House of Commons Committees

Defence Committee

The Security of 5G

Second Report of Session 2019–21

HC 201

House of Commons
Committees

Defence Committee

The Security of 5G

Second Report of Session 2019–21 HC 201

Report, together with formal minutes relating to the report

Ordered by the House of Commons to be printed 22 September 2020

Published on 8 October 2020 by authority of the House of Commons

The Defence Committee

The Defence Committee is appointed by the House of Commons to examine the expenditure, administration, and policy of the Ministry of Defence and its associated public bodies.

Current membership

Rt Hon Tobias Ellwood MP (*Conservative, Bournemouth East*) (Chair)

Stuart Anderson MP (*Conservative, Wolverhampton South West*)

Sarah Atherton MP (*Conservative, Wrexham*)

Martin Docherty-Hughes MP (*Scottish National Party, West Dunbartonshire*)

Richard Drax MP (*Conservative, South Dorset*)

Rt Hon Mr Mark Francois MP (*Conservative, Rayleigh and Wickford*)

Rt Hon Kevan Jones MP (*Labour, North Durham*)

Mrs Emma Lewell-Buck MP (*Labour, South Shields*)

Gavin Robinson MP (*Democratic Unionist Party, Belfast East*)

Rt Hon John Spellar MP (*Labour, Warley*)

Derek Twigg MP (*Labour, Halton*)

Powers

The committee is one of the departmental select committees, the powers of which are set out in House of Commons Standing Orders, principally in SO No 152. These are available on the Internet via www.parliament.uk.

Publications

© Parliamentary Copyright House of Commons 2020. This publication may be reproduced under the terms of the Open Parliament Licence, which is published at www.parliament.uk/copyright.

Committee reports are published on the Committee's website at www.parliament.uk/defcom and in print by Order of the House.

Committee staff

Matthew Congreve (Second Clerk), Mark Etherton (Clerk), Arvind Gunnoo (Committee Assistant), Dr Greg Hannah (Committee Specialist), Ian Thomson (Committee Specialist), Dr Lauren Twort (Committee Specialist), Sarah Williams (Senior Committee Assistant) and George Woodhams (Committee Specialist).

Contacts

All correspondence should be addressed to the Clerk of the Defence Committee, House of Commons, London SW1A 0AA. The telephone number for general enquiries is 020 7219 5745; the Committee's email address is defcom@parliament.uk. Media inquiries should be addressed to Joe Williams on 075 4651 7626 or Toni McAndrew-Noon on 075 6243 5286.

You can follow the Committee on Twitter using @CommonsDefence.

Contents

Summary 3

Context of the inquiry 7

Our Inquiry 7

Debates on telecoms network security 8

Overview of 5G in the UK 10

What is 5G? 10

5G - A step change? 12

Threats associated with 5G 14

Government ambitions for the UK's 5G rollout 17

Mobile network operators 17

The UK 5G vendor market 19

Government restrictions on Huawei 24

January 2020: The conclusions of the Telecoms Supply Chain Review and initial restrictions on high-risk vendors 24

May 2020: US sanctions against Huawei 28

July 2020: The banning of the purchase of Huawei equipment from 2021 and Huawei's removal from 5G by 2027 30

Technical Considerations 33

Cyber attacks 33

The security of Huawei's products 36

Network security and Huawei's involvement 40

Why the restrictions on Huawei had to change - the US sanctions 41

5G in Defence and National Security 42

Geopolitical considerations 44

The Geopolitics of 5G 44

Huawei and the Chinese state 49

Ownership and links to the Chinese Communist Party 49

Chinese subsidies 50
The National Intelligence Law 50
The Chinese state's reaction to the removal of Huawei 52
Working with allies on 5G provision 54
Global standards 58
Conclusions for the UK market 61
Timescales for the removal of Huawei 61
The economic impact on operators 63
Diversifying the UK's consolidated vendor market 65
Attracting other 5G vendors 66
The problem of non-interoperability and Open-RAN 68
Network security and the Telecoms Security Requirements 71
Conclusions and recommendations 75
Sub-Committee Formal Minutes 81
Tuesday 22 September 2020 81
Members present: 81
Minutes 81
Next meeting 81
Committee Formal Minutes 82
Tuesday 22 September 2020 82
Members present: 82
Minutes 82
Next meeting 82
Witnesses 83
Tuesday 28 April 2020 83
Published written evidence 86

Summary

5G will transform lives of many in the UK and across the world by facilitating the Internet of Things. This is a positive development and will bring with it numerous economic and social advances. We share the Government's objective that the UK remains at the forefront of the 5G rollout as we move into the next technological era. However, 5G will increase our reliance on mobile connectivity, and this represents a security risk whether from 'espionage, sabotage or system failure'. Many more items will be connected to the Internet through 5G meaning a greater surface for illicit actions which represents a risk to individuals as well as to defence and government.

Our inquiry into the security of 5G was launched in the context of a lively debate on the security of the UK's 5G network in Parliament and across the country from late 2019 and through 2020 with a focus on the presence in our network of high-risk vendors, particularly Huawei. A significant Government announcement took place in January with restrictions placed on high-risk vendors followed by stricter rules announced in July, with Huawei to be removed from the UK's 5G network by 2027.

During our study we found that the UK, and its allies, face many malicious cyber-attacks both from rogue individuals and state-sponsored attacks from states such as Russia and China. These attacks are diverse in their nature and in their aims, with some attacks aiming to steal individual data and state secrets whilst others seek to bring down the network in its entirety. These attacks impact our 5G networks as well as more widely in the cyber sphere. It is important that the Government calls out cyber-attacks from adversaries on the international stage and works to find a deterrent to counter them. There is currently a lack of global rules regulating international cyber-attacks and the Government

should be working with allies to formulate a system to provide accountability for perpetrators. It should clarify why it is not deploying a cyberattack capability to deter aggressors.

The presence of Huawei equipment in our network increased the risk posed by these attacks and there is no doubt that Huawei's designation as a high-risk vendor was justified. The Huawei Cyber Security Evaluation Centre consistently reported on its low-quality products and concerning approach to software development, which has resulted in increased risk to UK operators and networks. The presence of Huawei in the UK's 5G networks posed a significant security risk to individuals and to our Government. We do, however, recognise that, prior to the United States' sanctions placed on Huawei in May, advice to Government was that the presence of Huawei in the UK's networks was a manageable risk. We know that the UK has one of the most active and effective cyber-security regimes in the world, and, from our public and private conversations with Government, we were confident that GCHQ and the NCSC were able to appropriately manage any increased risk posed by the presence of Huawei or other high-risk vendors in the UK's 5G. Furthermore, we recognised that whilst the risk remained manageable, it was important to remember the benefits in having a greater number of vendors involved in 5G network provision, despite Huawei's designation as high-risk, as this improves overall network resilience should a single vendor fail. Therefore prior to the US sanctions announced in May, the risk of Huawei products remaining in the UK's 5G networks was, according to the Government, significant but manageable through monitoring and regulation. The situation changed when Huawei was deprived of reliable chip manufacturing capabilities and following these sanctions, it became much more difficult to guarantee and measure the quality of Huawei products. In principle, the Government has therefore made the correct technical decision to ban the purchase and presence of Huawei products in the future.

Some have contended that Huawei's presence in 5G poses risks to our national security sites and sensitive communications, however we are content that Huawei has been, and continues to be, sufficiently distanced from sensitive defence and national security sites. The Defence Secretary has informed us that no Huawei 5G equipment is present on the defence estate and that sensitive communications are safe from compromise. Huawei's continued presence in commercial 5G networks therefore does not impact on our ability to share sensitive information with partners.

We recognise that the Government has had to balance its own technical considerations with pressures from allies such as the United States and Australia. Our closest allies within Five Eyes originally embarked on a policy at odds with the UK's and this had the potential to damage the UK's close intelligence, security and defence relationship with them, although reassurances have been given by Ministers that this was not the case. The framing of the issue by the United States as a technical concern about the presence of Huawei in our

networks has generated disagreement between the two Governments, given the contrasting conclusions of technical experts on either side of the Atlantic. Whilst the Government decision was ultimately taken because of the technical considerations resulting from the US sanctions the Government should have considered the potential damage to key alliances enough of a risk to begin to remove Huawei from the UK's 5G network before the US sanctions were imposed.

A further geopolitical consideration our inquiry highlighted was Huawei's relationship with the Chinese state. It is clearly strongly linked to the Chinese state and the Chinese Communist Party, despite its statements to the contrary, as evidenced by its ownership model and the subsidies it has received. Additionally, Huawei's apparent willingness to support China's intelligence agencies and China's 2017 National Intelligence Law are further cause for concern. Having a company so closely tied to a state and political organisation sometimes at odds with UK interests should be a point of concern and the decision to remove Huawei from our networks is further supported by these links. Concern about Huawei is based on clear evidence of collusion between the company and the Chinese Communist Party apparatus, and it is important that the West does not succumb to ill-informed anti-China hysteria and recognises the mutual benefits of Chinese involvement in our economy. We recommend that the UK, and allies, should ensure that decisions taken around the involvement of Chinese companies are taken in an evidence-based manner, and only when risk is demonstrable should decisions around removal be made.

In the lead up to the decision surrounding Huawei's removal, pressure had been exerted by the Chinese Government on the UK Government to retain the presence of Huawei in its 5G infrastructure through both covert and overt threats. Following the decision, China has threatened to withdraw from some areas of the UK's economy, including in critical infrastructure such as nuclear. Whilst ending China's involvement in the UK's critical infrastructure would be a radical step with huge implications for the UK's economy, if threats by the Chinese state continue and worsen, the Government should carefully consider China's future presence in critical sectors of the economy. We recommend that the Government should make provision in its proposed National Security and Investment Bill to give it the power to intervene and stop investments in critical industries should threats or risks be present.

China dominates the telecommunications industry and it is evident that the UK has a lack of industrial capacity in this sector. This is not unique to the UK and in order to combat China's dominance, we support the principle of proposals for forming a D10 alliance of democracies to provide alternatives to Chinese technology. Following consultation with allies, the Government should set out exactly what the role of this alliance would be, both regarding 5G and wider security considerations, and seek to make progress as quickly as possible on formulating joint 5G policy.

Following its decision to remove Huawei, the Government has faced pressure to remove it more quickly than by 2027. The evidence we have received, however, would suggest that a quicker timescale could result in signal blackouts, delay the 5G rollout significantly and cost both operators and the economy greatly. Therefore, for the time being, we consider the plan for a removal by 2027 to be a sensible decision. However, should pressure from allies for a speedier removal continue or should China's threats and global position change so significantly to warrant it, the Government should consider whether a removal by 2025 is feasible and economically viable. Clearly these restrictions will delay the 5G rollout and economically damage the UK and mobile network operators. The Government should take necessary steps to minimise the delay and economic damage and consider providing compensation to operators if the 2027 deadline is moved forward.

The UK vendor market for 5G kit is not diverse enough and even with the inclusion of Huawei the market was "sub-optimal". The Government's decision to remove Huawei completely from 5G by 2027 poses a risk that could result in an even less diverse market, which brings security and resilience concerns of its own. The Government should work with mobile network operators to bring in new vendors to the UK, for example Samsung or NEC, as well as encouraging the development of industrial capability in the UK. This will not only improve market diversity but make our networks more resilient and lessen the potential security risks by removing Huawei and therefore leaving the UK reliant on Nokia and Ericsson alone. In addition to this, OpenRAN presents an opportunity to move away from the current consolidated vendor environment to one in which operators no longer have to consider which vendor to source from. The UK Government and mobile service operators should continue investment in OpenRAN technology and work to make the UK a global leader in both technological development and production.

