legacy networks, sensitive functions were grouped together in a couple of locations that are called the 'core'. Amongst other things, the sensitive 'core' functions provide user services nationwide and process extensive confidential data. In 5G these functions may spread out more towards the edge of the network in order to reduce latency, for example, to several hundred data centres across the UK that can be sensibly managed or protected.

The key to the NCSC's security analysis therefore is that it is focused on understanding critical *functions* and providing appropriate security controls wherever those functions sit in the network - both now and in the future. The NCSC's guidance to industry sets out clearly what these critical safety functions are.[2]

If operators were to start pushing core functionality to the edge of the network under 5G, high risk vendors will be excluded from performing that functionality, irrespective of where in the network the operator is performing that critical function. This would apply, for instance, to Mobile Edge Compute (MEC) or virtualisation. On this basis, it is still possible and desirable to distinguish the security critical functions.

What credible alternatives are available to Huawei systems?

The leading telecoms equipment suppliers in the UK access market are Huawei, Ericsson and Nokia. These three companies can provide end-to-end network equipment and supply the main UK mobile operators. These three players also dominate the global telecoms equipment market, together with Samsung, Fujitsu, NEC, and ZTE who operate in fewer markets[3].

High risk vendors are already excluded, on a voluntary basis, from the sensitive network functions where there are a number of alternative suppliers. The lack of supplier diversification applies to the radio antenna and equipment in the access network, where the UK supply base is limited to Huawei, Nokia and Ericsson, and where the Government has said that Huawei's presence should be limited to 35%.

The lack of alternative vendors with the capacity to support the major UK mobile network operators represents a market failure. That is why the Government has established diversity in the market as one its priorities for the future of telecommunications, and are developing a targeted diversification strategy to address this market failure. One of the

---

[2] https://www.ncsc.gov.uk/guidance/ncsc-advice-on-the-use-of-equipment-from-high-risk-vendors-in-uk-telecoms-networks

[3] NCSC has assessed ZTE to be a high risk vendor.

key pillars of this will be to attract other scale players to the UK market. The Government has committed to working with our Five Eyes and other partners to develop new supply chain capacity in our critical national infrastructure in this Parliament as part of our diversification strategy, and that will include working to encourage alternative suppliers to the UK market.

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

The Government's decision on the use of equipment from high risk vendors in UK telecoms networks was the result of a comprehensive, evidence-based review, and is in direct response to the technical and security advice and recommendations provided by the National Cyber Security Centre. The decision was further informed by economic analysis conducted by KPMG as part of the Review which included analysis of the market dynamics underlying the supply chain arrangements for telecoms equipment.

The decision taken by the National Security Council was based first and foremost on the security advice of the NCSC that a model that would exclude high risk vendor equipment from the security critical functions of the network and installing a 35% cap on the access network was the optimal approach from a cyber security perspective that still enabled the utilisation of 5G connectivity within the UK. The economic analysis conducted as part of the Supply Chain Review pointed in the same direction. The relationship that the UK experiences with its telecoms providers and the insight provided by the Huawei Cyber Security Evaluation Centre and its Oversight Board, ensured that 5G connectivity could be brought to the UK without imposing an unmanageable risk to our national security interests.

These recommendations, and an explanation of how the NCSC reached them, can be found in Section 8 of the NCSC's summary of its security analysis.[4]

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

The Government has a shared understanding of the threat and the same overall objectives as our closest allies: increasing global telecoms security standards, reducing the presence of high risk vendors and supporting a greater diversity of suppliers.

The decision on the use of high risk vendors in UK telecoms networks is right for the UK's specific circumstances. The Government is committed to working with international partners to achieve our objectives on telecoms security. We engaged with our allies closely through the duration of the Review, and will continue to engage with them on this issue going forward.

The relationship between MoD and our international partners is particularly close, and we will continue to leverage our world-class MoD platforms and people to ensure that our important work with our allies, and the deterrence of malign activity by our adversaries, continues to provide strong national security for the UK and its allies.

How have the UK's allies, particularly those in Five Eyes, responded to this decision?

Our Five Eyes and other partner relationships are incredibly important. The Government has spoken to them all about our decision and will continue to work closely with them, including on the issue of telecoms security. The US and Australia have gone further in the controls they have chosen to impose on Huawei, and have taken the decision to ban

[4] https://www.ncsc.gov.uk/report/summary-of-ncsc-security-analysis-for-the-uk-telecoms-sector

Huawei from their telecoms networks. We will work closely with our allies to develop greater market diversification and to encourage effective vendors to spread their presence in the global market.

Every country has different security and economic circumstances and are making their own sovereign decisions. The Government has been clear that this decision is right for the UK's specific national circumstances and reflects (i) our current and future network configuration, (ii) our level of cyber security expertise and thorough and unparalleled understanding of the threat and risk (led by the NCSC), (iii) our existing regulatory arrangements and the robustness of our regulator, and (iv) the maturity of our relationship with industry. It is a sophisticated, risk-based approach that reflects our national circumstances. It will not be easily replicated in other countries.

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

The Telecoms Supply Chain Review was focused on the UK's telecoms critical national infrastructure supporting public electronic communications networks and services (within the meaning of the Communications Act 2003). It covered terrestrial infrastructure and those parts of the network most critical to the operation of 5G and full fibre.[5]

With respect to intelligence sharing, we have been clear that the decision does not affect our ability to share sensitive intelligence data over highly secure networks both within the UK and with our partners, including the Five Eyes. GCHQ have confirmed categorically that how we construct our 5G and full fibre public telecoms networks has nothing to do with how we share classified data. During his visit to the UK in January and following the announcement of the Government's decision on high risk vendors, US Secretary of State Mike Pompeo said on intelligence sharing that the Five Eyes relationship is strong and would remain, and that all the elements of the Five Eyes will work together to ensure the systems are sufficiently secure.[6] High risk vendors never have been and never will be in our most sensitive networks. The Government would never take a decision that threatens our national security, or that of our allies.

Additionally, our Global Operations and Security Control Centre (GOSCC) at MoD Corsham is equipped with sophisticated cyber defence capabilities in support of its role to defend our networks and provide worldwide assured communications for Defence.

We have enhanced our MoD cyber defence capabilities with over £40 million in developing a new Cyber Security Operations Capability (CSOC). The CSOC enhances our ability to secure Defence networks and systems against cyber threats and bring together our defensive cyber capability to enable us to continue to operate safely and securely.

The upcoming Integrated Security, Defence and Foreign Policy Review will reassess the nation's place in the world covering all aspects of international policy from defence to diplomacy and development. We have previously assessed Cyber as a Tier 1 threat to the UK, and defending the UK against cyber threats will remain a core aspect of our cyber capability.

---

[5] The full scope of the Telecoms Supply Chain Review can be found in its terms of reference at: https://www.gov.uk/government/publications/telecoms-supply-chain-review-terms-of-reference

[6] https://www.state.gov/secretary-michael-r-pompeo-and-british-foreign-secretary-dominic-raab-discussion-on-the-future-of-the-special-relationship/

The UK will remain able to operate closely with our allies and we are leading the way in collaborative cyber operations - both offensive and defensive in nature - by being a leading cyber-voice at NATO; and the first NATO country to offer its Offensive Cyber capabilities in support of NATO allied operations and missions.

