Written evidence submitted by James Sullivan, Head of Cyber Research, RUSI

About this submission

This submission is NOT a published RUSI product and should not be treated as such. It is intended to be used as evidence to assist UK Parliament's Defence Committee with its inquiry into the security of 5G technology.

For the full published RUSI research paper on '5G Cyber Security: A Risk Management Approach' please visit:
https://rusi.org/publication/occasional-papers/5g-cyber-security-risk-management-approach

In responding to this call for evidence, and within the accompanying RUSI cyber research paper, we answer the following two questions:

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

Overview

RUSI cyber research explored whether it was possible to risk manage the presence of equipment supplied by high-risk vendors (including Huawei) in the rollout of 5G networks. Our research concluded that from an evidence-based, technical risk management perspective, the UK's decision to exclude Huawei technology from the most sensitive parts of 5G networks, while allowing it to supply peripheral components such as mobile phone masts and antennae is practical and realistic. However, managing the risks from this level of involvement from Huawei is only possible if cyber security measures are implemented to a high standard.

RUSI cyber research identified multiple measures to manage risk to 5G networks, including resilient network architecture, access management, testing and monitoring, and cyber security standards. The findings demonstrate how core and edge functions do remain technically distinct in 5G networks and highlight multiple ways to isolate and localise risks. While recognising that 5G poses new challenges for cyber security practitioners, we found multiple ways to manage the risk. In doing so, operators must not dismiss measures that have historically reduced risk to telecommunications networks.

Our research acknowledges that for some states, it is entirely legitimate for political and economic considerations to be the dominant factors in decisions about banning particular vendors. However, governments must clearly distinguish between political and technical factors when justifying these decisions. Otherwise, it confuses the argument and undermines the authority of national technical experts. Policymakers should be clear about their reasons to ban certain vendors from 5G networks.

From a technical risk management perspective, labelling vendors as 'trusted' or 'untrusted' is misleading and unhelpful. Policymakers must recognise that no network will ever be 100% secure and no vendor can guarantee 'trustworthy' equipment. Instead, evaluation of all 5G components, regardless of vendor, should be informed by the degree of confidence in the security of components and infrastructure. The national origin of a component may be one factor to consider, but it is not the most important one. When assessing confidence in a component, the extent to which any particular

piece of technology contains inherent vulnerabilities (through malicious or poor engineering practices) and the extent to which any risk can be mitigated is more important.

Such vulnerabilities can exist wherever the technology is developed and produced. China's growing technological dominance means there is frequently a Chinese element somewhere. The level of risk tolerance to any cyber vulnerabilities should also depend on national context, including the geographic location of equipment, national cyber security experience, vendor availability, and cost.

In the following sections, we explain five reasons why the risk from vendors (including Huawei) can be managed within 5G networks. In doing so, we explain why a full ban of Huawei would not solve the issue of cyber risk in 5G networks. From a technical risk management perspective, reducing the number of 5G vendors (by fully banning Huawei) could actually increase the amount of overall cyber risk to 5G networks.

Reason 1: Lack of vendor diversity

Many experts believe vendor diversity is critical for creating secure networks.[1] Eliminating single points of failure and implementing back-up measures creates redundancy and thereby resilience. Vendors often reuse code or components in multiple products, meaning a single problematic line of code can bring down multiple types of equipment.[2] However, equipment from multiple vendors is extremely unlikely to all fail in the same way. Vendor diversity is therefore critical for 5G networks' resilience.[3]

Currently, redundancy is difficult to achieve, as few companies supply 5G components. For the UK (and much of mainland Europe) there are only three feasible providers for the Radio Access Network (RAN): Huawei, Ericsson, and Nokia. While ZTE and Samsung are also global providers of RAN equipment, they are not viable solutions in mainland Europe. ZTE has direct and well-documented ties with the Chinese government.[4] Meanwhile, Samsung does not currently have a presence in Europe, and most of its equipment is designed for a different frequency than most European countries have allocated for 5G (mmWave versus sub-6).[5] This means that, while Samsung is a suitable vendor for many Asian countries and the United States, they would have difficulty developing equipment for a European market.