Finally, we found that the current regulatory situation for network security is outdated and unsatisfactory. The planned Telecoms Security Bill is required to bring regulations up to date and allow the Government to compel operators to act in the interests of security. The current situation has led to commercial concerns trumping those of national security, which is unacceptable. The Government should not allow a situation where short-term commercial considerations are placed ahead of those for national security and defence. The Telecoms Security Bill is necessary in order to enhance the Government's and Government bodies' regulatory powers and should be introduced before 31 December 2020.

Context of the inquiry

Our Inquiry

1. On 6 March 2020 we launched our inquiry into the security of 5G, following the UK Government's decision to exclude high risk vendors, notably Huawei, from the most sensitive parts of the UK's 5G network, while allowing it to supply peripheral components such as mobile phone masts and antennae. At the time we invited written evidence submissions on the following points:

- What are the risks to the UK's 5G infrastructure? How can these be mitigated?
- What is the role of government in 5G cyber security?
- 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 credible alternatives are available to Huawei systems?
- To what extent was the UK Government's decision on Huawei driven by political rather than technical factors?
- How will the UK Government's decision impact the UK's geopolitical position?
- How will the UK's allies, particularly those in Five Eyes, respond to this decision?

- How will this decision impact the UK's security and defence capabilities and the UK's interoperability with allies?
- How important is it for the UK, separately or with allies, to maintain industrial capability in this field?[1]

We received 22 submissions of written evidence, which we have published on our website.[2] We received several other submissions which were shared with us confidentially and have therefore not been published but nevertheless informed our work. We held five public oral evidence sessions.[3] In addition to these public meetings we spoke privately with government cyber security experts and met with the Telecom Infra Project.

We are grateful to all who contributed to the inquiry and shared their insights with us, this was particularly valuable during a period where there were a number of developments in government policy in this area.

Debates on telecoms network security

2. In order to contextualise our inquiry, and the subsequent Government policy in this area, it is important to recognise that debates on telecoms network security have been long running.

In 2019 and early 2020 there was a wide-ranging debate in Parliament, Government, and the media about the extent to which high-risk vendors (HRVs), in particular Huawei, should be used in UK 5G networks.[4] Other Parliamentary bodies have previously inquired into telecoms networks with differing levels of focus on the security of the networks. In 2019 the Intelligence and Security Committee of Parliament released a statement on 5G suppliers, and the Science and Technology Committee has previously questioned government on this topic with the current committee holding an inquiry on UK telecommunications infrastructure and the UK's domestic capability.[5]

3. The debate surrounding Huawei's involvement has centred not only on technical considerations but on broader geopolitical issues. There are concerns about the security standards of Huawei equipment in general, the extent to which Chinese law could compel the company to assist the State's intelligence services, coupled with broader ethical and ideological concerns about the

1 Defence Committee, 6 March 2020, Defence Committee launches Sub-Committee on the security of 5G
2 Defence Committee, The Security of 5G, All written evidence
3 Defence Committee, The Security of 5G, All oral evidence
4 Urgent Question, 25 April 2019, UK Telecoms: Huawei; Debate, 22 July 2019, Telecoms Supply Chain Review; Westminster Hall, 4 March 2020, Huawei and 5G; Debate, 10 March 2020, Telecommunications Infrastructure (Leasehold Property) Bill
5 Intelligence and Security Committee of Parliament, 19 July 2019, Statement on 5G suppliers; Science and Technology Committee, 10 July 2019, Letter to the Secretary of state for Digital, Culture, Media and Sport; Science and Technology Committee, UK telecommunications infrastructure and the UK's domestic capability

growing global presence of Chinese technology companies.[6] This is in addition to growing pressure from UK allies, particularly the USA and Australia, to resist Huawei's technology.

6 Cabinet Office, 28 March 2019, Huawei cyber security evaluation centre oversight board: annual report 2019,; House of Commons Library Briefing Paper, Georgina Hutton, 6 September 2019, 5G; Henry Jackson Society, Bob Seely MP, Dr Peter Varnish OBE and Dr John Hemmings, May 2019, Defending Our Data: Huawei, 5G and the Five Eyes, p.9

Overview of 5G in the UK

What is 5G?

4. 5G is the next generation of wireless technology: it is a new global wireless standard being rolled out across the world and will offer faster mobile broadband connections and the ability to connect a greater number of devices online.[7] It follows previous generations of mobile technology, including 3G and 4G, which fundamentally changed the way people use mobile devices; as André Pienaar, CEO and Founder of C5 Capital, told us:

> 1G and 2G enabled voice and texts; 3G enabled us for the first time to access the internet on our phones; and then 4G and 4G LTE really created the app economy.[8]

5. David Hanke, who submitted evidence on behalf of a number of technology companies, explained that the range of services provided by mobile networks will expand dramatically in the future to encompass activities well beyond just voice and data communication.[9] Ericsson, a global telecommunications equipment vendor, suggested that 5G will enhance the Internet of Things (IoT) citing examples not only in consumer electronics but in the automotive, railway, mining, utilities, healthcare, agriculture, manufacturing and transportation sectors.[10] They explained that with "powerful, ultrareliable and ultra-low latency capabilities", 5G networks are going to enable time-critical communications.[11] TechUK, a UK technology membership organisation, concurred with this

7 Written evidence submitted by techUK (SFG0020), p1
8 André Pienaar, CEO and Founder, C5 Capital (Q4)
9 Written evidence submitted by David Hanke (SFG0021), p1
10 Written evidence submitted by Ericsson (SFG0023), p2
11 Written evidence submitted by Ericsson (SFG0023), p3

assessment, telling us that 5G is designed to support multiple, specific use cases and the value that it adds over 4G is principally in the enterprise market as it will enable optimisation of manufacturing, autonomous unloading at container ports, real time inventory and more.[12]

6. 5G networks are therefore highly sophisticated, complex systems comprised of a wide variety of hardware, software and people each performing inter-related and complex tasks.[13] Broadly speaking, they are made up of the radio access network (RAN) and the core.[14] The RAN comprises the masts, antennas and associated parts that mobile network operators (MNOs) use to connect wirelessly with mobile devices like smartphones. The core coordinates how these signals are sent and received, as well as tracking usage for billing and authentication.[15] BT Group, who run one of the UK's biggest telecoms networks, told us that the core networks handles customer-sensitive data and connect users to each other and other networks whilst the RAN (also known just as the access or the 'edge') has no decision-making capabilities and just provides access to the core network.[16] BT Group's interpretation is, however, disputed by some and they acknowledge that, when 5G reaches a level of maturity, the core-access configuration will be different than that for 3G and 4G with some of the core functions moving further out (physically) in the network (so called ' edge computing').[17] André Pienaar told us that 5G is increasingly being virtualised, through hardware being replaced by software.[18] Emily Taylor, CEO at Oxford Information Labs, added:

> 5G really changes the way that the network behaves. It embeds software into the core of the network, so that it can be much more responsive to demand. Say you have a massive event in a stadium, and many tens of thousands of people gather together at one stage. Instead of the network failing, it could scale up to support that sort of demand and then scale back down again, so it will be much more dynamic.[19]

7. In addition, it is expected that 5G will provide faster connections with much higher capacity and very fast response times (a low latency - the time between instructing a wireless device to perform an action and that action being completed), allowing many more users and devices to access fast internet connections and large amounts of data at the same time.[20] André Pienaar told us that 5G will be even more transformative than previous mobile generations

12 Written evidence submitted by techUK (SFG0020), p2; A detailed discussion of 5G technology and applications is provided in UK Parliament POST, Lorna Christie, 24 July 2019, 5G Technology
13 Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p11
14 Written evidence submitted by techUK (SFG0020), p5
15 Written evidence submitted by Telecom Infra Project (SFG0027), p2
16 Written evidence submitted by BT Group (SFG0022), p3
17 Written evidence submitted by BT Group (SFG0022), p4
18 André Pienaar, CEO and Founder, C5 Capital (Q7)
19 Emily Taylor, CEO, Oxford Information Labs (Q3)
20 House of Commons Library Briefing Paper, Georgina Hutton, 6 September 2019, 5G, p.3

as it operates on different frequency bands simultaneously which will enable much faster speeds, lower latency and the ability to connect more devices.[21] A comparison of 3G, 4G and 5G is provided below.[22]

Graphic 1: A comparison of 3G, 4G and 5G

		3G	4G	5G
	Deployment	2004-05	2006-10	2020
	Bandwidth	2mbps	200mbps	>1gbps
	Latency	100-500 milliseconds	20-30 milliseconds	<10 milliseconds
	Average Speed	144 kbps	25 mbps	200-400 mbps

5G - A step change?

8. Whilst 5G certainly represents a step change it is important to remember that the technology is in its infancy.[23] During a private briefing from Government cyber security experts we were told that the big differences between 4G and 5G, in terms of operation, are:

- A 5G network can support many more devices than 4G;
- 5G has much faster connectivity–more bandwidth and the round-trip time to go into the network (the latency) is much lower; and
- 5G allows for network segregation into slices, this allows the network to reserve 'chunks' of resources for different purposes, for example a 'chunk' for autonomous vehicles or for video calls etc.

9. Dr Ian Levy, Technical Director of the National Cyber Security Centre (NCSC), calls 5G an evolution and not a revolution, as it builds on previous iterations of mobile networks.[24] Professor Tafazolli, Director of the 5G Innovation Centre at the University of Surrey, told the Science and Technology Committee

21 André Pienaar, CEO and Founder, C5 Capital (Q4)
22 Raconteur, Heidi Vella, 15 May 2019, 5G vs 4G: what is the difference?
23 Written evidence submitted by Dr Steven Conlon (SFG0015), p1
24 National Cyber Security Centre, Dr Ian Levy, 9 March 2020, The future of telecoms in the UK

that 5G depends on the core technology that 4G has.[25] Sir Richard Dearlove, former Head of the Secret Intelligence Service, however, wrote that 4G has only limited relevance to 5G and that 5G represents a very large technology step change which will have far reaching implications for the UK's national security and almost every aspect of the country's civic life.[26]

10. The evidence we received indicated that 5G is deeply intertwined with 4G. Dr Steven Conlon, VP Corporate Intelligence at Rivada Networks, explained that early 5G networks will be built on legacy 4G LTE technologies.[27] TechUK explained that this is because the UK is deploying Non-Standalone (NSA) 5G New Radio. This means that 5G antennae make use of existing base stations that already have 2G/3G/4G on them. This approach has the benefit of an accelerated rollout and lower cost to end-users compared to other markets such as the USA which has pursued a Standalone approach. However, TechUK adds that this approach limits new entrants coming into the market as there are compatibility challenges when deploying 5G antennae that are different to the vendor for the 4G equipment.[28] Written evidence from the University of Strathclyde stated that for each site from which mobile operators intend to deploy 5G, they must use the same vendor as they use on that site for 4G, with significant deliberate "vendor lock-in".[29] Brigadier General Robert Spalding, a Senior Fellow at the Hudson Institute, told us that he favoured a standalone 5G network that is built securely, alongside existing networks rather than on top of them, because it allows you to "take a clean sheet of paper and design a secure network from the ground up".[30] Howard Watson, Chief Technology and Information Officer at BT Group, explained that through this NSA technology customers are simultaneously using both the 4G signal and the 5G signal at the same time which is known as aggregating or dual connectivity. This allows networks to take the amount of capacity of both of those and pull them together and for that reason they need the same vendor for the two technologies.[31]

5G represents a very large technology step change which will have far reaching implications for the UK's national security

25 Science and Technology Committee, Oral evidence: UK telecommunications infrastructure, HC 2200, Professor Tafazolli (Q2)
26 Sir Richard Dearlove in Henry Jackson Society, Bob Seely MP, Dr Peter Varnish OBE and Dr John Hemmings, May 2019, Defending Our Data: Huawei, 5G and the Five Eyes, p.9
27 Written evidence submitted by Dr Steven Conlon (SFG0015), p5
28 Written evidence submitted by techUK (SFG0020), p6
29 Written evidence submitted by the University of Strathclyde (SFG0019), p1
30 Brigadier General (ret.) Robert Spalding, Senior Fellow, Hudson Institute (Q97)
31 Howard Watson, Chief Technology and Information Officer, BT Group (Q262)