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

The Government has been clear that we want to get to a position where we do not have to use high risk vendors in our telecoms networks at all, but to do that, we have to work with our Five Eyes and other partners to develop new supply chain capacity in our critical national infrastructure. We have set out that we will do that in this Parliament.

The lack of diversity of supply is a global problem. That is why the Government has committed to developing a diversification strategy. We recognise however that the UK represents a small part of the global telecoms equipment market. It will therefore be necessary to work with like-minded international partners as we develop this strategy to ensure we achieve real, sustainable and long-term change.

To effectively tackle this problem, the Government will need to introduce measures both on the demand and on the supply side. This will require coordinated international action by a critical mass of markets, using a range of policy, regulatory and financial levers. Working with our international partners, the UK will be looking to pursue two strategies simultaneously in attracting existing scale players to key European markets and disrupting the market via lowering barriers to entry to new players and supporting their growth.

National Cyber Security Centre
a part of GCHQ

DEFENCE SELECT COMMITTEE INQUIRY
'THE SECURITY OF 5G'

Annex - Technical Evidence from the National Cyber Security Centre

I. Introduction and summary

1. In support of the evidence from the Department of Digital, Culture, Media and Sport (DCMS) and the Ministry of Defence (MoD), this memorandum is intended to clarify technical aspects related to the 5G decision. The role of the National Cyber Security Centre (NCSC) throughout has been to provide objective, expert technical advice on cyber security risk around telecommunications, or telecoms, networks as mobile networks migrate to 5G. Therefore, this memorandum focuses on the technical issues around 5G and high risk vendors (HRV) and does not consider wider policy or political issues, other than insofar as they relate to cyber security risk. So, this paper does not deal with the UK's overall approach to relations with China, for example. Cyber security risk is one aspect of a complex policy debate; it is for policymakers and Parliamentarians, not the NCSC, to evaluate the issue in the round.

2. It should be noted that for cyber security purposes, successive Governments have assumed that any company based in China could be fully compelled to act at the direction of the Chinese state. Everything in the NCSC's advice, summarised in this memorandum, works on this assumption. It is one of two key assumptions underpinning the NCSC's analysis. The other is that any piece of equipment, anywhere, in any network, can fail, or be compromised by a hostile attacker. The essence of both assumptions is that what matters for security is how the network is built and operated in order to be able to limit and contain harm, whether caused by accidental failure or malicious attack, with or without control of a vendor company.

3. It should also be noted that the NCSC's advice to Government on high risk vendors is part of a much wider suite of advice on the security of telecoms infrastructure for the next generation. Telecoms infrastructure has, historically and at a global level, been proven to be insufficiently secure. Addressing these endemic security flaws in telecoms networks is the most fundamental challenge for the security of all networks, but particularly 5G. From the perspective of assessing the technical security of 5G networks, the national identity of vendor companies is a secondary issue, albeit an important one to which the UK has given very considerable attention. But countries which exclude Chinese vendors completely will still have first order telecoms security issues to address. So too will countries that allowed limited involvement. That is in part because of the intrinsic risk involved in these complex networks. It is also in part because of the nature of the modern supply chain, where all major suppliers have extensive input from non-Western countries, including China, whether the company is Western or not.

4. It is in this context – the need for wide-ranging reforms to the security of telecoms which the UK Government is recommending – that the high-profile technical issue of whether there are such things as core and non-core functions in 5G networks should be seen. As paragraphs 15 to 35 of this memorandum make clear in some detail, telecoms networks are highly complex, with many different constituent parts,

requiring different, specific approaches to security within and between them. As paragraphs 36 to 46 go on to make clear, the claim that the distinction between such functions collapses in 5G networks is not just simplistic but wrong, and rejected by the telecoms industry that is responsible for building the networks. It is also an assertion disproved by the extensive and technically-detailed standards for 5G networks agreed by the international industry standards bodies.

5. From a security perspective, the acceptance of the contention that there is no distinction between core and non-core functions in the telecoms networks of the future is, in addition to being wrong, dangerously wrong. This is because it means, by extension, that 5G networks are a single risk entity, and different security practices cannot be applied to different parts of the network. If that were true, it would mean 5G networks could not be defended because any penetration of a network, in which all equipment is vulnerable, by any attacker, is an existential threat to the whole network. In such an eventuality, 5G networks would be too dangerous to build. In reality, the security of 5G means understanding a hugely complex and detailed mix of hardware, software, and operations. Failing to understand this complexity will make for poorer standards of security in 5G. It remains fundamental to the long-term security of telecoms networks now and in the future to be able to segregate any telecoms network to account for different risks and impacts that various equipment and functions attract.

6. There are wider policy issues around the role of high risk vendors in 5G for policy makers and Parliamentarians to consider. However, it is imperative for the technical security of 5G networks that the technical canard – often asserted but, as this memorandum shows, usually without any credible supporting evidence – that there is no distinction between core and non-core functions in 5G, is firmly rejected. If this 5G fallacy is accepted as a basis for regulating the security of telecoms in the UK's 5G networks, those networks cannot be secured because the fundamental assumption underpinning the security regime will be technically wrong and completely at odds with the way telecoms networks actually function in real life.

7. Finally, the NCSC fully endorse the point made in the DCMS and MoD memorandum about the structural problem of diversity in the market for supply of Radio Access Network equipment; the area of the network on which the Huawei debate focuses. The NCSC strongly supports the Government's agenda to broaden and diversify provision in this, and other, technical infrastructure supply chains.

II. Background: telecommunications networks and their security

8. Telecoms networks are highly sophisticated, complex systems comprised of a wide variety of hardware, software and people each performing inter-related and complex tasks. As with any complex system, it is not possible to completely remove risk. Running a complex, national-scale telecoms network is a continuous balance of different risks. While operators are ultimately responsible for the security of their networks, Government sets the parameters within which operators manage risk through regulation, setting this regulation based on its national security risk appetite.

9. As telecoms networks have developed, they have become increasingly based on data (rather than voice services) and begun to converge with internet services. While modern telecoms networks continue to be exposed to traditional threats and risks, for example random equipment failure, physical damage to cables or supply chain interdiction, today they are also exposed to a range of internet-like attacks, including cyber attack from both highly sophisticated and less sophisticated actors. Despite the increasing reliance on, and development of these networks, the security

management of networks has remained broadly the same for the last few decades. This has led to shortcomings in the security of networks we rely on today, which must be remediated if we are to avoid further attacks on our networks of the types we have already seen.

10. For example, HM Government, on the basis of NCSC evidence, publicly attributed a successful attack on a UK telecoms network to the Russian state, a highly sophisticated cyber actor[7]. However, attacks of this nature do not require specialist knowledge of a particular vendor's equipment.

11. On top of the suboptimal security in the networks themselves, the supply market for important network equipment has also, over the last decade, consolidated to the point that, in and of itself, it has become a point of concern.

12. Acting on these concerns, DCMS undertook a range of steps to understand and reduce the cyber security risk within the telecoms sector, including the Telecoms Supply Chain Review. This will culminate in the introduction of a new, robust telecoms security framework, with new Telecoms Security Requirements (TSRs) at its core, alongside additional controls for high risk vendors and an intent to diversify the market in the future.

13. The NCSC has provided expert technical advice to DCMS throughout this process, completing the security analysis for DCMS as part of the Supply Chain Review, drafting the TSRs in support of the new framework and publishing detailed advice on mitigating the risk from high risk vendors. This included a summary security analysis explaining the security rationale, the framework for high risk vendors describing the permitted uses in the networks and a blog explaining – in non-technical language – the underlying security risks and mitigations in 5G networks. This was published[8] when the National Security Council (NSC) decision on high risk vendors was announced. The NCSC is actively working with DCMS today to define appropriate measures, both nationally and internationally, to support the diversification of the telecoms equipment market.