Much like 4G, UK 5G regulation will require the presence of at least two vendors in its 5G networks. A full ban on Huawei, would leave only two vendors who provide UK RAN components, thereby reducing network redundancy and resilience. Eliminating competition limits incentives for other vendors to increase security or quality of their components. This lack of vendor diversity is an enduring challenge.

In the longer term, governments should think about how they might cultivate more vendors to increase network diversity. This may require governments to develop targeted investment schemes

---

[1] NIS Cooperation Group, 'EU Coordinated risk assessment of the cybersecurity of 5G networks', published 9 October 2019, <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62132>.
[2] Finite State, 'Huawei Supply Chain Assessment', <https://finitestate.io/finite-state-supply-chain-assessment/>.
[3] Defense Innovation Board, 'The 5G Ecosystem: Risks and Opportunities for DoD,' 4 October 2019, <https://media.defense.gov/2019/Apr/03/2002109302/-1/-1/0/DIB_5G_STUDY_04.03.19.PDF>.
[4] Jamie Davies, 'ZTE gets ahead of the game with cybersecurity centre launch', *telecoms.com,* 10 July 2019, <https://telecoms.com/498428/zte-gets-ahead-of-the-game-with-cybersecurity-centre-launch/>.
[5] Samsung, 'Integrating mmWave 5G Technical Innovations', <https://www.samsung.com/global/business/networks/products/radio-access/access-unit/>, accessed 16 April 2019.

to enable diversification or leverage its procurement power. Initiatives promoting interoperability, such as OpenRAN, may also help lower barriers to market entry. OpenRAN is a group of companies trying to make it technically possible for different vendors' equipment to interoperate in the RAN. However, such initiatives face serious challenges. Even if interoperability is feasible, it may not yet be economically viable. While creating long-term market diversity is an important aim, it will take a long time to achieve.

Reason 2: The distinction between sensitive and non-sensitive network layers

Core and edge functions remain technically distinct in 5G networks. Defining core and edge is not a precise science. This research adopts the NCSC's definitions. 'Core' components have more control over the network than access-layer ('edge') components. Core components know more about the context of a 5G network and include routing and switching functions on base stations. If these functions fail or are compromised, the impact on the rest of the network could be high, as they overlay and control the entire network.[6] In the UK, 5G networks will have more cores than previous networks.[7]

Edge functions are in networks' peripheries, interfacing between networks and customers.[8] The failure of individual edge components, such as a radio access network (RAN)[9] antenna, is usually highly localised.[10] Therefore, the impact of failure or compromise has a limited impact on the network overall. Edge components also have limited access to sensitive data. Data within this layer includes who is accessing the network and what information they are sending and receiving.

Some experts argue that, in 5G networks, the network core and edge of are no longer separated.[11] However, network operators and international standards bodies have published standards to segment

---

[6] Ian Levy, 'Security, Complexity, and Huawei; Protecting the UK's Telecoms Networks', blog, National Cyber Security Centre (NCSC), 22 February 2019, <https://www.ncsc.gov.uk/blog-post/blog-post-security-complexity-and-huawei-protecting-uks-telecoms-networks>, accessed 22 July 2019. Core components include network function virtualisation infrastructure, virtual network function, management and network orchestration, operational support systems and business support systems.

[7] Author's interview with UK G1, UK government official, 29 October 2019.

[8] The authors chose to use this definition as this reflects the risk-management approach adopted by the UK, and it is the approach that has been scrutinised by other nations. It defines that peripheral 5G components will only sit within the access layer of the network. It is a precise definition that makes a clear distinction between the access layer (edge) and other parts of the network. The definition of edge does not include the transport layer (that is, wires, fibres, microwaves and other methods of transmission).

[9] The RAN is the part of 5G network infrastructure that connects end user devices with the network's transport and transmission layer that aggregates traffic and carries it to the network's central control functions. The UK Supply Chain Review Report assessed that RAN carried less critical security risks than other parts of the network, which could be sufficiently mitigated through diversity of supply. DCMS, UK Telecoms Supply Chain Review Report, p. 26; House of Commons, Science and Technology Committee, 'Oral Evidence'.