Threats associated with 5G

11. André Pienaar told us that 5G has very significant national security implications, and James Sullivan, Head of Cyber Research at the Royal United Services Institute, pointed out that 5G networks have inherent vulnerabilities.[32] Huawei Technologies, a Chinese vendor of telecommunications equipment at the centre of the UK's debate around the technology, told us that the threat landscape in 5G is continuously evolving.[33] On top of concerns specifically about 5G we were told by Ericsson that the wider cybersecurity environment is deteriorating, as evidenced by the large number of attacks on the UK's networks every day.[34]

12. The NCSC told us that telecoms infrastructure has, historically and at a global level, been proven to be insufficiently secure with Brigadier General Robert Spalding explaining that operators are adding 5G to what are already insecure networks in 2G, 3G and 4G.[35] The NCSC say that their analysis shows that because modern telecoms networks are highly connected, complex systems they are exposed to a range of risks.[36] They argue that addressing these endemic security flaws in telecoms network is the most fundamental challenge for the security of all networks, and particularly 5G.[37] The Department for Digital, Culture, Media and Sport's Telecoms Supply Chain Review (TSCR) acknowledges that "5G's technical characteristics create a greater surface for potential attacks."[38] The University of Strathclyde told us that there are three main risks to the UK's 5G infrastructure:

5G networks have inherent vulnerabilities

- The loss of availability of one or more mobile network, causing knock-on impact to the country and wider economy due to the inability of people to communicate;
- The inability to source "end-to-end trustworthy" components to build 5G infrastructure for a secure and resilient future; and

32 André Pienaar, CEO and Founder, C5 Capital (Q7); Written evidence submitted by James Sullivan, Head of Cyber Research, RUSI (SFG0027), p7
33 Written evidence submitted by Huawei Technologies (SFG0010), p1
34 Written evidence submitted by Ericsson (SFG0023), p6; Emily Taylor, CEO, Oxford Information Labs (Q13)
35 Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p10; Brigadier General (ret.) Robert Spalding, Senior Fellow, Hudson Institute (Q87)
36 Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p12–13
37 Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p10
38 Department for Digital, Culture, Media & Sport, July 2019, CP158, UK Telecoms Supply Chain Review Report, p4

- A targeted attack carried out to compromise the confidentiality or integrity of messages travelling over the UK's 5G networks (which could exist undetected, they argue).[39]

13. Alluding to the first point above Emily Taylor told us that reliance on the network will be significant in 5G and techUK argued that down-time for the network for whatever reason will therefore have greater consequences.[40] Dr Steven Conlon highlighted the risks of network disruption or failure:

> Disruption to 5G managed utilities such as power in a particularly cold weather period would see the loss of life. Similarly, an impact on network communications for first responders could cause serious social unrest.[41]

The University of Strathclyde told us that concerns around 5G networks, and the threat from adversaries, includes espionage, sabotage and blackmail.[42] Dr Robert Dover, Associate Professor of Intelligence and Security Studies at the University of Leicester, explained that the threats from foreign interference include direct targeting of services and infrastructure reliant on 5G, interception of critical communications, broadcasting of disinformation or signals designed to cause disruption, and societal level profiling (the widespread collection of individuals' data).[43] NCSC analysis highlighted systemic equipment failure as a risk associated with 5G where failures may not be associated with an external attack but could 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 event such as a flood or fire.[44] They cite examples of significant system failures affecting EE, Three, Telenor Norway and O2 in the last six years.[45]

14. The second risk to the UK's 5G infrastructure, the inability to source "end-to-end trustworthy" components to build 5G infrastructure, is the subject of much of this report, with significant debate having taken place over the past few years over the security of 5G vendors. TechUK told us that the increased risk to the network for a rogue or malicious device is a lot larger due to the capacity and capabilities of a 5G network.[46]

15. Whilst we have received evidence that the inclusion of HRVs such as Huawei increases the level of risk posed to the UK's 5G networks, it is important to recognise that all networks pose risks to some degree and that all vendors have potential vulnerabilities.[47] The NCSC's written evidence made clear that it

39 Written evidence submitted by James Sullivan, Head of Cyber Research, RUSI (SFG0027), p1; Written evidence submitted by the University of Strathclyde (SFG0019), p3
40 Emily Taylor, CEO, Oxford Information Labs (Q3); Written evidence submitted by techUK (SFG0020), p2
41 Written evidence submitted by Dr Steven Conlon (SFG0015), p3
42 Written evidence submitted by the University of Strathclyde (SFG0019), p1
43 Written Evidence submitted by Dr Robert Dover, University of Leicester (SFG0008), p1–2
44 Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p14
45 Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p14
46 Written evidence submitted by techUK (SFG0020), p3
47 Written evidence submitted by techUK (SFG0020), p2

assumes that any piece of equipment, anywhere, in any network, can fail, or be compromised by a hostile attacker and that it is impossible to remove risk in 5G.[48] In oral evidence, the NCSC's CEO, Ciaran Martin, told us that they do not trust any equipment as it is all vulnerable in some ways, a point which was reiterated by the Culture Secretary.[49]

James Sullivan told us that human error is a key source of vulnerabilities in 5G. He, along with Emily Taylor, explained that the software that supports 5G networks comprises millions of lines of code and that defects exist on a large scale, many of which cause vulnerabilities.[50]

16. The inability to source "end-to-end trustworthy" components is linked to the consolidated vendor market, with techUK telling us that one of the risks to 5G networks in the UK is the existing reliance on a very small number of equipment vendors.[51] Telecom Infra Project, a global community of companies and organisations working in telecoms, made the point that a more diverse market has direct security implications, as it provides greater incentives to compete on security and trust, as well as greater flexibility to MNOs. The opposite, in a consolidated market, lacks incentives for vendors to compete on security and restricts operator choice.[52]

All networks pose risks to some degree and all vendors have potential vulnerabilities

17. We discussed the third risk category, targeted attacks carried out to compromise the confidentiality or integrity of messages travelling over the UK's 5G networks, in a private session with government cyber security experts. They told us that whilst it is possible that attacks will take place undetected, operators are asked to build networks such that they would know quickly if, for example, a radio station has been compromised. They explained that there should be regular monitoring and detection and when equipment does something unexpected, remediation should be straightforward. Nevertheless, the risk remains that equipment within the 5G network could be compromised without detection, despite the mechanisms which operators and Government appear to have in place.

18. 5G will transform lives across the world by facilitating the Internet of Things. Whilst this is undoubtedly a positive development, 5G will increase our reliance on mobile connectivity, and this represents a security risk whether from 'espionage, sabotage or system failure'. Many more items

48 Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p10–11
49 Ciaran Martin, Chief Executive Officer, National Cyber Security Centre (Q223)
50 Written evidence submitted by James Sullivan, Head of Cyber Research, RUSI (SFG0027), p5; Emily Taylor, CEO, Oxford Information Labs (Q6)
51 Written evidence submitted by techUK (SFG0020), p3
52 Written evidence submitted by Telecom Infra Project (SFG0027), p3

will be connected to the internet through 5G meaning a greater surface for illicit actions. This represents a risk to individuals as well as to defence and government.

Government ambitions for the UK's 5G rollout

19. Individuals, companies and Government have recognised that the rapid and extensive rollout of 5G infrastructure is key to delivering the UK's future economic ambitions. TechUK told us that the deployment of 5G and full-fibre broadband underpins the economic transformation of the UK over the next decade.[53] BT Group highlighted the significant economic advantages offered by 5G and Huawei Technologies told us that 5G would help support the UK's development of the IoT, and make sure that the UK is well placed to benefit from the 'Fourth Industrial Revolution'.[54]

20. TechUK pointed out that the UK Government has said that it wants to be a global leader in 5G.[55] The Government's strategy for future digital infrastructure has a target that most of the population will be covered by a 5G signal by 2027.[56] In the Future Telecoms Infrastructure Review (FTIR) the Government stated an ambition to be a world leader in 5G, noting that 5G has the potential to generate "significant economic benefits from the digital transformation of many sectors".[57] The Government's policy focus, as set out in the FTIR, is to support a "market expansion model" for 5G in the UK. This means supporting a competitive market of MNOs, which the Government believes is an important driver of investment in 5G, as well as promoting innovation by new providers that could deliver "innovative solutions" to challenges such as rural coverage.[58]

Mobile network operators

21. 5G is being rolled-out by private MNOs: EE (BT), O2, Vodafone and Three. The first commercial networks went live in major UK cities in 2019. Howard Watson, from BT, told us that the UK was the second country in Europe, after Switzerland, to launch 5G.[59] Initially, 5G is expected to be deployed largely from existing 4G base stations in busy urban areas. Detailed roll-out plans of private operators are not publicly available.[60]

53 Written evidence submitted by techUK (SFG0020), p2
54 Written evidence submitted by BT Group (SFG0022), p1; Written evidence submitted by Huawei Technologies (SFG0010), p1
55 Written evidence submitted by techUK (SFG0020), p1
56 Department for Digital, Culture, Media and Sport, 23 July 2018, Future Telecoms Infrastructure Review
57 Department for Digital, Culture, Media and Sport, Future Telecoms Infrastructure Review, 23 July 2018, page 53
58 Department for Digital, Culture, Media and Sport, Future Telecoms Infrastructure Review, 23 July 2018, para 187.
59 Howard Watson, Chief Technology and Information Officer, BT Group (Q264)
60 House of Commons Library Briefing Paper, Georgina Hutton, 6 September 2019, 5G, p.3

22. MNOs procure equipment from vendors and it has been reported that each MNO in the UK has contracted the following vendors to supply their RAN:

- Vodafone: Ericsson and Huawei;[61]
- BT (EE): Huawei and Nokia;[62]
- O2: Ericsson and Nokia[63]
- Three: Huawei and Nokia.[64]

O2 reportedly used Huawei to provide 5G at a relatively small number of sites in London, where it tested the equipment before opting to purchase other suppliers' equipment.[65] Before the Government restrictions in January 2020 it was reported in the Financial Times that BT had expected to use Huawei equipment in around two-thirds of its networks, Vodafone in a significant portion of its network, and that Three, which is owned by Hong Kong based C K Hutchison, had opted to procure its RAN from Huawei only.[66] The graphic below provides a summary of BT and Vodafone's 4G and 5G networks in the UK.[67]

Graphic 2: BT and Vodafone's 4G and 5G networks

Where the Huawei technology is	
BT (EE)	**Vodafone**
4G core network (data centres)	
6 using Huawei, Nokia and Ericsson technology	**0** using Huawei **6** using Ericsso
4G base stations (masts and antenas)	
19,000 of which two thirds are Huawei	**18,000** of which one third is Huawei
5G expansion has been built on top of existing 4G technology	
5G core network EE plans to transfer all 4G and SG core networks to Ericsson by 2023	**0** using Huawci
Coverage locations **80** places with majority using Huawei	**45** places with majority using Ericsson and the rest Huawei

23. In oral evidence to the Committee, Scott Petty, Chief Technology Officer at Vodafone UK, explained that they are developing a 5G RAN on top of their 4G through a NSA mode.[68] Scott Petty told us that because Vodafone use single RAN