14. As well as advising government, we provide detailed security advice and guidance to the UK's operators and convene a cross-industry security group for the larger operators, called the Network Security Information Exchange (NSIE). Members of the NSIE share security knowledge and details of attacks in a non-commercial manner to ensure that the impact of attacks are minimised across operators for the benefit of the country. The NSIE also has subgroups covering topics including, but not limited to, supply chain risk management, Domain Name System (DNS) security and signalling security.

III. Overview of NCSC's technical security analysis

15. In the NCSC, we have undertaken a detailed, expert-led analysis of the risks to telecoms infrastructure, including 5G networks. To our knowledge, no analysis to a similar level of detail has been performed anywhere else in the world, and certainly none has been published to the same level of detail for scrutiny and debate.

16. Given that, as our analysis shows, modern telecoms networks (whether fixed or mobile) are highly connected, complex systems, they are exposed to a range of

[7] Russian state-sponsored cyber actors targeting network infrastructure devices, NCSC advisory, April 2018, https://www.ncsc.gov.uk/news/russian-state-sponsored-cyber-actors-targeting-network-infrastructure-devices

[8] 5G round-up, NCSC, January 2020, https://www.ncsc.gov.uk/information/5g-round-up

risks. While it is not possible to completely remove risk – cyber security or otherwise – from any complex system, we are confident that the UK's approach will result in UK networks having world-leading security.

17. This dynamic is about every aspect of a network, and the choice of vendor is only one consideration. However, to illustrate the point, it should be obvious that no equipment can ever be perfect and without defects or vulnerabilities. Telecoms equipment is made by people and even completely honest people make mistakes. No vendor can ever guarantee the honesty of every single one of their staff, plus the staff of their suppliers. All vendors in this sector are highly internationalised, with large global workforces. Most have many thousands of employees in Europe, India, China and the US and all telecoms vendors have a Chinese component in their supply chain. As Matt Beale, then Vodafone's Director of Technology and Strategy, told the Prague 5G conference in May 2019, "There is one supply chain for telecommunications, and it all runs through China". Given this reality, it is obvious that the national identity of vendors is an important, but ultimately secondary, issue in the security of our national telecoms networks.

18. The result of this must be an assumption that any piece of telecoms equipment could contain defects, vulnerabilities and other issues that could cause operational risks. Mitigating these risks needs to be considered when designing networks. The security of 5G networks cannot be based on vendor perfection, or vendors creating zero risk, as this assumption is fundamentally unachievable. Ultimately, taking a binary view of risk, where vendors are either 'good' or 'bad', is a flawed approach to managing risk which would leave our networks more vulnerable. There is no binary division between 'trusted' and 'untrusted' vendors. National security risk management could not possibly be based on such an assumption given the reality of modern telecoms networks.

19. There are many ways of considering the different risks that exist around a telecoms network and mitigations that can be applied to reduce, but often not remove, those risks. The NCSC produced a comprehensive assessment of the risks and mitigations as part of the DCMS Supply Chain Review. Here, we will look only at some of the more obvious and impactful risks, and then only at high level.

Cyber attack:

20. The most obvious class of risk to a telecoms network is a cyber attack from an external entity. If successful, such an attack could give the attacker a capability to perform espionage or to disrupt the operation of the network. As a part of GCHQ, the NCSC is one of the preeminent agencies globally in its understanding of the cyber capabilities and campaigns of both state actors and organised cyber criminals.

21. As mentioned in paragraph 10, in 2018, the UK Government, informed by NCSC evidence, led a coalition of like-minded nations in publicly attributing attacks against global telecoms networks, including in the UK, by the Russian state. We also see a range of state and non-state actors targeting global telecoms systems.

22. In these cases, and others which are not in the public domain, the attackers were able to penetrate their target networks, because of exploitable vulnerabilities caused by poor network design or operational practice in the operators affected. These attacks did not need to take advantage of pre-placed vulnerabilities in the equipment, or human agents working within the operators. They are purely a result of poor network security. That is not to say that human agents and pre-placed vulnerabilities

are not useful to an attacker, but they are neither necessary nor the lowest risk way of attacking a network.

Systemic equipment failure:

23. The next class of risk are faults that cause systemic equipment failure. These are not caused by an external attack, but still cause widespread network disruption. These failures would normally be due to an error in the operational management of a network, a defect in one of the many components used within the network, or an unplanned external event (flood, fire etc.). This class of risk is the one that tends to lead to the most disruption of service to network users.

24. Naturally, the impact of systemic equipment failures is proportional to the scale of use of the equipment. Equipment diversity is a key factor that helps to mitigate the risk due to systemic equipment failures – if equipment from one vendor fails, the impact will necessarily be reduced if there is a greater variety of unaffected equipment from other vendors. Having very low diversity in the market, such as one or two vendors, will significantly increase the risk of nationwide, systemic failure of our telecoms networks.

25. Real world examples of such network outages include:
    a. 2014 – EE was affected for several hours due to damage to a fibre cable,
    b. 2016 – Three's service fails due to a lack of resilience[9],
    c. 2016 – Telenor Norway services were affected due to ongoing security testing of their external signalling network,
    d. 2018 – O2 services were affected for several hours due to a software flaw[10].

'Backdoor' threat:

26. Another class of risk is brought about through the procurement of equipment, and the choice of equipment supplier. This is the class of risk that is mainly talked about with respect to Huawei, and the insertion of 'backdoors', or malicious functionality. There are several ways in which such functionality can be inserted into a product:

    a. The company itself is malicious and acting under the control of a state hostile to the UK. The company is compelled to covertly build in malicious functionality to its products that can be exploited once the equipment is installed. Whilst we have not seen any specific evidence in respect of the UK, given its close relationship with the Chinese state, this scenario is our standing assumption since Huawei entered the UK market in 2003.

    b. The company itself is not malicious or operating under direction from an external party, but people working within in it are. These individuals could be building covert malicious functionality into the company's products and not be caught by the company's audit processes. This is our standing assumption for all vendors, and we have been involved in cases where this type of activity has been discovered.

    c. A malicious actor performs a cyber attack against a company's development or corporate network and uses that access to add covert malign functionality to the company's products prior to being shipped to UK customers. There is one public example of this happening, against Juniper Networks (a US network

[9] Three fined £1.9m for emergency call service failure, Ofcom, June 2017, https://www.ofcom.org.uk/about-ofcom/latest/media/media-releases/2017/three-fined-emergency-call-service-failure

[10] O2 network outage, Ofcom, November 2019, https://www.ofcom.org.uk/__data/assets/pdf_file/0014/175010/o2-network-outage-cceb.pdf

infrastructure company), where threat actors added covert functionality to the product, that went undiscovered for over a year (during which time all customers were vulnerable to exploitation by those actors)[11]. Again, the possibility of this happening is our standing assumption for all vendors.

27. Therefore, while there are obviously differences between vendors that could be under the control of a hostile state and those that are not, the threat model in the design of a critical network must acknowledge the risk of malicious functionality in all equipment and software.