[10] Author's interview with UK G3, UK government official, 8 November 2019. '[B]ase station on the roof is going to fail at some point – what does that mean? ... Well it can only talk to the base stations nearby'. In Levy, 'Security, Complexity, and Huawei', it is noted that 'Transport nodes only care about the directly adjacent nodes that they're physically connected to'.

[11] There are numerous sources that explain this argument, including: Chris Duckett, '5G Stakes Couldn't Be Higher So We Advised Huawei Ban: ASD', ZDNet, 30 October 2018; Elsa B Kania, 'Securing Our 5G Future: The Competitive Challenge and Considerations for US Policy', Center for a New American Security, 7 November 2019; Justin Sherman, 'Making Sense of a Huawei "Partial Ban"', blog post, New America, 3 July 2019, <https://www.newamerica.org/cybersecurity-initiative/c2b/c2b-log/making-sense-huawei-partial-ban/>, accessed 13 December 2019; Leigh Hartman, 'Get Smart: Core vs. Edge in 5G Networks', US Embassy and Consulates in the United Kingdom, 17 September 2019, <https://uk.usembassy.gov/get-smart-core-vs-edge-in-

a network and separate the layers.[12] Implementing these measures to a high standard ensures these functions remain technically distinct in 5G infrastructure.[13] Further, if there is no distinction at all between sensitive and non-sensitive parts of a 5G network, this dismisses historical measures for reducing risk to telecommunications networks, such as network segmentation.

Reason 3: Managing risk from virtualised hardware and low latency communications

RUSI cyber research recognises that 5G poses new cyber security challenges, owing to technical advancements such as virtualisation and low-latency communication. However, RUSI's research concluded that there are measured ways to manage the risk from both.

Historically, software has been run on proprietary hardware, assigning specific physical boxes to specific network functions. With virtualised hardware, 5G networks can run multiple functions across the network on shared physical components in a cloud-based environment. Virtualised networks need not rely on one vendor, but can be built with components from many, allowing operators to pick and choose. In this new 'interoperable' context, some analysts perceive no physical or logical separation between core and edge functions.[14] However, in reality firewalls and other measures do continue to segregate network layers in a virtualised environment.[15] The challenge for cyber security practitioners is to ensure that measures are implemented effectively in the context of 5G networks. Prescriptive and rigorous cyber standards relating to the cyber security of virtualised networks will be critical.

Second, 5G networks are designed to support low-latency data transfer in microseconds. Achieving communication at this speed requires processing power closer to the edge of 5G networks. This means moving network cores closer to the end user. In theory, this could require putting core components in the same location as edge components – for example, putting core functions on RAN antennae. However, this would be unwise and unnecessary and there are no use cases where this is currently required.[16]

Reason 4: Supply chain complexity

The growing complexity, length, and global nature of supply chains means that operators and countries can no longer assume that any equipment is trustworthy, regardless of the vendor. This is largely the result of three factors: the difficulty of tracing supply chains, human error, and the sheer number of attack vectors for malicious actors.

The national origin of a company does not accurately reflect where equipment is manufactured. Many reputable global tech companies have factories in China. The sheer number of third-party vendors and subcontractors around the globe complicates tracking where components for a particular piece of

---

5g-networks/>, accessed 13 December 2019; Colin Packham, 'Australia Spy Chief Says 5G Risks High, in Nod to China Firms' Exclusion', Reuters, 30 October 2018.

[12] House of Commons, Science and Technology Committee, 'Oral Evidence: UK Telecommunications Infrastructure, HC 2200', 10 June 2019, <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/uk-telecommunications-infrastructure/oral/102931.html>, accessed 24 July 2019.

[13] Levy, 'Security, Complexity, and Huawei'.

[14] Simeon Gilding, '5G Choices: A Pivotal Moment in World Affairs', Australian Strategic Policy Institute, 29 January 2020, <https://www.aspistrategist.org.au/5g-choices-a-pivotal-moment-in-world-affairs/>, accessed 31 January 2020.

[15] Amazon Web Services, 'Shared Responsibility Model', <https://aws.amazon.com/compliance/shared-responsibility-model/>, accessed 31 January 2020.