61 Science and Technology Committee, UK telecommunications infrastructure and the UK's domestic capability, HC 450, Written Evidence Submitted by Vodafone UK (UKT0002), p2
62 LightReading, Iain Morris, 15 April 2020, Ericsson beats Cisco and Nokia to replace Huawei in BT core
63 BBC News, Leo Kelion, 25 July 2019, O2 to launch 5G network in UK in October
64 LightReading, Iain Morris, 7 February 2019, Three UK Ditching Samsung for Huawei as It Rolls Out 5G
65 BBC News, Leo Kelion, 14 July 2020, Huawei: What does the ban mean for you?
66 Financial Times, Nic Fildes, 30 January 2020, Huawei curbs force UK telecoms groups to review 5G plans
67 The Times, Tom Knowles and Lucy Fisher, 15 July 2020, BT to keep Huawei parts in grid for emergency services
68 Scott Petty, Chief Technology Officer, Vodafone UK (Q261)

(technology that allows operators to support multiple generations of mobile networks on a single network) they are required to use the same product vendor on each base station for 2G, 3G and 4G of which Huawei represents roughly one-third of the RAN with the remainder being Ericsson. He explained that Vodafone do not use Huawei technology in the core, using a mixture of vendors including Ericsson, Nokia, Cisco and others.[69] Howard Watson of BT told us that they launched in June 2019 and are also rolling out using a NSA solution.[70] For 4G, Mr Watson explained, two-thirds of BT's network is provided by Huawei in the RAN. He added that the core for the 4G network is also provided by Huawei but that they are in the process of removing that technology from the core as they upgrade base stations from 4G to 5G. Howard Watson added that because of the existing underlying supply of the 4G equipment most of their 5G deployment so far is with Huawei, although they also have Nokia which supplies about a third of their 4G base and now is rolling out 5G too.[71]

5G will require long-term and very significant capital investment

24. It is important to remember that 5G rollouts will take a significant amount of time: André Pienaar told us that the UK is still a long way from actually implementing 5G and that it will require long-term and very significant capital investment.[72] Initial estimates suggested majority coverage by 2027 but Government restrictions are likely to have delayed this.[73]

25. We share the Government's objective that the UK remains at the forefront of the 5G rollout as we move into the next technological era. It is imperative that the UK is amongst the first countries to benefit from the technological advances that 5G will bring. *The Government's ambitions for the rollout of 5G are laudable and cybersecurity policy should take into account the strategic value of the UK maintaining its position as a global market leader in this technology.*

The UK 5G vendor market

26. As discussed briefly in the previous section, MNOs procure equipment from telecoms vendors. The TSCR notes:

69 Scott Petty, Chief Technology Officer, Vodafone UK (Q267)
70 Howard Watson, Chief Technology and Information Officer, BT Group (Q262)
71 Howard Watson, Chief Technology and Information Officer, BT Group (Q267)
72 André Pienaar, CEO and Founder, C5 Capital (Q4)
73 The Rt Hon. Oliver Dowden CBE MP, Secretary of State for Digital, Culture, Media and Sport (Q220); Department for Digital, Culture, Media and Sport, 14 July 2020, Huawei to be removed from UK 5G networks by 2027

> The lack of diversity across the telecoms supply chain creates the possibility of national dependence on single suppliers, which itself poses a range of risks to the security and resilience of UK telecoms networks.[74]

The TSCR concluded that the UK telecoms equipment market displayed sufficient vendor diversity but that ideally this diversity would be strengthened in the future. TechUK, on the other hand, described the current vendor situation as "sub-optimal".[75]

27. There are varying degrees of competition in the RAN and core of 5G, described in the TSCR.[76] In the UK there are three main scale providers of RAN: Nokia, Ericsson and Huawei.[77] Nokia is a Finnish multinational, Ericsson is a Swedish multinational telecommunications company and Huawei a Chinese multinational technology company. These three companies can provide end-to-end network equipment and supply the main UK mobile operators.[78] The NCSC said that the RAN is a high cost, low margin, hardware heavy part of the network where the problem is a lack of market diversity, arguing that the market had consolidated to the point that it had become a point of concern.[79]

28. The NCSC said that 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.[80] Brigadier General Robert Spalding told us that, globally, on the core provider side, a mix of companies have been selling to the telecom providers based on a service-based architecture.[81]

74 Department for Digital, Culture, Media & Sport, July 2019, CP158, UK Telecoms Supply Chain Review Report, p4
75 Written evidence submitted by Huawei Technologies (SFG0010), p5; Written evidence submitted by techUK (SFG0020), p1
76 Written evidence submitted by techUK (SFG0020), p6
77 Written evidence submitted by Huawei Technologies (SFG0010), p5; Written evidence submitted by techUK (SFG0020), p6
78 Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p6
79 Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p11–12, 19
80 Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p25
81 Brigadier General (ret.) Robert Spalding, Senior Fellow, Hudson Institute (Q93)

Why does the UK have a consolidated telecoms vendor market?

Dr Ian Levy from the NCSC suggests the following reasons for the UK supply market having consolidated to just three vendors of RAN:

- **Low margins**–It is difficult for manufacturers of telecoms equipment to raise margins, because operators have low margins;
- **High R&D requirements**–Telecoms infrastructure is extremely complex and bespoke with a significant investment in Research & Development required both to enter the market and to keep up with the pace of development;
- **Patents**–Telecoms technology is built on standards under which companies contributing have patented key technologies; there is thus a significant cost to new entrants to the market to pay for licenses for these key technologies (called Standard Essential Patents);
- **Spectrum & regional requirements**–Frequency usage and preferred radio technology vary around the world which means that vendors often must have slightly different products for different markets, which further adds to expense;
- **Operator confidence**–Operators are cautious by nature, given their business is built upon minimising outage and as a result, vendors must prove they can be reliable, which again puts new entrants to the market at a significant disadvantage. This also means they require a local engineering force, support structures and logistics for spares which can make it hard for existing vendors to enter a new regional market;
- **Interoperability**–While equipment is built on standards, there are often gaps or inconsistencies which mean that equipment will not necessarily connect automatically, giving the incumbent vendor an advantage. There is no incentive for vendors to interoperate with smaller vendors as it would make competition better;
- **A one-stop shop**–Creating a telecoms network requires building equipment, integrating equipment and operating the equipment. There is a division of effort between operator and vendor and, when something goes wrong, it is easier for the operator to have a single vendor who is accountable; and
- **Scale of delivery**–Selling to a major operator requires the vendor to be able to deliver a very large quantity of equipment in a short timeframe to meet the operator's plans for network rollout. Any business could grow to accommodate these demands, but such growth takes time.[82]

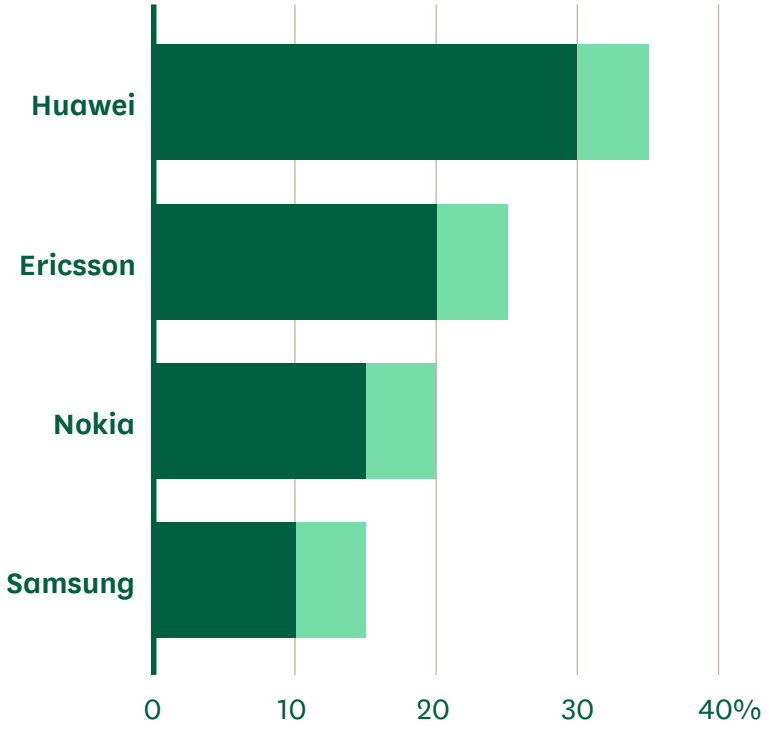
82 National Cyber Security Centre, Dr Ian Levy, 28 January 2020, The future of telecoms in the UK

29. To an extent, the UK vendor market reflects a global consolidated market. Evidence from the Telecom Infra Project highlights figures from industry analysts Analysys Mason, which calculates that the top three vendors held around 75% of the market in 2018.[83] A more recent paper commissioned by the Telecom Infra Project and produced by Heavy Reading, a telecoms research group, suggests that the top three vendors now have a combined revenue market share of approximately 80% and the market share of the top five vendors is higher than 95%.[84]

The UK vendor market reflects a global consolidated market

The Government told us that Huawei, Ericsson and Nokia dominate the global telecoms market, together with Samsung, Fujitsu, NEC, and ZTE who operate in fewer markets.[85] A graphic using data from the Wall Street Journal illustrates the estimated market shares of the top four vendors.[86]

Graphic 3: 5G radio access network world-wide market share*



*Estimated ranges

83 Written evidence submitted by Telecom Infra Project (SFG0027), p2; Analysys Mason, 11 September 2019, Radio access networks and small cells: worldwide market shares 2018

84 Heavy Reading, May 2020, TIP OpenRAN: Toward Disaggregated Mobile Networking

85 Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p6

86 The Wall Street Journal, Elizabeth Koh, 7 September 2020, Samsung, Verizon Sign $6.65 Billion 5G Contract

30. Many experts believe that vendor diversity is critical for creating secure networks and argue that it is therefore important that the Government take steps to improve the diversity of the vendor ecosystem in the UK.[87] James Sullivan explains that eliminating single points of failure and implementing back-up measures creates redundancy and thereby resilience. He adds that vendors often reuse code or components in multiple products, meaning a single problematic line of code can bring down multiple types of equipment. However, equipment from multiple vendors is extremely unlikely to all fail in the same way. Vendor diversity is therefore critical for 5G networks' resilience.[88]

31. Following the Government decision to remove Huawei from the networks by 2027 there is a risk that the three-player market in the UK for vendors will be reduced to two in the future which could increase risks around dependency.[89] James Sullivan told us that from a technical risk management perspective, reducing the number of 5G vendors by banning Huawei could actually increase the amount of overall cyber risk to 5G networks, by increasing dependency on a reduced number of vendors.[90] The NCSC told us that diversity of equipment vendors is a key factor that helps to mitigate the risk due to systemic equipment failures. In line with James Sullivan's comments above, they explain that if 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, they add, will significantly increase the risk of nationwide, systemic failure of telecoms networks.[91] The NCSC told us that they always ask operators to use two vendors in their radio networks to deliver better resilience.[92]

32. The Government has acknowledged that the lack of alternative vendors with the capacity to support the major UK MNOs represents a market failure.[93] BT Group's evidence emphasises that a more diverse and competitive supply chain would be beneficial both economically and in terms of quickening technological advances.[94]

33. It is clear that the UK vendor market for 5G kit is not diverse enough. Even with the inclusion of Huawei the market was "sub-optimal" and the Government's decision to remove Huawei completely from 5G by 2027 poses a risk that could potentially result in an even less diverse market, which could bring security and resilience concerns of its own.