Managed services and third-party administration:

28. A significant class of risk is around the use by telecoms operators of managed services and third-party administrators. Every telecoms network is run by a combination of the operator itself, and several third parties. In some cases, these third parties run the entire network on behalf of the operator, but in most UK cases they provide specific services to an operator as necessary. Similar to how we look at equipment vendors, the risk here can be split depending on whether the managed service provider or third-party administrator is itself hostile or not.

29. The Government, using NCSC information, was part of an international coalition including our crucial Five Eyes partners in the United States and Australia in 2019 to publicly attribute to the Chinese state a global cyber campaign that compromised many managed service providers and vendors – including some relevant to the telecoms sector in the UK[12]. In this campaign, actors associated with the Chinese Ministry of State Security, known in industry as APT10[13], had compromised several companies whose onward contracts and connections gave the attackers control over their customer's networks. Again, this was a broad attack against global networks that were built and operated differently, not against any one managed service provider or equipment vendor.

National dependence:

30. Finally, there is the risk of national dependence. Given the ongoing reliance of telecoms operators on the involvement of their equipment vendors, it is possible for a network and, in extremis, a country to become reliant on the ongoing relationship with a particular vendor. This would be a bad outcome in that it provides no resilience, regardless of the vendor involved, but the impact would be particularly acute with a high risk vendor that may be susceptible to a direction from a hostile state to do something that would not otherwise be in their commercial interest. Limiting the presence of such vendors, and ensuring diversity of supply more generally, ensures that individual networks and the country are resilient to both the managed (gradual run down) and unmanaged (company failure or malicious removal of service) exit of a vendor from the UK market. A range of suppliers is important.

31. For all these reasons, the Telecoms Supply Chain Review recommended the most sweeping changes to the regulation of UK telecoms operators ever seen. At the core of the package to come before Parliament is the introduction of the TSRs. These TSRs are a detailed set of requirements and tests designed to significantly improve the security of UK telecoms networks and the vendors that supply them. The full documentation can be provided to the committee privately, but the TSRs seek to address the main risks detailed above:

---

[11] Juniper Networks 2015-12 Out of Cycle Security Bulletin, https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10713

[12] APT10 continuing to target UK organisations, NCSC, December 2018 https://www.ncsc.gov.uk/news/apt10-continuing-target-uk-organisations

[13] Operation Cloud Hopper, PwC, April 2017, https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-report-final-v4.pdf

- Direct cyber attacks against a network,
- Systemic failures,
- Signalling attacks,
- Equipment vulnerabilities, (whether deliberate or accidental),
- Attacks from third party administrators and managed service providers,
- National dependence,
- Plus, a range of other risks that were identified through NCSC analysis.

32. Implementing these requirements is necessary within all telecoms networks, regardless of the vendors that individual operators choose, and must be seen as a baseline for the future security of the UK's telecoms infrastructure. Extra mitigations must be taken for high risk vendors, which will be discussed later in this evidence.

33. It should be noted that the NCSC's security analysis is subject to constant review. If new attack vectors are discovered as attackers' capabilities evolve, or new vulnerabilities are uncovered, then the resulting mitigations would need to change. This is normal practice and is not specific to 5G networks.

34. It is also important to note that our regulatory regime for 5G security can adapt over time to the different services that use 5G as an enabler. What matters about 5G is what it is ultimately used for. Here, as always, it is important to separate out hype and fearmongering from reality. For example, one probable use-case for 5G is the large-scale uptake of autonomous vehicles. Whilst 5G will enable these services, 5G security regulation cannot plausibly be the final word on safety for these vehicles on the road. No transport safety regulator will license a system whereby the safety of humans in high speed transit depends entirely on a continuous and uninterrupted mobile network connection. Realistic, use-specific, regulations will develop over time.

35. For all the reasons set out in this section, it is the overall implementation of the TSRs, coupled with secondary issue of high risk vendors, which matters most for the security of 5G. Without the TSR framework the NCSC cannot be confident about the security of UK 5G networks, irrespective of Parliament's final conclusion on high risk vendors, the subject on which the rest of this memorandum focuses.

IV. The UK's mitigation strategy for High Risk Vendors

36. Based on our security risk analysis of telecoms systems, the NCSC proposed a comprehensive, robust and effective strategy to mitigate these risks. General cyber risk would be mitigated through operator adoption of the TSRs, with extra mitigations adopted for specific high risk vendor risks.

37. Specifically, the NCSC advised that high risk vendors must be:

    a. Excluded from security critical 'core' functions of the UK's telecoms networks; and
    b. Excluded from sensitive geographic locations; and
    c. Limited to a minority presence of no more than 35 per cent[14] in the edge of the network, known as the access network, which connect devices and equipment to the services they consume; and
    d. Excluded from all safety related and safety critical networks in wider Critical National Infrastructure; and

[14] A 35% cap is applied across a number of different parameters, as described in detail in: https://www.ncsc.gov.uk/information/hrv-faq.

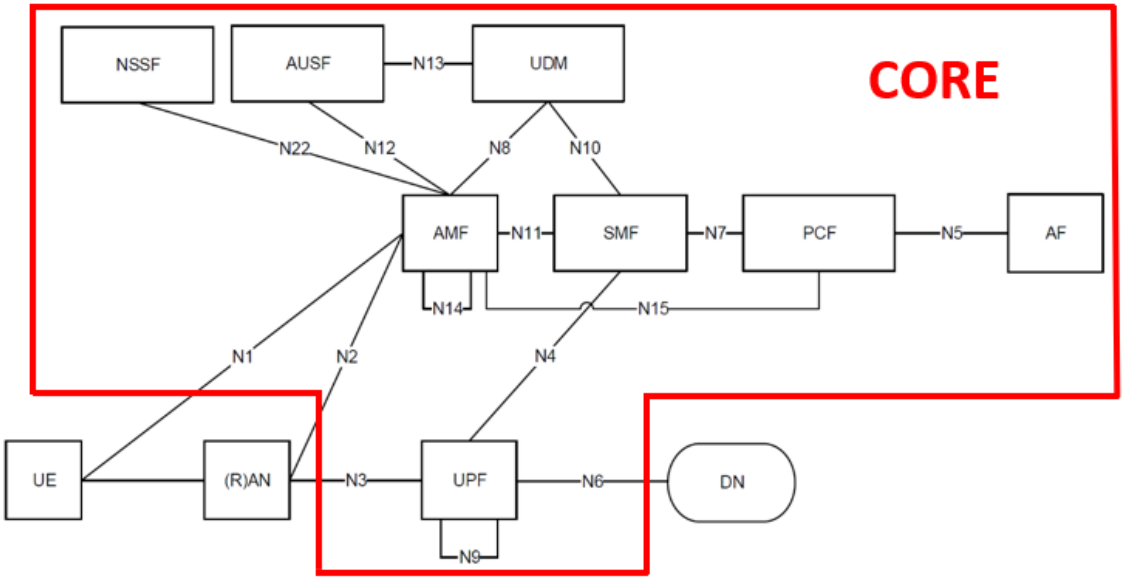
e. Only permitted into the UK market in accordance with a vendor-specific mitigation strategy.

38. The primary technical argument invoked against this mitigation strategy has been that in 5G networks it is no longer feasible to distinguish between core and edge. However, the claim that there is no distinction between core and edge in a 5G network is the great fallacy of the international 5G debate. It is a claim without any basis in fact and without any technical credibility in the global telecoms industry. The core and edge are distinct today and will also be distinct in fully mature 5G networks.