[16] Levy, 'Security, Complexity, and Huawei'.

equipment originate or travel.[17] Malware or backdoors can be installed at any level of the process.[18] And the farther upstream a malicious actor alters a component, the more of a multiplier effect it can have.[19]

Regardless of location, human error is a key source of vulnerabilities in 5G. The software that supports 5G networks comprises millions of lines of code drawn from multiple locations. Experience shows that defects per thousand lines of code exist on a large scale, many of which cause vulnerabilities. The amount of code in 5G networks is prone to human error and will continue to cause inadvertent vulnerabilities.[20]

The scale and complexity of supply chains creates multiple attack vectors.[21] Even equipment from a supposedly "safe" location can have malicious back doors. China, or another threat actor, could insert an operative into a western vendor.[22] Vendors can also lie about the origin of their equipment.[23] Policymakers have discussed the advantage state actors gain from internal access at length, but cyber criminals could also create back doors.[24]

All of this is also a concern when networks need maintenance and patching. While original vendors are often involved, there is also a large ecosystem of third-party suppliers and subcontractors.[25] Software patching and maintenance are key attack vectors, both because the patch itself can be compromised along the supply chain, and as a result of the access needed to install the patch.[26]

Reason 5: Partial bans of high-risk vendors

The NCSC designates Huawei a High-Risk Vendor (HRV) based on the following HRV criteria: a vendor's strategic position in the UK and in other telecommunications networks; quality and transparency of

---

[17] NIS Cooperation Group, 'EU Coordinated risk assessment of the cybersecurity of 5G networks', published 9 October 2019, <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62132>.
[18] DCMS, 'Telecoms Supply Chain Review', 22 July 2019, <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/819469/CCS001_CCS0719559014-001_Telecoms_Security_and_Resilience_Accessible.pdf>.
[19]Ariel Levite, 'ICT Supply Chain Integrity: Principles for Governmental and Corporate Policies', Carnegie Endowment for International Peace, <https://carnegieendowment.org/2019/10/04/ict-supply-chain-integrity-principles-for-governmental-and-corporate-policies-pub-79974>.
[20] 'O2 4G data network restored after day-long outage', *BBC*, 7 December 2018, <https://www.bbc.co.uk/news/business-46464730>. and NIS Cooperation Group, 'EU Coordinated risk assessment of the cybersecurity of 5G networks', 9 October 2019, <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62132>.
[21] '5G and security in Italy', *The European House*, November 2019, <https://www.ambrosetti.eu/wp-content/uploads/191104_Ambrosetti_5G.pdf>.
[22] Ciaran Martin, 'Ciaran Martin at Cyber 2019, Chatham House', NCSC, 20 June 2019, <https://www.ncsc.gov.uk/speech/ciaran-at-chatham-house>.
[23] Jonathan Dienst and Joe Valiquette, 'Long Island Tech Firm Accused of Selling Chinese Equipment to US Military', *NBC*, 7 November 2019, <https://www.nbcnewyork.com/news/local/Long-Island-Tech-Firm-Accused-Of-Selling-Chinese-Equipment-to-US-Military-564606271.html>.
[24] Ariel Levite, 'ICT Supply Chain Integrity: Principles for Governmental and Corporate Policies', Carnegie Endowment for International Peace, <https://carnegieendowment.org/2019/10/04/ict-supply-chain-integrity-principles-for-governmental-and-corporate-policies-pub-79974>.
[25] NIS Cooperation Group, 'EU Coordinated risk assessment of the cybersecurity of 5G networks', published 9 October 2019, <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62132>.
[26] Ariel Levite, 'ICT Supply Chain Integrity: Principles for Governmental and Corporate Policies', Carnegie Endowment for International Peace, <https://carnegieendowment.org/2019/10/04/ict-supply-chain-integrity-principles-for-governmental-and-corporate-policies-pub-79974>.

the vendor's engineering and cyber security; past behaviour and practices; vendor resilience; and domestic state apparatus, laws and offensive cyber capabilities of the vendor's country of origin.

Experts have suggested security-enhancing measures for 5G networks to include market caps, extensive testing[27], restricting high-risk vendors to certain parts of the network[28], and geographic bans[29]. The European Union toolkit in December recommends how member states can best protect 5G networks.[30] Countries are taking different approaches to secure their networks from high-risk vendors.