87 Written evidence submitted by James Sullivan, Head of Cyber Research, RUSI (SFG0027), p2; NIS Cooperation Group, 9 October 2019, EU coordinated risk assessment of the cybersecurity of 5G networks
88 Written evidence submitted by James Sullivan, Head of Cyber Research, RUSI (SFG0027), p2
89 Written evidence submitted by Huawei Technologies (SFG0010), p2
90 Written evidence submitted by James Sullivan, Head of Cyber Research, RUSI (SFG0027), p2
91 Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p14
92 Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p25
93 Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p6
94 Written evidence submitted by BT Group (SFG0022), p5

Government restrictions on Huawei

January 2020: The conclusions of the Telecoms Supply Chain Review and initial restrictions on high-risk vendors

34. The Government conducted a comprehensive review into the telecoms supply chain, which was launched in October 2018, with initial conclusions published in July 2019.[95] The TSCR sought to answer three questions:

i. How should we incentivise telecoms operators to improve security standards and practices in 5G and full fibre networks?

ii. How should we address the security challenges posed by HRV?

iii. How can we create sustainable diversity in the telecoms supply chain?[96]

The Government announced the final conclusions of the TSCR in relation to HRVs on 28 January 2020.[97] The Government told us that the conclusions set out

95 Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p1
96 Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p3
97 Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p1

"stringent controls" that should be imposed on the use of the equipment from HRVs to ensure that risk is managed and will not impact on sensitive networks.[98] At this point the Government pledged to:

- Exclude HRV equipment from the core of the UK's 5G and full fibre networks;
- Limit HRV 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 HRV equipment remaining within our telecommunications network.[99]

Specifically, the NCSC advised that HRVs must be:

- Excluded from security critical 'core' functions of the UK's telecoms networks;
- Excluded from sensitive geographic locations;
- Limited to a minority presence of no more than 35 per cent in the edge of the network;
- Excluded from all safety related and safety critical networks in wider Critical National Infrastructure; and
- Only permitted into the UK market in accordance with a vendor-specific mitigation strategy.[100]

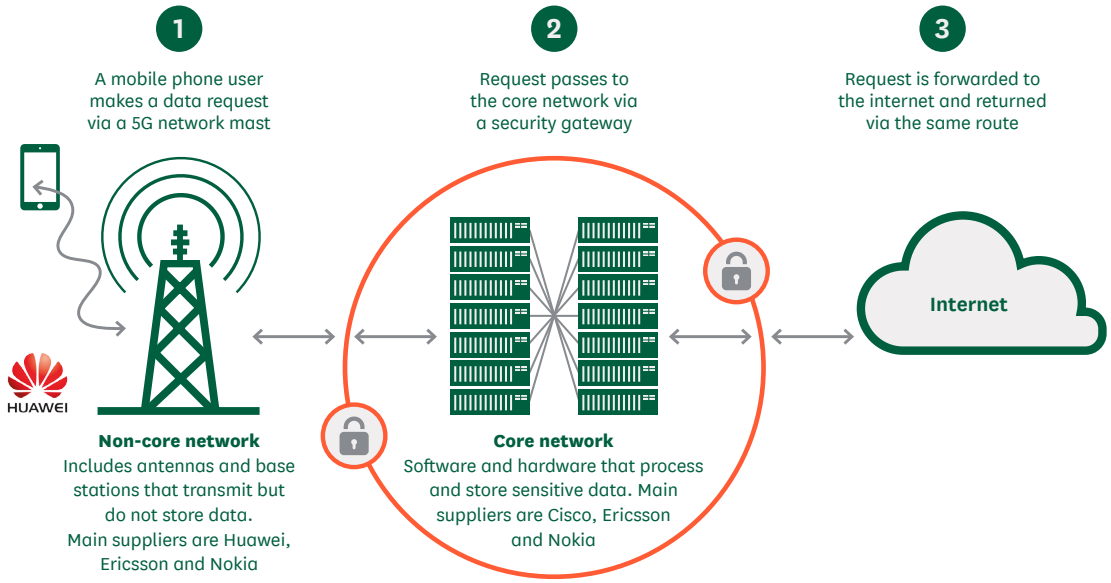
35. NCSC guidance published alongside this was clear that, within three years, all HRVs, including Huawei, should not be present in the sensitive core networks and only compose 35% of the access networks.[101] BT Group's evidence explained that for 5G this was defined as both a maximum of 35% of an operator's base stations where HRV equipment can be deployed and a maximum of 35% of network traffic to travel over HRV equipment.[102] The Government's evidence explained that this decision was based on the security advice given to it by the NCSC and that these new controls were contingent on an NCSC-approved risk mitigation strategy for any operator who chooses to use a HRV.[103] The then Culture Secretary, the Rt Honourable Baroness Morgan of Cotes, noted that the

98 Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p1
99 Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p1
100 Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p16–17
101 National Cyber Security Centre, 30 March 2020, FAQs on the NCSC's advice on the use of equipment from high risk vendors in UK telecoms networks
102 Written evidence submitted by BT Group (SFG0022), p3
103 Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p1; 4

recommended cap of 35 per cent will be kept under review to determine whether it should be further reduced as the market diversifies.[104] Under these restrictions Huawei's role in the UK's 5G networks is illustrated below.[105]

Graphic 4: Huawei's role under January 2020 restrictions

Chinese company can only supply 'non-core' kit



36. We received conflicting evidence on the feasibility of the Government's plan announced in January to exclude Huawei technology from the most sensitive parts of the UK's 5G network while allowing it to supply peripheral components, with a dispute focusing on whether there remains a distinction between the core and 'edge' (the RAN) in 5G.

37. On the one hand, some argue that 5G's ultra-low latency will mean communication will have to take place at the edge of the network and therefore the distinction between a 'dumb' edge and 'smart' core no longer remains.[106] On the other hand, Huawei Technologies argued that whilst it is true that core networks will be bigger and closer to the end user for 5G, there will still be a clear distinction between a user accessing the network through a mobile mast or small cell, and the centralised management of the network for different regions of the

The USA's technical experts along with those in Australia and Japan disagree with the NCSC's position

104 UK Government, 28 January 2020, Baroness Morgan's Written Ministerial Statement to the House of Lords on UK Telecommunications

105 Financial Times, George Parker, Helen Warrell and Kiran Stacey, 28 January 2020, Huawei decision jolts UK-US 'special relationship' at sensitive time

106 Written evidence submitted by The Scotland 5G Centre (SFG0024), p2; Written evidence submitted by Dr Robert Spalding (SFG0001), p1; Written Evidence submitted by Dr Robert Dover, University of Leicester (SFG0008), p2; Written evidence submitted by Mr Declan James Ganley (SFG0013), p1; Written evidence submitted by Dr Steven Conlon (SFG0015), p5 and Written evidence submitted by David Hanke (SFG0021), p1

country.[107] Other evidence also argued that the distinction remained and it is clear that this was the view of the Government and agencies.[108] Dr Ian Levy argued that despite the fact that sensitive functions are more dispersed in 5G networks, it is still possible to group and separate them accurately.[109] The Government's written evidence stated that it is both possible and desirable to exclude HRVs from the most sensitive functions and restrict them to less critical functions.[110]

It was clear that the view of some allies contrasted with that of the UK Government. Senator Tom Cotton, United States Senator for Arkansas, told us that the USA's technical experts along with those in Australia and Japan disagree with the NCSC's position.[111] Robert Strayer, the top cybersecurity official at the US State Department, told the Henry Jackson Society in June that the US rejected any distinction between the core and edge in 5G.[112]

38. On the 35% figure, Emily Taylor told us that she understood that the figure was quite close to Huawei's current market share, an assessment which André Pienaar agreed.[113] The NCSC explained to us that this figure was a judgement and not a scientific calculation. They argue that it ensures that the UK will not become nationally dependent on any vendor, especially a HRV, while retaining competition in the market and allowing operators to continue to use two RAN vendors.[114] The CEO of the NCSC told us that the 35% is not just a 'target' and that if the Telecoms Security Bill passes this would be a strict, legally binding limit, consistent with the risk analysis of the NCSC.[115]

39. BT labelled the conclusions of the TSCR as "proportionate and evidence-based". In 2018, BT said it would remove Huawei equipment from its core networks within two years (2020) but in April this year, BT stated that "100% of core mobile traffic" will be on its new Ericsson-built equipment by 2023, this is compliant with the Government's deadline, but is three years later than BT had originally proposed.[116] Making the announcement, BT said that the delay was due to the extra resources required to comply with the Government's direction to reduce Huawei's market share in the RAN.[117] In evidence to the Committee, Howard Watson said it would cost BT £500 million to meet that requirement by

107 Written evidence submitted by Huawei Technologies (SFG0010), p3
108 Written evidence submitted by BT Group (SFG0022), p3; Written evidence submitted by James Sullivan, Head of Cyber Research, RUSI (SFG0027), p1; Written evidence submitted by Professor J A McDermid, University of York (SFG0025), p1
109 National Cyber Security Centre, Dr Ian Levy, 22 February 2019, Security, complexity and Huawei; protecting the UK's telecoms networks
110 Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p6
111 Senator Tom Cotton, United States Senate (Q48)
112 The Times, Lucy Fisher, 22 June 2019, GCHQ hits back at US official over Huawei security claims
113 Emily Taylor, CEO, Oxford Information Labs (Q22); André Pienaar, CEO and Founder, C5 Capital (Q23)
114 Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p19
115 Ciaran Martin, Chief Executive Officer, National Cyber Security Centre (Q193)
116 Financial Times, Nic Fildes, 15 April 2020, BT delays Huawei strip out despite signing Ericsson deal
117 The Times, Tom Knowles, 17 April 2020, We can't remove Huawei kit until 2023, admits BT; BBC News, 15 April 2020, BT delays removal of Huawei from EE's core network by two years

January 2023.[118] Scott Petty told us that for Vodafone they were supportive of these restrictions and did not feel that it would have any material impacts on their network either financially or from a deployment point of view.[119] The Culture Secretary told us that the Government think the impact of these restrictions will be roughly £1.5 billion with about a year-long delay.[120]

40. The response to the decision from the United States was negative. Following the announcement in January, Senator Tom Cotton told us that his reaction was similar to that of the US Government in that the announcement disappointed him and that he hoped the UK Government "refines its decision, if it does not reverse it outright".[121] 42 US lawmakers wrote to the House of Commons Defence Committee and Foreign Affairs Committee urging a reversal of the decision to allow Huawei in the UK's 5G network.[122]

The response to the decision from the United States was negative

41. Despite pressure for a complete removal of Huawei, the NCSC told us that the case for complete exclusion of Huawei could not be made on cyber security grounds alone.[123] It was clear that in January this was intended to be the final decision on the inclusion of HRVs in the 5G networks. However, in the following months geopolitics had an impact on the technical considerations surrounding Huawei's viability.

May 2020: US sanctions against Huawei

42. Concerns around supply chain viability led to further restrictions announced on Huawei equipment in July of this year and these were a response to US sanctions announced in May 2020.[124]

43. On 15 May 2020, the U.S. Department of Commerce outlined plans to "protect U.S. national security" by restricting Huawei's ability to use U.S. technology and software to design and manufacture its semiconductors abroad.[125] Under the rules, a US government licence is required to sell to Huawei any semiconductors made abroad with American technology which

118 Howard Watson, Chief Technology and Information Officer, BT Group (Q269)
119 Scott Petty, Chief Technology Officer, Vodafone UK (Q270)
120 The Rt Hon. Oliver Dowden CBE MP, Secretary of State for Digital, Culture, Media and Sport (Q220)
121 Senator Tom Cotton, United States Senate (Q82)
122 C4ISRNET, Joe Gould, 4 February 2020, Huawei: 42 US lawmakers urge UK Parliament to reject 'dangerous' 5G decision
123 Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p26
124 Ciaran Martin, Chief Executive Officer, National Cyber Security Centre (Q214)
125 Financial Times, James Politi and Kiran Stacey, 15 May 2020, US escalates China tensions with tighter Huawei controls; U.S. Department of Commerce, 15 May 2020, Commerce Addresses Huawei's Efforts to Undermine Entity List, Restricts Products Designed and Produced with U.S. Technologies

therefore blocks global chip supplies to Huawei.[126] Ciaran Martin explained that the sanctions impact on Huawei's products as they are "targeted at Huawei's future ability to source hardware, particularly chips and things that would more affect 5G".[127] Ciaran Martin told us that once the sanctions in May 2020 were announced the NCSC viewed it instantly as "potentially a material change in the facts".[128]

44. Just over a week later, on 24 May 2020 the Government announced that it was launching a fresh review into allowing Huawei telecoms equipment to be used in 5G networks.[129] Gordan Corera, security correspondent at the BBC, wrote:

> Even though this review is based on the technical considerations about the impact of US sanctions, it could potentially offer the government a route to move away from its earlier decision and exclude the company or impose further limits - although that may involve economic costs at home and increased tension with Beijing.[130]

Government cyber security experts told us that the May 2020 sanctions removed the ability of Huawei specifically to use US technology to either design or manufacture their own chips. The semiconductor industry relies on a type of software known as electronic design automation (EDA) and, as outlined by Leo Kelion, technology desk editor at the BBC, the problem for Huawei is that the three leading EDA software-makers all have ties to the US. The sanctions forbid Huawei, and the third parties that manufacture its chips, from using "US technology and software to design and manufacture" its products.[131] The government's experts told us that this meant Huawei can no longer use existing EDA tools to make technology.