39. It remains fundamental to the long term security of telecoms networks, now and in the future, to be able to segregate any telecoms network to account for different risks and impact that various equipment and functions attract. As telecoms networks have evolved over the last 20 years, they have maintained a consistent underlying structure and this structure will likely continue to be used going forward. Despite some claims to the contrary, 5G networks are structurally consistent with previous generations of mobile networks, and the security analyses and tools remain applicable. 5G is an evolution of existing technologies coupled with some technologies from the wider ICT sector that are previously unused in the telecoms sector. It is not a fundamentally new scientific discipline.

40. Telecoms networks are generally defined by internationally adopted and recognised industry standards which cover in intricate detail the operation and function of the various network components. For 5G, the overall architecture for the various network configurations is defined by 3GPP in TS 23.501[15].

    Fig 4.2.3-2 of this standard, reproduced below is instructive:



41. The ‘UE’ element is representative of the mobile handsets and other terminals that use the system. The element marked ‘(R)AN’ is representative of the Radio Access Network and is the only part of the system that we are advising high risk vendors be permitted to supply into and then only to a hard market share cap (defined by coverage, expected data usage and share of the ITU K.100 power classes). The rest

[15] 3GPP TS 23.501, version 15.9.0, http://www.3gpp.org/ftp//Specs/archive/23_series/23.501/23501-f90.zip.

of the elements on this diagram consist of the sensitive and core functions from where our advice is that high risk vendors should be excluded[16].

42. Of course, such a high-level architecture diagram hides significant complexity, but it does clearly demonstrate that there are well defined interfaces between the part of the network where a high risk vendor may supply equipment and the rest. Given this is based on the industry standard for 5G, this view is shared by industry (both operators and suppliers), and governments across the globe. To give some idea of the scale of the standardisation process, it is instructive to look at the membership of the '3rd Generation Partnership Program' (3GPP) which brings together members of regional standards organisations to define the single, global standards. While not every member organisation will participate in, provide expertise or intellectual property to or implement every part of the standard set, there are currently 690 different Individual Members in 3GPP. 113 of these are via the China Communication Standards Association (CCSA) and are Chinese organisations. 440 are affiliated through the European Telecoms Standards Institute (ETSI) although not all are European and 54 are affiliated through the Alliance for Telecoms Industry Solutions (ATIS) and are mainly US and Canadian. 3GPP finished the first 5G standard in June 2018, a success that was hailed by the world's telecoms companies[17].

43. The TS 23.501 paper from which the architectural map is reprinted, runs to over 200 pages, and is just one of 884 specifications that cover all aspects of the 5G standard[18]. This body of work is the result of this international expert collaboration between industry and Government over many years. Its introductory section on definitions defines a "5G system" as a "3GPP system consisting of 5G Access Network (AN), 5G Core Network and UE" (UE is explained in paragraph 41 above). The term 'core' is used so often in the document that it is abbreviated simply to '5GC' throughout. Put simply, if it were the case that there was no distinction between core and non-core functions in 5G, these standards documents would look very different indeed. In reality, the global telecoms industry does not debate whether or not there is a 'core' and 'non-core' in 5G. Instead it analyses carefully the component parts of each. The NCSC concurs with this internationally accepted approach.

44. To be clear, to secure a 5G network you must secure its most sensitive functions. If compromise of a single edge device (for example in the (R)AN element above) leads inevitably to the compromise of a sensitive function (for example, the Authentication Server Function (AUSF)) and therefore the entire network, you cannot secure the most sensitive functions and, consequently, you cannot secure a 5G network. If it were possible that core and edge were required to collapse together in a 5G network such that a vulnerability in one part of a network was an unmitigable risk to the whole network, then the NCSC's advice to the Government would be not to allow the building of any 5G networks in the UK. If this were true, the risks of allowing these networks to be used would be too great and the completely unmanageable.

---

[16] The High Risk Vendor Framework, published on the day the NSC decision was made (28 January 2020), lists in section 11.a.2 the functions specific to a 5G network that an high risk vendor may not be involved in as : 5G Core database functions, 5G core-related services including but not limited to Authentication Server Function (AUSF), Access and Mobility Management Function (AMF), Unstructured Data Storage Function (UDSF), Network Exposure Function (NEF), Intermediate NEF (I-NEF), Network Repository Function (NRF), Network Slice Selection Function (NSSF), Policy Control Function (PCF), Session Management Function (SMF), Unified Data Management (UDM), Unified Data Repository (UDR), User Plane Function (UPF), UE radio Capability Management Function (UCMF), Application Function (AF), 5G-Equipment Identity Register (5G-EIR), Network Data Analytics Function (NWDAF), Charging Function (CHF), Service Communication Proxy (SCP), Security Edge Protection Proxy (SEPP), Non-3GPP InterWorking Function (N3IWF), Trusted Non-3GPP Gateway Function (TNGF), Wireline Access Gateway Function (W-AGF), and future 5G core functions as specified by 3GPP TS 23.501.

[17] Rel-15 success spans 3GPP groups, https://www.3gpp.org/news-events/1965-rel-15_news

[18] 5G specifications are listed here: https://www.3gpp.org/dynareport/SpecList.htm?release=Rel-15&tech=4&ts=1&tr=0. These specifications define the totality of what a 5G network can do, including support for 4G. There are around 100 specifications that define '5G' in its purest sense.

45. Network segregation is so fundamental to the security of networks that the TSRs specify that both physical and logical segregation is maintained between sensitive core functions and the more-vulnerable, exposed edge. For example, 5G radio networks need many smaller basestations as well as the traditional large cells used in previous generations of mobile networks. This is a function of physics. These small cells will be deployed in areas of high traffic with easy access to power and network connectivity, such as bus shelters and lampposts and other places that are not secure from physical interference by adversaries. If the network design means that those physically insecure network elements need to run sensitive functions that can affect the entire network, the design is fundamentally inappropriate for a critical national network. If this were the case, *reductio ad absurdum*, the security of the entire UK 5G critical infrastructure is contingent on no-one climbing up a lamppost to interfere with a small cell.

46. Instead, the UK's approach has been to look at the different parts of the network and their different security requirements, resulting in the detailed measures summarised above in paragraph 37. As well as complete exclusion from the core functions of a 5G network, high risk vendors are limited to a 35 per cent share of the Radio Access Network. The RAN is a high cost, low margin, hardware heavy part of the network where the problem of a lack of market diversity (see section VI of this memorandum) is at its most acute. The 35 per cent figure, as we have made clear, is a judgment, not a scientific calculation. It ensures that the UK will not become nationally dependent on any vendor, especially a high risk vendor, while retaining competition in the market and allowing operators to continue to use two RAN vendors. There are provisions in the detailed guidance to make sure the system cannot be gamed, for example by using a high risk vendor's basestations in all the cities and a non-high risk vendor products in the countryside.

V. Commentary on the NCSC analysis

47. There has been commentary in Parliament, the media and elsewhere claiming that the UK's technical view on 5G security is a minority one. But, as the preceding section on industry standards implies, the UK's technical assessment, which is the most detailed security assessment of 5G published by any country in the world, is firmly in the global mainstream. This section analyses some of the commentary on the global debate on 5G security, and on the UK's published approach to high risk vendors in particular.