Standard cyber risk management requires the identification of 'crown jewels': the data or operational capabilities that must be protected, and where risk must be kept low. As discussed elsewhere in this submission, the conclusion that the integrity of the entire network would be unacceptably compromised, even if a single component is derived from an HRV, is highly unlikely from a technical risk-management perspective. However, banning technology from an HRV from sensitive parts of a network is a realistic risk-management measure.

The recent UK decision adopted such an approach, introducing criteria to identify an HRV and a framework for managing any risk they may pose to the network.[31] The associated risk-management framework states that any HRV will have a limited role in UK networks (not just 5G), excluding them from all core functions such as security, operational support, management and authentication, virtualisation infrastructure, network monitoring, lawful intercept and any future 5G core functions.[32] Meanwhile, the proportion of HRV components in peripheral parts of UK 5G infrastructure should have a hard cap of 35% to allow for effective cyber security risk management. Finally, the HCSEC will continue to facilitate detailed inspection of Huawei equipment.

Limiting Huawei equipment to 'peripheral' parts of the infrastructure does not automatically grant it access to the entire network. Network segmentation (or segregation) is an accepted measure for ensuring resilience in existing networks.[33] International standards bodies, such as 3GPP, work extensively to support the separation of different layers of the network.[34] While operators cannot

---

[27] Amit Katwala, 'Here's how GCHQ scours Huawei hardware for malicious code,' *Wired,* 22 February 2019, <https://www.wired.co.uk/article/huawei-gchq-security-evaluation-uk>.

[28] Michael Holden and Jack Stubbs, 'Britain to allow Huawei restricted access to 5G network', *Reuters,* 24 April 2019, <https://uk.reuters.com/article/uk-britain-huawei/britain-to-allow-huawei-restricted-access-to-5g-network-idUKKCN1S00M8>.

[29]For a detailed explanation of countries' approaches to 5G, see the written evidence submitted by RUSI for the Joint Committee on the National Security Strategy's inquiry, 'Ensuring Access to "Safe" Technology: The UK's 5G Infrastructure and National Security Issue', <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/national-security-strategy-committee/ensuring-access-to-safe-technology-the-uks-5g-infrastructure-and-national-security/written/105189.html>, accessed 30 January 2020.

[30] European Commission, 'Member States publish a report on EU coordinated risk assessment of 5G networks security', 9 October 2019, <https://europa.eu/rapid/press-release_IP-19-6049_en.htm>.

[31] NCSC, 'NCSC Advice on the Use of Equipment from High Risk Vendors in UK Telecoms Networks'. HRV criteria include: the vendor's strategic position in the UK and in other telecommunications networks; the quality and transparency of the vendor's engineering and cyber security; past behaviour and practices; the vendor's resilience; and the domestic state apparatus, laws and offensive cyber capabilities of the vendor's country of origin.

[32] As specified by 3GPP TS 23.501.

[33] 5G Americas, 'The Evolution of Security in 5G', July 2019, <https://www.5gamericas.org/wp-content/uploads/2019/07/5G_Americas_5G_Security_White_Paper_Final.pdf>, accessed 29 January 2020; author's interview with T1, member of the telecommunications sector, 27 September 2019.

[34] 3GPP, 'Release 15'.

guarantee that they have prevented attackers from moving between layers, they can make it much more difficult, time-consuming and resource-intensive.[35] Further, the more hurdles an attacker has to surpass to move between layers, the more likely it is that the attacker will eventually be found.[36]

To secure 5G networks, operators must continue to closely regulate and supervise vendor access to the network.[37] Access controls could include supervising vendors while they are in the network and limiting the amount of time that vendors have access to it.[38] For many, network access is the strongest justification for banning vendors where confidence is low in their equipment.[39] Other experts argue that if operators keep close control over the process and use the proper protocols and procedures, anyone should be able to provide this support without jeopardising the network.[40] Certainly, the supply chain vulnerabilities discussed above apply both to vendors and individuals performing maintenance and patching functions.[41]

Segregation and access management are therefore critical components of 5G network security. Such controls significantly decrease the risk of an outside attacker gaining unauthorised access or a vendor abusing authorised access to exploit existing vulnerabilities or insert backdoors. This is true regardless of who the vendors are.