45. Whilst the Financial Times reported that Huawei had secured up to two years of supplies of "the most essential components" the Culture Secretary told us at the end of June that the sanctions were "likely to have an impact on the viability of Huawei as a provider for the 5G network".[132]

126 The Times, Lucy Fisher, New inquiry into security risk posed by Huawei technology
127 Ciaran Martin, Chief Executive Officer, National Cyber Security Centre (Q214)
128 Ciaran Martin, Chief Executive Officer, National Cyber Security Centre (Q214)
129 BBC News, Mary-Ann Russon, 24 May 2020, Fresh UK review into Huawei role in 5G networks
130 BBC News, Mary-Ann Russon, 24 May 2020, Fresh UK review into Huawei role in 5G networks
131 BBC News, Leo Kelion, 25 June 2020, Why Huawei's days in the UK could be numbered
132 Financial Times, Lauly Li and Cheng Ting-Fang, 8 June 2020, Huawei builds up 2-year reserve of 'most essential' US chips; The Rt Hon. Oliver Dowden CBE MP, Secretary of State for Digital, Culture, Media and Sport (Q188)

July 2020: The banning of the purchase of Huawei equipment from 2021 and Huawei's removal from 5G by 2027

46. On 14 July 2020 the Secretary of State for Digital, Culture, Media and Sport made a statement to the House of Commons announcing an update to the restrictions placed on Huawei in UK networks, with important changes in that operators will be banned from buying any 5G equipment from Huawei from 31 December 2020 and with a timetable announced for the removal of Huawei from 5G networks by 2027.[133]

Removal of Huawei from 5G networks by 2027

The Rt Hon Oliver Dowden MP concluded that the US sanctions created uncertainty around Huawei's supply chain and that the UK could no longer be confident it would be able to guarantee the security of future Huawei 5G equipment. The Government clarified that the existing ban on Huawei from the most sensitive 'core' part of 5G networks, announced in January, remained.[134] He acknowledged that this decision would delay the rollout of 5G and increase costs:

> Today's decision to ban the procurement of new Huawei 5G equipment from the end of this year will delay rollout by a further year and will add up to half a billion to the costs. Requiring operators, in addition, to remove Huawei equipment from their 5G networks by 2027 will add hundreds of millions to the cost and further delay roll out. This means a cumulative delay to 5G rollout of two to three years and costs of up to two billion pounds.[135]

47. Network providers such as BT and Vodafone had previously expressed concern about banning Huawei from the network, citing the significant economic costs of a ban and potential delays to 5G roll-out. For instance, Vodafone commented:

> A partial to full restriction on Huawei in the telecoms supply chain could result in an 18–24-month delay to the widespread availability of 5G in the UK. This would result in the UK failing to be a world leader in 5G–something that has been central to the UK government's 5G strategy.

133 Department for Digital, Culture, Media and Sport, 14 July 2020, Digital, Culture, Media and Sport Secretary's statement on telecoms
134 Department for Digital, Culture, Media and Sport, 14 July 2020, Huawei to be removed from UK 5G networks by 2027
135 Department for Digital, Culture, Media and Sport, 14 July 2020, Digital, Culture, Media and Sport Secretary's statement on telecoms

> Using the government's own estimates on the benefits of 5G, the cost to the UK economy of a delay in rollout is calculated at between £4.5bn and £6.8bn.
>
> As well as the measurable financial impact, the UK will also suffer in terms of lower inward investment and lost productivity gains through stagnation of digital infrastructure.[136]

48. In February Enders Analysis, a technology research company, estimated that a full ban would cost BT, Vodafone and Three a total of about £1.5 billion, with BT facing the majority "as it is by far the biggest user of Huawei for 4G and it would have to strip these out and replace them to put in 5G equipment from another supplier".[137] James Barford, a telecoms analyst at Enders Analysis, is quoted in the Times as saying that "The overall delay might be around 18 to 24 months, at significant cost to the UK mobile consumer and wider economy".[138] It is worth noting, however, that Ericsson reportedly disagrees with this analysis and the costs mentioned above.[139]

49. Following the announcement BT issued a brief press release outlining its initial assessment of the revised policy:

> BT currently estimates that full compliance with these revised proposals would require additional activity, both in removing and replacing Huawei equipment from BT's existing mobile network, and in excluding Huawei from the 5G network that BT continues to build. However, now we have clarity on the timing, it is estimated that these costs can be absorbed within BT's initial estimated implementation cost of £500m, as announced by BT on 30 January 2020 in order to comply with the previous proposal by the NCSC.[140]

Scott Petty told us that as Vodafone deploy their 5G base stations they will need to swap out Huawei 4G base stations to an alternate vendor. This would create both disruption in the network and an incremental cost for their 5G deployment plans.[141]

50. The international response to the decision was predictably mixed. China's ambassador to the UK, Ambassador Liu Xiaoming, said the decision was "disappointing and wrong" and that "it has become questionable whether the UK can provide an open, fair and non-discriminatory business environment for companies from other countries".[142] But US Secretary of State Mike Pompeo

136 Written evidence submitted by Vodafone UK (UKT0002)
137 The Telegraph, James Cook, 12 June 2020, UK plan for 2023 Huawei cut-off is 'impractical' and could cost £1.5bn
138 The Times, Alex Ralph, 10 February 2020, Full Huawei ban 'could cost phone firms £1.5bn'
139 The Telegraph, James Cook and Christopher Williams, 11 July 2020, Ericsson says £2bn price tag to remove Huawei is a 'myth'
140 BT Group, 14 July 2020, BT's initial assessment of revised policy on Huawei in 5G networks
141 Scott Petty, Chief Technology Officer, Vodafone UK (Q271)
142 Lui Xiaoming, Chinese Ambassador to the UK, 14 July 2020, Tweet

welcomed the news, saying: "the UK joins a growing list of countries from around the world that are standing up for their national security by prohibiting the use of untrusted, high-risk vendors."[143]

51. It is fair to say the Government's policy on 5G has been shaped by a number of factors and has been impacted by geopolitics as well as technical considerations.[144]

52. This inquiry was launched in the context of a lively debate on the security of the UK's 5G network in Parliament and across the country from late 2019 and through 2020 with a focus on the presence in our network of high-risk vendors, particularly Huawei. A significant Government announcement took place in January with restrictions placed on high-risk vendors followed by stricter rules announced in July, with Huawei to be removed from the UK's 5G network by 2027. The UK Government has had to balance technical considerations with wider geopolitical considerations when formulating its 5G policy.

143 BBC News, Leo Kelion, 14 July 2020, Huawei 5G kit must be removed from UK by 2027
144 BBC News, Gordon Corera, 13 July 2020, Huawei: UK prepares to change course on 5G kit supplier

Technical Considerations

Cyber attacks

53. The role of the NCSC is to provide objective, expert technical advice on cyber security risk and through it the UK has a world-leading independent authority and an internationally recognised centre of excellence which has a deep understanding of the UK's mobile networks.[145] The NCSC told us whilst 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 digital attacks, including cyber-attack from both highly sophisticated and less sophisticated actors.[146]

54. The Government told us that they have assessed Cyber as a Tier 1 threat to the UK, and that defending the UK against cyber threats will remain a core aspect of its cyber capability.[147] The NCSC told us that the most obvious class of risk to a telecoms network is a cyber-attack from an external entity. If successful, they add, such an attack could give the attacker a capability to perform espionage or to disrupt the operation of the network.[148] They explain

Cyber is a tier 1 threat to the UK

145 Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p10; Written evidence submitted by techUK (SFG0020), p4; André Pienaar, CEO and Founder, C5 Capital (Q43)

146 Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p11

147 Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p8

148 Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p13

that attackers are able to penetrate target networks because of exploitable vulnerabilities caused by poor network design or operational practice in the operators concerned. The NCSC cite previous attacks which did not need to take advantage of pre-placed vulnerabilities in the equipment, or human agents working within the operators and were purely a result of poor network security, but add that this is not to say that human agents and pre-placed vulnerabilities are not useful to an attacker.[149] The NCSC said that there is a range of state and non-state actors targeting global telecoms systems.[150] The University of Strathclyde cite research, outlined in the Journal of Strategic Studies, that cyber espionage is the most common type of state sponsored cyber operations.[151]

55. Emily Taylor told us Russia had conducted cyber-attacks on the UK's mobile infrastructure and the NCSC cite the example of the Government publicly attributing a successful attack on a UK telecoms network to the Russian state, which the NCSC describe as "a highly sophisticated cyber actor".[152]

56. Additionally, John W Strand, CEO of Strand Consult, told us that China is responsible for the greatest number of cyberattacks by any nation over the past dozen years.[153] He suggested that the Chinese Government is deeply involved in hacking and cyberattacks and that "China's 100,000 hackers are part of its military and attack foreign targets of all kinds at the behest of the Chinese government".[154] André Pienaar also told us that the Chinese state has and will continue to carry out cyber-attacks against the UK with these cyber-attacks including advanced surveillance to collect information about key individuals, the theft of intellectual property on an "unprecedented scale" and, in certain instances, the prepositioning of cyber weapons (within software) for possible future use on networks.[155] Congressman Mike Turner, a member of the U.S. House of Representatives from Ohio, told us that China has been very active in hacking both the United States and the UK, stating that it seeks personal information on our citizenry and those who serve in Government.[156] The University of Strathclyde cited research that shows that out of a total 266 publicly known cyber incidents

149 Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p13–14
150 Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p13
151 Written evidence submitted by the University of Strathclyde (SFG0019), p3; Journal of Strategic Studies, 2012, Vol. 35 (1): 5 -32, Thomas Rid, Cyber War Will Not Take Place; Brandon Valeriano and Ryan C Maness. 2015. Cyber War versus Cyber Realities: Cyber Conflict in the International System. Oxford: Oxford University Press
152 Emily Taylor, CEO, Oxford Information Labs (Q13); Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p12; National Cyber Security Centre, 15 April 2018, Russian state-sponsored cyber actors targeting network infrastructure devices
153 Written evidence submitted by John W Strand (SFG0016), p5
154 Written evidence submitted by John W Strand (SFG0016), p4
155 André Pienaar, CEO and Founder, C5 Capital (Q16)
156 Congressman Mike Turner, US House of Representatives (Q109)

between rival states from 2000 to 2015, 74 (28%) were initiated by China.[157] According to another database, they add, 140 out of 390 (36%) cyber incidents since 2005 were conducted or sponsored by the Chinese government.[158]

Whilst Government evidence did not implicate China in direct attacks on the networks in the UK, the NCSC told us that the Government was part of an international coalition including 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.[159] They told us that in this campaign, actors associated with the Chinese Ministry of State Security, known as APT10, had compromised several companies whose onward contracts and connections gave the attackers control over their customers' networks.[160] During a private briefing with government cyber security experts we were told that Chinese state cyberattacks have been tracked by security services for a long time and, whilst they are prolific and competent, the UK is well prepared for these attacks.