48. The relatively small number of governments which have excluded Huawei and other Chinese vendors completely from their networks have not published any technical detail in support of their decision. There are those who assert that the UK is wrong to differentiate core and non-core functions, but the UK Government is unaware of any published or unpublished technical rebuttals of our assessment by other governments. The UK Government, via the NCSC, has shared and discussed its analysis with a wide range of cyber security partners and will continue to do so.

49. Different countries are at different stages of considering their approach to the regulation of 5G security and the position of high risk vendors. Within the Five Eyes, it is a matter of public record that the Governments of the United States and Australia have taken a different approach to the UK on high risk vendors. But there is a good degree of commonality between the approach taken by the UK and those taken by cyber security agencies in partner countries to the technical issues.

50. The Government of Canada is undertaking a review that has yet to conclude: giving evidence to the Canadian Parliament on its technical aspects, the head of the Canadian Cyber Security Centre set out assumptions for the work that are based on the same industry consensus on how telecoms work that the UK uses. He said: "the approach for 5G is under review right now in terms of the approach for Canada. I'm very confident of the relationship we've built with Canada's telecoms providers and the work we've done to increase the cybersecurity elements regardless of the network. The collaboration we have in terms of how we respond to incidents is something we'll need to continue, no matter what. We need to continue to build multiple layers of security, regardless of where the technology comes from. In my job, I actually trust nothing. I assume that there are vulnerabilities in every single piece of product we have, so how can we layer more and more protections on?"[19]

51. In France, speaking after the UK Government's policy announcement earlier this year, the head of ANSSI, the French equivalent of the NCSC, commented: "[the UK] are on the same risk analysis as us … in their decision, the equipment manufacturers at risk are excluded from the heart of the 5G network and they will only have 35% of the deployment of the antennas. It is anything but a blank check [sic] to do anything"[20]. His German counterpart has described the UK's approach as "reasonable" and has set out a similar risk analysis for Germany[21], as indeed the EU has for the 27 member states of the EU as a whole[22].

52. The position in New Zealand is often mischaracterised: there, the GCHQ equivalent, the Government Communications Security Bureau, is a statutory regulator which can block applications for contracts with New Zealand's operators on national security grounds following an analysis of the specifics. It has dealt with one 5G case so far, when Huawei bid for a contract with Spark, the country's leading telecoms operator. After initially turning down a bid from Huawei on national security grounds, a modified version of the bid was allowed to proceed. Ultimately, Huawei did not win the contract.[23]

53. The above is not to suggest that these countries support, or do not support, the UK's decision. Partner countries and partner agencies are clear these are sovereign decisions for sovereign countries. It is simply to dispel the fundamentally erroneous notion that the UK is alone among allied Governments in its technical analysis about the way in which 5G security works. As we have already seen, the global telecoms industry works on the basis that networks are complex and varied and need nuanced, sophisticated approaches to network architecture and maintenance. Similarly, the analysis of partner agencies, whatever the decision of the national government on high risk vendors, is, much more often than not, based on common technical understanding of this complexity. It is for that reason that globally respected

---

[19] Canadian House of Commons Standing Committee on Public Safety and National Security, Evidence Session, January 2019, https://www.ourcommons.ca/DocumentViewer/en/42-1/secu/meeting-146/evidence

[20] 5G en France: Huawei sera-t-il de l'aventure? La mise au point de l'Anssi, Guillaume Poupard, Le Parisien interview, http://www.leparisien.fr/high-tech/5g-en-france-huawei-sera-t-il-de-l-aventure-la-mise-au-point-de-l-anssi-30-01-2020-8248623.php

[21] German cyber security chief backs 5G 'no spy' deal over Huawei, Arne Schoenbohm, FT interview, https://www.ft.com/content/5a0fe826-3b34-11e9-b856-5404d3811663.

[22] EU Toolbox for 5G Security, https://ec.europa.eu/digital-single-market/en/news/eu-toolbox-5g-security

[23] Spark New Zealand keeps Huawei on preferred suppliers list, but leads 5G rollout with Nokia, Reuters, https://www.reuters.com/article/spark-nz-huawei-tech/update-2-spark-new-zealand-keeps-huawei-on-preferred-suppliers-list-but-leads-5g-rollout-with-nokia-idUSL5N27X0CU

bodies like the Royal United Services Institute (RUSI) have commented that “from a purely technical perspective, this [the NSC decision] was a practical and realistic decision that adheres to the principles of cyber risk management”.[24]

54. Other influential parliamentary oversight bodies who have also requested evidence on this topic, such as the Intelligence and Security Committee, have commented that “the 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.”[25]. Similarly, Norman Lamb, former chair of the Science and Tech committee in the last Parliament (on behalf of the whole Committee) stated that “we have found no evidence from our work to suggest that the complete exclusion of Huawei from the UK’s telecoms networks would, from a technical point of view, constitute a proportionate response to the potential security threat posed by foreign suppliers…Supply chains for telecommunications networks have become global and complex. Many vendors use equipment that has been manufactured in China, so a ban on Huawei equipment would not remove potential Chinese influence from the supply chain…We heard unanimously and clearly that a distinction between the ‘core’ and ‘non-core’ parts of a 5G network will still exist… Although it is no guarantee of future security, the operators also noted that there has not yet been any evidence of an increased security risk from the use of Huawei equipment… Overall, my Committee concludes that – subject to: restrictions on access to highly sensitive elements of the relevant networks; continued close scrutiny; and satisfactory improvements in Huawei’s cyber security in response to the HCSEC Oversight Board – there are no technical grounds for excluding Huawei entirely from the UKs 5G or other telecommunications networks.”[26]

55. Furthermore, leading computer security professionals such as Bruce Schneier, an American cryptographer, computer security professional, privacy specialist and writer and fellow at the Berkman Center for Internet & Society at Harvard Law School, has publicly said “Chinese, Iranians, North Koreans, and Russians have been breaking into U.S. networks for years without having any control over the hardware, the software, or the companies that produce the devices. (And the U.S. National Security Agency, or NSA, has been breaking into foreign networks for years without having to coerce companies into deliberately adding backdoors.) Nothing in 5G prevents these activities from continuing, even increasing, in the future.”[27]

56. The NCSC has published a more detailed technical body of evidence than any other country because we welcome scrutiny and technical debate. But despite the extensive controversy around 5G and high risk vendors, we are aware of only two published articles to question the UK's technical view of 5G security risk. One is a paper by the Henry Jackson Society titled “Defending Our Data: Huawei, 5G, and the Five Eyes”[28] (16 May 2019); the other an article written for the Australian Strategic

---

[24] Executive summary, RUSI 5G Cyber Security: A risk-management approach, February 2020 https://rusi.org/sites/default/files/20200602_5g_cyber_security_final_web_copy.pdf

[25] ISC statement on 5G suppliers, July 2019, http://isc.independent.gov.uk/files/20190719_ISC_Statement_5GSuppliers_Web.pdf?attredirects=0

[26] Letter from Norman Lamb to the DCMS SoS, dated 10 July 2019, https://www.parliament.uk/documents/commons-committees/science-technology/Correspondence/190710-Chair-to-Jeremy-Wright-re-Huawei.pdf

[27] 5G Security, Schneier on Security blog, January 2020, https://www.schneier.com/blog/archives/2020/01/china_isnt_the_.html

[28] Defending Our Data: Huawei, 5G, and the Five Eyes, Henry Jackson Society, May 2019, https://henryjacksonsociety.org/wp-content/uploads/2019/05/HJS-Huawei-Report-A1.pdf

Policy Institute (ASPI) by Simeon Gilding[29] (29 January 2020), previously of the Australian Signals Directorate.