Recommendations

- 5G networks have inherent vulnerabilities. As a policy priority, governments should implement appropriate technical cyber risk-management measures that protect against most risks. In doing so, it must be noted that no network will ever be 100% secure and no vendor can guarantee 'trustworthy' equipment. Instead, all equipment should be assessed on a scale of confidence. Banning any particular vendor, such as Huawei, will not fully address the issue of cyber risk in 5G networks and does not automatically make 5G networks safer. And the financial costs associated with such a ban may be significant.
- Policymakers and practitioners should seek to maintain the distinction between sensitive and non-sensitive parts of a 5G network when assessing approaches to 5G cyber security, even if this division is slightly blurred. 5G is not a technology where every component is of instrumental importance to network security and there are multiple ways to isolate and localise the risk.

Political and economic considerations may be the overriding factors that lead to the decision to ban a particular vendor for some governments. This may be an entirely legitimate policy approach. But governments must be clear about the extent to which political, rather than technical, factors inform their decision-making relating to 5G. They should not seek to mask these political considerations with weak assertions about technical risk management.

---

[35] Author's interview with UK G3, UK government official, 8 November 2019.
[36] Author's interview with T3, member of the telecommunications sector, 3 October 2019.
[37] Author's interview with UK G1, UK government official, 29 October 2019; author's interview with UK G3, UK government official, 8 November 2019; author's interview with UK G4, UK government official, 11 November 2019; author's interview with UK G3, UK government official, 8 November 2019; author's interview with T5, member of the telecommunications sector, 29 October 2019.
[38] Author's interview with UK G4, UK government official, 11 November 2019.
[39] Simeon Gilding, '5G Choices: A Pivotal Moment in World Affairs', Australian Strategic Policy Institute, 29 January 2020, <https://www.aspistrategist.org.au/5g-choices-a-pivotal-moment-in-world-affairs/>, accessed 31 January 2020.
[40] Author's interview with T5, member of the telecommunications sector, 29 October 2019.
[41] Author's interview with UK G3, UK government official, 8 November 2019.

About RUSI

The RUSI cyber programme brings much-needed research focus and capacity to support UK and international strategic responses to cyber security challenges. In so doing, the programme helps inform approaches to tackling cyber threats by conducting research and running events that develop a strong evidence base for policymakers and practitioners alike.

Our outputs include:

- **Research and analysis**: Research and related publications on cyber security. Findings and recommendations are disseminated to stakeholders (including the public where applicable) in the following formats: research papers, policy briefs, open access journal articles, edited collections, short-form monographs, and translated texts.
- **Convening and coordination:** A series of conferences, roundtables, panels and workshops dedicated to cyber security issues. RUSI will leverage a network of researchers, policy-makers and practitioners to exploit fully the opportunities that cyber security research and dialogue provides, with the aim of influencing policy and practice across government and industry.
- **Education, awareness and behaviour:** To improve understanding of cyber security challenges, the RUSI Leadership Centre is able to work with public and private sector partners to develop and deliver appropriate material on cyber security education awareness and behaviour

RUSI recently conducted a nine month research project on the high-level technical cyber security risks relating to 5G telecommunications infrastructure and the extent to which they could be mitigated. Recommendations were based on a risk-management framework, which acknowledged that it is impossible to completely eradicate risk, particularly in complex, dynamic systems such as 5G. Instead, the challenge is to set a realistic risk tolerance or level of acceptable risk and develop mitigation methods that have the greatest likelihood of supporting that risk tolerance.

The project included extensive research using academic literature, media reports, open source government documents and in-depth semi-structured interviews with senior cyber security experts. For these interviews, experts were chosen based on their subject-matter expertise and experience, using a non-probabilistic (selective) sampling method. Interviewees included government officials, law enforcement, private sector experts and academics.

The project concluded with research paper on 5G. More detailed answers to many of the Committee's questions can be found in that report, which is available on the RUSI website.

16 April 2020