57. The Defence Secretary, the Rt Hon Ben Wallace MP, pointed out that the Chinese have been named on a number of occasions for using cyberattacks against the UK and its allies.[161] He later added that China has on a regular basis, engaged in cyber-espionage, in the same way Russia and North Korea have.[162] Franklin C. Miller, Principal of The Scowcroft Group, told us that the West needs to raise concerns persistently on the international stage about cyberattacks and malpractice by foreign powers.[163] The Defence Secretary told us that the UK, along with allies, call out the culprits to make an example of them or embarrass them in front of an international community.[164] Franklin C. Miller also explained that there needs to be a deterrent as at the moment Russia, China and North Korea are doing this without cost.[165] A Ministry of Defence statement acknowledged this stating that global players such as Russia and China are operating in the "expanding grey zone between war and peacetime" in domains such as cyber.[166]

China has, on a regular basis, engaged in cyber-espionage

157 Written evidence submitted by the University of Strathclyde (SFG0019), p3; Journal of Strategic Studies, 2012, Vol. 35 (1): 5 -32, Thomas Rid, Cyber War Will Not Take Place; Brandon Valeriano and Ryan C Maness. 2015. Cyber War versus Cyber Realities: Cyber Conflict in the International System. Oxford: Oxford University Press
158 Council on Foreign Relations, Cyber Operations Tracker
159 National Cyber Security Centre, 20 December 2018, APT10 continuing to target UK organisations
160 Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p15
161 The Rt Hon. Ben Wallace MP, Secretary of State for Defence (Q242)
162 The Rt Hon. Ben Wallace MP, Secretary of State for Defence (Q248)
163 Franklin C. Miller, Principal, Scowcroft Group (Q162)
164 The Rt Hon. Ben Wallace MP, Secretary of State for Defence (Q254)
165 Franklin C. Miller, Principal, Scowcroft Group (Q162)
166 Ministry of Defence, 13 September 2020, Chief of Defence Intelligence comments on threats the UK will face in coming decades

58. There is evidence that the UK, and our allies, face many malicious cyber-attacks both from rogue individuals and state-sponsored attacks from states such as Russia and China. These attacks are diverse in their nature and in their aims. Some attacks aim to steal individual data and state secrets whilst others seek to bring down the network in its entirety.

59. It is important that the Government continues to call out cyber-attacks from adversaries on the international stage and works to find a deterrent to counter them. *There is currently a lack of global rules regulating international cyber-attacks and the Government should work with allies to formulate a system to provide accountability for perpetrators. The Government should clarify why it is not deploying a cyberattack capability to deter aggressors.*

The security of Huawei's products

60. James Sullivan told us that the NCSC designated Huawei a HRV based on the following criteria:

- A vendor's strategic position in the UK and in other telecommunications networks;
- Quality and transparency of the vendor's engineering and cyber security;
- Past behaviour and practices;
- Vendor resilience;
- Domestic state apparatus, laws and offensive cyber capabilities of the vendor's country of origin.[167]

61. Specifically, the NCSC concerns include:

- As a Chinese company Huawei could, under China's National Intelligence Law of 2017, be ordered to act in a way that is harmful to the UK;
- The Chinese State (and associated actors) have carried out and will continue to carry out cyber-attacks against the UK and its interests;
- Huawei's cybersecurity and engineering quality is low and its processes opaque. For example, the Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board raised significant concerns in 2018 about Huawei's engineering processes. Its 2019 report confirmed that "no material progress" had been made by

167 Written evidence submitted by James Sullivan, Head of Cyber Research, RUSI (SFG0027), p5–6

Huawei in the remediation of technical issues reported in the 2018 report and highlighted "further significant technical issues" that had not previously been identified; and

- Many Huawei entities (companies owned or closely linked with Huawei) are currently included on the US Entity List. Although the NCSC do not know whether these entities will remain on the US Entity List, they explain that this listing may have a potential impact on the future availability and reliability of Huawei's products.[168]

62. The Government's written evidence told us that HRVs are those which pose greater security and resilience risks to UK telecoms and said it regards Huawei as a HRV.[169] TechUK told us that HRVs require additional and bespoke mitigation strategies, which are in place for Huawei's products.[170] The UK's security services, along with the cyber security functions of telecommunications operators, have been operating with bespoke mitigation strategy for HRVs for over a decade.[171]

63. The HCSEC, mentioned in government evidence above, provides specific mitigation of risks arising from Huawei's involvement in the UK.[172] Dr Steven Conlon notes that the UK is home to the world's experts on Huawei due to the HCSEC and evidence from the BT Group argues that the UK, via the HCSEC, leads the world in its ability to understand, analyse and assure the quality and integrity of Huawei's hardware and software.[173] The HCSEC Oversight Board has operated since 2010 under a set of arrangements between Huawei and the UK Government and raised significant concerns in 2018 about Huawei's engineering processes. Its 2019 report confirmed that "no material progress" had been made by Huawei in the remediation of technical issues reported in the 2018 report and highlighted "further significant technical issues" that had not previously been identified and lead to new risks in the UK telecommunications network.[174] Overall, the 2019 report stated that:

> The Oversight Board can only provide limited assurance that all risks to UK national security from Huawei's involvement in the UK's critical networks can be sufficiently mitigated long-term.[175]

168 National Cyber Security Centre, January 2020, NCSC advice on the use of equipment from high risk vendors in UK telecoms networks
169 Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p3
170 Written evidence submitted by techUK (SFG0020), p2
171 Written evidence submitted by techUK (SFG0020), p5
172 Written evidence submitted by Huawei Technologies (SFG0010), p3
173 Written evidence submitted by Dr Steven Conlon (SFG0015), p11; Written evidence submitted by BT Group (SFG0022), p1
174 Huawei Cyber Security Evaluation Centre Oversight Board, March 2019, Annual Report: A report to the National Security Advisor of the United Kingdom
175 Huawei Cyber Security Evaluation Centre Oversight Board, March 2019, Annual Report: A report to the National Security Advisor of the United Kingdom

64. Government evidence told us that they have always considered Huawei to present higher risk and have developed a bespoke risk mitigation strategy to risk-manage their presence since they first came to the UK in 2003. They told us that the HCSEC 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.[176] A number of experts highlighted HCSEC reports as evidence of Huawei's technical vulnerabilities.[177] The NCSC told us that the main class of risk that is associated with Huawei is the insertion of 'backdoors' or malicious functionality and that there are several ways in which such functionality can be inserted into a product:

Huawei's general practice of security is objectively lower

i. 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 the NCSC have not seen any specific evidence in respect of the UK, given its close relationship with the Chinese state, this scenario is their standing assumption since Huawei entered the UK market in 2003.

ii. The company itself is not malicious or operating under direction from an external party, but people working within 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 the NCSC's standing assumption for all vendors, and they told us that they have been involved in cases where this type of activity has been discovered.

iii. 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 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). Again, the possibility of this happening is the NCSC's standing assumption for all vendors.[178]

176 Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p4

177 Written evidence submitted by Prof. Christopher Balding, Associate Professor, Fulbright University and an Associate Fellow at the Henry Jackson Society (SFG0012), p4; Written evidence submitted by Dr Steven Conlon (SFG0015), p1, 2, 6; Emily Taylor, CEO, Oxford Information Labs (Q9)

178 Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p14–15

The CEO of the NCSC told us that the oversight board reports reveal that Huawei's general practice of security is objectively lower at present than their main competitor. He said that they are objectively weaker in general standards but added that evidence of poor engineering and security practice does not constitute direct evidence of deliberate insertion of "backdoors" by the Chinese state.[179]

65. Huawei Technologies argue that the HCSEC offers unprecedented levels of scrutiny and oversight on Huawei relative to other vendors.[180] Huawei Technologies' written evidence argues that the security of networks will not be high until all vendors are subject to a level of scrutiny similar to that placed upon Huawei. They suggest that this could potentially be exercised through the National Telecommunications Laboratory proposed by the Government, so that the performance of all network equipment can be properly assessed.[181]

66. Whilst BT Group's evidence told us that Huawei has invested significantly in 5G RAN technology and, as such, has taken a leadership position, others have told us that Huawei equipment is not a market leader and is of low-quality.[182] The NCSC does not believe that Huawei's equipment is in a leadership position and in its view, Nokia, Ericsson and Huawei are all in broadly the same position in terms of maturity, given the maturity of standards, and functionality of 5G provision to operators.[183] André Pienaar and Emily Taylor told us that Huawei is not an intellectual leader but is instead attractive due to its price.[184]

67. There is no doubt that Huawei's designation as a high-risk vendor is justified. The Huawei Cyber Security Evaluation Centre has consistently reported on its low-quality products and concerning approach to software development, which has resulted in increased risk to UK operators and networks. The presence of Huawei in the UK's 5G networks therefore poses a significant security risk to individuals and to our Government. Whilst Huawei is a market leading company, we do not believe it to be higher in quality or more functional than its rivals, Nokia and Ericsson.

68. The establishment of the Huawei Cyber Security Evaluation Centre has resulted in the UK leading the world in understanding Huawei's equipment. *Despite the planned withdrawal of Huawei from our 5G networks, the Huawei Cyber Security Evaluation Centre should continue to operate to assess Huawei equipment in other areas of our telecommunications. The Government should consider assessing all equipment vendors in a similar fashion, given the vulnerabilities of all equipment.*

179 Ciaran Martin, Chief Executive Officer, National Cyber Security Centre (Q222)
180 Written evidence submitted by Huawei Technologies (SFG0010), p3
181 Written evidence submitted by Huawei Technologies (SFG0010), p3
182 Written evidence submitted by BT Group (SFG0022), p5; André Pienaar, CEO and Founder, C5 Capital and Emily Taylor, CEO, Oxford Information Labs (Q31)
183 Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p25
184 André Pienaar, CEO and Founder, C5 Capital and Emily Taylor, CEO, Oxford Information Labs (Q31)

Network security and Huawei's involvement

69. Huawei Technologies claims that "experts at the NCSC have been clear on public record that this package of measures [the January restrictions on HRVs] satisfies them that potential risks have been properly mitigated."[185] James Sullivan believes that from an evidence-based, technical risk management perspective, the UK's initial 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 was practical and realistic.[186] Emily Taylor agreed with this assessment labelling it evidence-based and cautious.[187]

70. The Government told us that the decision on HRVs in UK telecoms networks was based first and foremost on the security advice of the NCSC.[188] Despite pressure from many for a complete removal of Huawei, the NCSC told us that the case for complete exclusion of Huawei could not be made on cyber security grounds alone.[189]

71. James Sullivan told us that from a technical risk management perspective, reducing the number of 5G vendors by banning Huawei at this point could have actually increased the amount of overall cyber risk to 5G networks.[190] The NCSC told us that equipment (vendor) diversity is a key factor that helps to mitigate the risk due to systemic equipment failures. They explain that if one vendor fails, the impact will necessarily be reduced if there is a greater variety of unaffected equipment from other vendors.[191] James Sullivan explains that equipment from multiple vendors is extremely unlikely to all fail in the same way and vendor diversity is therefore critical for 5G networks' resilience.[192] Having very low diversity in the market, such as one or two vendors, the NCSC adds, will significantly increase the risk of nationwide, systemic failure of telecoms networks.[193]

72. Advice to Government was clear, that the presence of Huawei in the UK's networks was a manageable risk. The UK has one of the most active and effective cyber-security regimes in the world, and, from our public and

185 Written evidence submitted by Huawei Technologies (SFG0010), p2
186 Written evidence submitted by James Sullivan, Head of Cyber Research, RUSI (SFG0027), p1
187 Emily Taylor, CEO, Oxford Information Labs (Q42)
188 Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p7
189 Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p26
190 Written evidence submitted by James Sullivan, Head of Cyber Research, RUSI (SFG0027), p2
191 Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p14
192 Written evidence submitted by James Sullivan, Head of Cyber Research, RUSI (SFG0027), p2
193 Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p14

private conversations with Government, we are confident that GCHQ and the NCSC are able to appropriately manage any increased risk posed by the presence of Huawei or other high-risk vendors in the UK's 5G.