57. The Henry Jackson Society (HJS) paper makes arguments more broadly than the technical analysis, well outside the remit of the NCSC and the scope of this memorandum. For the purposes of this evidence, we limit ourselves to commenting on the technical and cyber security content (Chapter 4, *Risks Associated with Huawei in the UK's Digital Infrastructure,* and Appendix 1 *Technical Description of Antenna Vulnerabilities*).

58. Although, as the report graciously notes, the NCSC met with the authors, we regrettably cannot find common ground with the account in these sections of how a 5G network operates, and therefore with any of the subsequent analysis. Here are a few of numerous examples.

    a. The paper states that "the "core" concept is becoming less relevant as 5G technology matures", without providing any further detail to support this statement, or on the risk. As previously stated, the 'core' becoming less relevant is a fallacy that goes against the internationally standardised technical definition of 5G. It repeatedly quotes others, mainly in the United States and Australia, asserting that the distinction between core and edge blurs in 5G. But these quotes often contain no supporting technical evidence, and where they claim to, the claims are not subjected to critical scrutiny in the report.

    b. The paper states that "antennas" could be somehow misused to disrupt communications. The threat that a radio transmitter, such as a 5G basestation, could interfere with other radio communications is theoretically true, but it was also true in 4G networks and the more general principle is true of all radio-frequency (RF)-based communications systems. There are also easy and inexpensive means to locally disrupt or jam radio communications and these do not require any vendor cooperation.

    c. The paper states that "Trojans" could provide "network control" and that there is a "high risk" that these Trojans would not be found by Huawei Cyber Security Evaluation Centre (HCSEC)[30]. This section appears to assume that HCSEC only performs external testing and has the misconception that HCSEC employs some form of "anti-virus" software. In fact, HCSEC has full access into all functionality within Huawei equipment, regardless of whether that functionality is enabled or disabled.

    d. The paper states that Huawei would gain access to UK data. However, there is no necessity for any equipment vendor, including Huawei, to gain access to user data as a result of supplying equipment. The TSRs require operators to control this data, and the controls on high risk vendors further reduce the risk.

    e. The paper makes a range of points about the Internet of Things (IoT) which highlight the need for realistic, use-specific, regulation, but are unrelated to the security of telecoms infrastructure.

---

[29] 5G choices: a pivotal moment in world affairs, Simeon Gilding, January 2020, https://www.aspistrategist.org.au/5g-choices-a-pivotal-moment-in-world-affairs/

[30] HCSEC is the Huawei Cyber Security Evaluation Centre in Banbury which independently evaluates the security of Huawei products used in the UK as part of the UK's long-standing mitigation strategy.

f. The paper asserts that 5G is fundamentally different to 4G because "one minute you're holding a 5G coffee cup that is transmitting back telemetric data on what the temperature is inside. And then the next moment that object can turn into something radically different". As the security of the network is independent of the data carried over that network, a change in use case does not make a 5G network any more vulnerable. Critical or safety-related uses of 5G networks will be subject to their own, independent regulation.

59. The HJS report relies significantly on the Huawei Cyber Security Centre Evaluation Board's Oversight Report for evidence of technical issues with Huawei's security, implying that these are not taken into account in the UK Government's posture. In fact, the report is written by the NCSC's Technical Director, and is fully factored into the overall security analysis. Indeed, this reinforces the point that because of the long-standing arrangements for risk mitigation, the UK knows more about Huawei's security than most countries.

60. Simeon Gilding's paper offers a more detailed technical analysis. However, among other problems it mischaracterises, repeatedly, the use of Huawei in the UK and the mitigations in place. We have previously provided a lay reader's introduction to the history of Huawei in the UK and the mitigations in place.[31]

61. The other technical and logical claims in the Gilding article with which we cannot concur include, but are not limited to:

    a. Mr Gilding, who, it should be noted, no longer works for the Government of Australia (who have made no comment on the claims in his article), sets out an account of how his team at the ASD undertook a study as to how a group of computer network attackers could use being able to compel a Radio Access Network vendor to carry out its tasks. He claims of his team "We concluded that we could be awesome, no one would know and, if they did, we could plausibly deny our activities". The NCSC is a part of GCHQ, which also has a publicly avowed, carefully regulated and overseen computer network exploitation mission, which is regarded as one of the best in the world. GCHQ does not share this view. Also, the fact that NCSC has a good view on our adversaries' attacks and has publicly attributed several nation state attacks – including from China - over the years shows that they can be, and consistently are being, detected.

    b. Mr Gilding's article describes a process of analysis that focussed entirely on the role of attack, with no regard for the defenders in the operators and regulators. In other words, to follow his own logic, he reached the conclusion that there was nothing defenders could do to stop his team, and reached this conclusion without even giving any consideration to what capabilities the defensive side might have. Again, it is necessary to point out that Mr Gilding does not, and does not claim to, speak for the Government of Australia. But given that his article received widespread attention, it is important to ensure confidence in the UK's technical assessment to point out that in contrast to Mr Gilding's account of his work, the UK's analysis was undertaken looking holistically across the whole intelligence and national security community in the UK at what attackers and defenders could do in terms of both technical and human capabilities. This, surely, is a more realistic and sensible way of analysing the balance of risk.

[31] Security, complexity and Huawei; protecting the UK's telecoms networks, NCSC Blog by Ian Levy, February 2019, https://www.ncsc.gov.uk/blog-post/blog-post-security-complexity-and-huawei-protecting-uks-telecoms-networks

c. Mr Gilding asserts that “legally compelled access to 5G vendors is game-changing for Chinese intelligence agencies because hacking is an increasingly tough business.” However, the argument put forward is made only in relation to Chinese vendors. The article fails to consider that Chinese Intelligence Law may be applied to all citizens and entities within China, including the many thousands working for most western vendors. An even-handed application of this argument would likely exclude all vendors from participation in 5G networks. Moreover, the NCSC did not regard the 2017 move to legally compelled access in China as “game-changing” precisely because from the moment Huawei entered the UK market in 2003, we have always worked on the assumption that such a practice was *de facto* in place, some fourteen years before it was codified.

d. Mr Gilding’s risk analysis appears to be limited to whether the existence of Huawei is of unmanageable benefit to Chinese Intelligence services. The article fails to contextualise that China is a highly-capable cyber actor in its own right. It does not address how vendor exclusion actually alters China’s prowess as a threat actor against national telecoms networks. We have already set out in this memorandum clear and compelling evidence that hostile states successfully exploit networks without ‘owning’ any of the equipment in that network and without any direct involvement in the third party support processes;

e. Mr Gilding states that “the reality is mature 5G networks actually require the collapse of the core–edge distinction.” This is one of the few technical assertions quoted in support of the argument that core and non-core distinctions collapse in 5G. His argument is that latency and efficiency require this, however he offers no evidence or technical argumentation as to why that may be the case. In this case, latency is a function of the speed of light in glass and is therefore dependent on the physical lay down of a network and so it is possible to build networks that meet latency requirements while still meeting security requirements. The article proceeds with a set of technical misunderstandings that further compound the analysis. Central is the belief that virtualisation, software defined networking and 5G use-cases mean that risk cannot be segregated, or that the ‘core’ and ‘edge’ collapse. As shown previously, if this is true, then no 5G network should ever be built. It would be too fundamentally unsafe, and impossible to secure.

62. These are the only two public documents that apparently contradict NCSC security analysis of 5G networks. This memorandum responds to their claims not in any attempt to foment a technical dispute; we welcome debate and scrutiny. It is simply to respond to the criticisms made in those papers so that Parliament can have a considered response to the only known technically based challenges to our assessment, as distinct from more general but unsubstantiated assertions about the collapse of the distinction between core and edge. It therefore remains clear that it is not only possible to segregate the access networks from the more sensitive functions, but that it is essential to do so for any 5G network that is built, regardless of the vendors chosen.

VI. Diversification: The market today and tomorrow

63. One area of apparent consensus in the debate around 5G infrastructure is the need for greater diversity in this part of the telecoms infrastructure. The main policy initiatives around that are set out in the DCMS/MoD memorandum. In this memorandum, the NCSC, which is fully supportive of these vital proposals, confines itself to some observations on market technicalities.

64. There is a significant amount of misinformation, and indeed hype, around the choice of vendors in the 5G market. The reality is complex and the details of how each vendor could be used in a particular country will vary depending on technical constraints, existing network lay down, skills in the operators, existing contracts and so on. One of the key pieces of hype that should be unambiguously corrected is that Huawei is always necessary to build a 5G network because they are more advanced than competitors. The NCSC does not recognise this purported fact or the corollary of it. In NCSC's view Nokia, Ericsson and Huawei are all in broadly the same position in terms of maturity, given the maturity of the standards, and functionality of 5G provision to operators.

65. The diversity within the market depends on which element of a network is being discussed. The access part of a 5G network – the 'edge' referred to previously – is the most constrained part of the market. Within the highly consolidated 5G 'macrocell' radio access network segment, the only current options in the UK are Nokia, Ericsson and Huawei. Within fixed access, the only current options are Nokia and Huawei. Globally, there are four additional companies able to provide macrocell sites: ZTE, Samsung, Fujitsu and NEC. ZTE is another Chinese company that will continue to be deemed a high risk vendor and NCSC has advised operators, to very good effect, against all use of ZTE in the UK market since April 2018[32]. None of Samsung, Fujitsu or NEC currently provide 5G infrastructure equipment at scale in the UK or Europe for various reasons. The UK Government is seeking to encourage them all to enter the UK market.

66. In the context of not recommending a complete ban on the use of Huawei network equipment, it is particularly important to note that the NCSC has always asked operators to use two vendors in their radio networks to deliver better resilience. To achieve resilience across multiple operators across the country this requires at least three vendors to be used. The only three vendors currently able to supply the UK at scale are Nokia, Ericsson and Huawei. However, where there are statements that there is no alternative to Huawei for the UK, it is in the context of being our third vendor. It is clear that the UK will continue to use Nokia and Ericsson and the Government has said that Huawei's share of the radio network will come down as the market diversifies. One major operator, BT, has already made a public statement setting out the costs it will incur as a result of the enforced reduction of Huawei's market share with the 35 per cent cap.

67. While the access part of the network is provided by a very constrained vendor base, other parts of the network, such as IP Core, OSS, virtualisation and orchestration and core functions, are served by a diverse set of companies from many countries. These network functions, where multiple alternative options exist, are also the places where the NCSC has advised Huawei should not provide equipment. While interoperability and market diversity are important outside the access network, the critical issue today is the lack of market diversity and lack of interoperability in the macrocell provision for 5G access sites and fixed access sites.

68. To fix the diversity issue, it has been suggested that existing small cell vendors are able to provide the UK market with diversity in the near future. However, most are

[32] The NCSC advised that the use of ZTE equipment in the context of the UK telecoms networks would lead to an unmanageable national security risk. This is because the UK's Huawei mitigation uses architectural controls to ensure that undetectable collusion across network elements cannot easily occur. The only sensible risk management assumption would be that Huawei and ZTE are controlled by a single controlling mind (the Chinese state) and therefore collusion between the two must be assumed. Permitting ZTE into the UK's telecoms networks would make management of the Huawei risk impossible.

only just starting to scale their engineering and product portfolio. As new market entrants, they are at an immediate disadvantage compared to existing players who have gained a reputation for building reliable equipment. Operators choosing to work with such newer companies do so at high risk, bearing in mind that major network failure may result in significant penalties by regulators. Hence the NCSC views these vendors as being at least five years from being able to compete in the 5G macrocell market with Ericsson, Nokia and Huawei.

69. Again, the Government is seeking to encourage these companies into the UK market and to set a technical environment that is conducive to new entrants, for example, by preferring open radio interfaces. However, it is unlikely that any new entrants to the radio access market will be able to scale sufficiently to meet multiple national requirements within a 3 to 5 year period. The telecoms market is complex, risk averse and rigorously standards-defined in ways that other sectors are not. The intense consolidation of the vendor base and lack of open interoperability testing engenders an incentive model that is not conducive to market diversification. The treatment of patents by the incumbent vendors makes entry into this market difficult for new companies.

70. Hence, the disincentives in the market are probably too great to overcome through pure commercial actions alone, and industrial capacity across the necessary supply chain will not scale sufficiently unless support from international governments is provided. This is the reason that the UK Government is looking at a significant and extensive diversification strategy under the leadership of DCMS. Diversification is essential to meeting the government's intent to reduce the UK's reliance on high-risk vendors.

71. Finally, when diversifying the market, it is important that we proceed with care. The details and technical complexity of different parts of the network really matter in terms of getting diversification right. The wrong initiatives could lead to unintended consequences that could easily exacerbate the problem. One consideration will be how any intervention will impact existing providers, in particular, Ericsson and Nokia. For example, some suggest that we should invest heavily in new core function and infrastructure providers, particularly those in the US. While this is part of a wider diversification strategy, it does not address the primary diversity issue in the access network, and may further reduce diversity in this critical market segment.

VII. Conclusion

72. The policy debate around 5G security across the globe has centred on whether or not Huawei should be permitted to take part in the building of any 5G networks, and if, so, subject to what restrictions. From a technical cyber security perspective, this issue, whilst important, is far from the most important issue of 5G security. The most important challenge is overall levels of network security.

73. It is not for the NCSC to comment on wider policy issues like the UK's approach to China. Our role is to provide advice on cyber security which is one aspect of a complex debate. This memorandum focuses purely on the technical security. From this standpoint, the firm position of the NCSC is that the case for complete exclusion of Huawei cannot be made on cyber security grounds alone. The technical case against the UK's position so far amounts to nothing more than unsubstantiated, unevidenced and technically fundamentally incorrect assertions that there is no – or in time will be no - distinction between core and edge functions in telecoms networks. As the standards written by global telecoms industry, which govern the build and operation of these networks set out, this is a fallacy. The NCSC is unaware of any

serious, technically credible, well-evidenced rebuttal of its analysis of 5G architecture and the consequent security requirements.

74. Whatever final legislation is enacted by Parliament on the basis of the balance of cyber security and other factors, the NCSC, as the UK's national technical authority for cyber security, believes that it will be impossible to provide for the security of 5G in the UK on the basis of accepting such fundamentally incorrect technical assumptions of there being no distinction between edge and core. The wider overhaul of telecoms security set out in the DCMS proposals, the most sweeping in terms of security in the history of the industry anywhere in the world, are of vital strategic importance to the UK's digital and national security. And they are based on this internationally shared, industry wide acceptance of the complex architecture of networks and the many and varied security requirements arising from them.