73. Furthermore, whilst the risk remained manageable, it is important to remember the benefits in having a greater number of vendors involved in 5G network provision, despite the designation as high-risk, as this improves overall network resilience should a single vendor fail.

Why the restrictions on Huawei had to change - the US sanctions

74. We have already described the US sanctions against Huawei announced in May 2020. Ciaran Martin told us that these sanctions targeted Huawei's future ability to source hardware, particularly chips and he explained that once the sanctions were announced, the NCSC viewed it as "potentially a material change in the facts".[194]

75. Government cyber security experts told us that the May 2020 sanctions remove the ability of Huawei specifically to use US technology to either design or manufacture their own chips: the Culture Secretary told us that the sanctions were "likely to have an impact on the viability of Huawei as a provider for the 5G network".[195] The NCSC reportedly believed it could no longer assure the security of Huawei's products as Huawei faced having to source other companies' chips for use in its equipment.[196] This was confirmed when the Culture Secretary announced to the House of Commons:

> The NCSC has now reported to ministers that they have significantly changed their security assessment of Huawei's presence in the UK 5G network.[197]

76. The restrictions meant that Huawei could no longer source its chips from reputable manufacturers or use reputable equipment in its manufacturing processes. This meant that the NCSC felt they could no longer adequately scrutinise Huawei's supply chain and guarantee its security.

77. Prior to the US sanctions announced in May, the risk of Huawei products remaining in the UK's 5G networks was, according to the Government, significant but manageable through monitoring and regulation. The situation changed when Huawei was deprived of reliable chip manufacturing

194 Ciaran Martin, Chief Executive Officer, National Cyber Security Centre (Q214)
195 Financial Times, Lauly Li and Cheng Ting-Fang, 8 June 2020, Huawei builds up 2-year reserve of 'most essential' US chips; The Rt Hon. Oliver Dowden CBE MP, Secretary of State for Digital, Culture, Media and Sport (Q188)
196 BBC News, Leo Kelion, 9 July 2020, 'UK faces mobile blackouts if Huawei 5G ban imposed by 2023'
197 Department for Digital, Culture, Media and Sport, 14 July 2020, Digital, Culture, Media and Sport Secretary's statement on telecoms

capabilities. Following these sanctions, as discussed in the Government's July announcement, it became much more difficult to guarantee and measure the quality of Huawei products. In principle, the Government has made the correct technical decision to ban the purchase and presence of Huawei products in the future.

5G in Defence and National Security

78. André Pienaar told us that Huawei equipment should not make its way into the critical aspects of our national defence and security infrastructure.[198] Senator Tom Cotton told us that the introduction of Huawei technology into the UK's 5G network could impact on the ability to share the most sensitive intelligence with Congressman Mike Turner telling us that Huawei's presence in the UK's network could threaten the ability to use or share information, for example between the US and UK concerning China's intent and its operations.[199]

79. Evidence from the University of Strathclyde, however, argues that it is important to remember that that the UK's public mobile networks are the issue so far as Huawei are concerned, not the dedicated military communications networks, and that, when acting internationally, the military use other communications techniques which are not part of the regular public commercial telecoms networks.[200] We have been told consistently that there is no Huawei or HRV equipment in sensitive networks or sensitive sites.[201] The Defence Secretary said:

We have been told consistently that there is no Huawei or HRV equipment in sensitive networks or sensitive sites

> I can give you the assurance that, on our sensitive sites and in our secure networks, there is no Huawei equipment.[202]

80. The CEO of the NCSC told us that there are no national security capability dependencies, whether that is confidentiality of information or availability of capacity, that are dependent on the sorts of network covered by this inquiry.[203] The Government told us that with respect to intelligence sharing the involvement, or not, of Huawei does not affect its ability to share sensitive intelligence data over highly secure networks both with the UK and with partners. They told us that GCHQ have confirmed categorically that how the UK's 5G network is equipped has nothing to do with the sharing of classified

198 André Pienaar, CEO and Founder, C5 Capital (Q27)
199 Senator Tom Cotton, United States Senate (Q58); Congressman Mike Turner, US House of Representatives (Q114)
200 Written evidence submitted by the University of Strathclyde (SFG0019), p15
201 The Rt Hon. Ben Wallace MP, Secretary of State for Defence (Q187; Q194)
202 The Rt Hon. Ben Wallace MP, Secretary of State for Defence (Q198)
203 Ciaran Martin, Chief Executive Officer, National Cyber Security Centre (Q193)

data. They told us that HRVs "have never been and never will be in the UK's most sensitive networks".[204] This is repeated in Huawei's written evidence which states that:

> 5G that uses Huawei equipment will not be used for intelligence sharing or other critical state activities[205]

The Defence Secretary said that the MoD is not dependent on any one mode of communications, including 5G, as this would leave it exposed to an adversary.[206] The CEO of the NCSC reiterated the Defence Secretary's comments stating that:

> The NCSC spends a lot of money and expertise supporting defence on sovereign cryptography for some things, where we do not allow any non-UK parts—never mind Chinese or Russian—into the supply chain. That is quite expensive, but in some small parts of key strategic national assets it is necessary. That has no dependency whatsoever on public telecommunications networks of any kind. Then we go through to things that have to be highly secure but interoperable with allies, all the way through to ordinary communications and business communications through public networks. It is very layered, depending on risk.[207]

81. A private briefing with government cyber security experts confirmed these comments and we were told that on top of Huawei equipment never being used in sensitive networks, it has never been allowed to be used where it understands the context of a sensitive system. It was explained that all government sensitive business is encrypted, and intelligence and military networks are encrypted using sovereign equipment, so hostile actors will not be able to access information even if they are able to record the traffic.

82. We are content that Huawei has been, and continues to be, sufficiently distanced from sensitive defence and national security sites. The Defence Secretary has informed us that no Huawei 5G equipment is present on the defence estate and that sensitive communications are safe from compromise. *The Government should ensure that Huawei continues to be distanced from sensitive networks until the complete removal of its equipment from 5G by 2027.*

83. Huawei's continued presence in commercial 5G networks does not impact on our ability to share sensitive information with partners. We have been told that Huawei is not present in our sensitive networks and that, due to encryption standards, even if adversaries were able to record information as it passes through systems, they would not be able to decipher it.

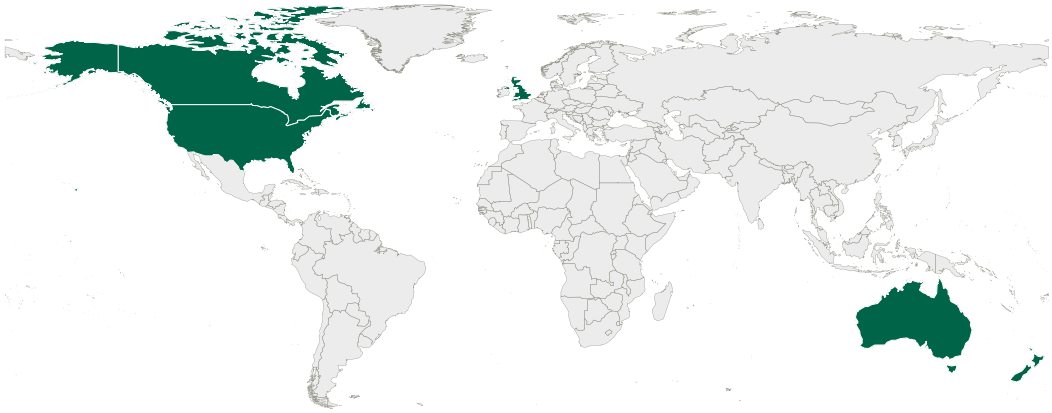
204 Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p8
205 Written evidence submitted by Huawei Technologies (SFG0010), p2
206 The Rt Hon. Ben Wallace MP, Secretary of State for Defence (Q186)
207 Ciaran Martin, Chief Executive Officer, National Cyber Security Centre (Q193)

Geopolitical considerations

The Geopolitics of 5G

84. As touched upon in this report so far there have been concerns that the UK's previous policy of including Huawei equipment in its 5G networks had isolated it from some allies.[208] This included concerns about the UK's place in the Five Eyes intelligence sharing alliance which includes Australia, Canada, New Zealand and the United States alongside the UK, and which Senator Tom Cotton described as the most valuable and powerful intelligence alliance in the world.[209]

Graphic 5: Five Eyes member states



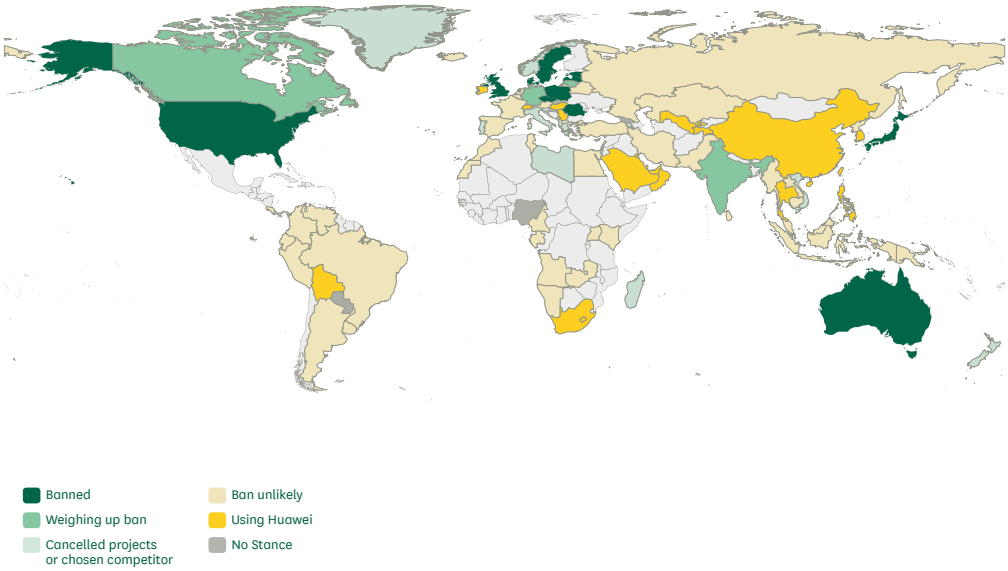
85. Other Five Eyes countries have placed an outright ban on using Huawei equipment.[210] The Government told us that they work closely with Five Eyes allies on the issue of telecoms security and note that the US and Australia originally went further than the UK with the controls they chose to impose on Huawei by banning them from their networks.[211] The NCSC told us that the Government of Canada is undertaking a review that has yet to conclude and that the situation in New Zealand is sufficiently different that a ban has not had to take place. The NCSC told us that the position in New Zealand is often mischaracterised.[212] There the NCSC explain, 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

208 Written evidence submitted by Declan James Ganley (SFG0013), p6
209 Senator Tom Cotton, United States Senate (Q58)
210 Written evidence submitted by TRL Technology (SFG0014), p5
211 Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p7–8
212 Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p19

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.[213]

Senator Tom Cotton told us that three of the Five Eyes partners have therefore rejected 5G technology from Huawei, or China at large - the US, Australia and New Zealand, and that he hoped that Canada will make a decision in line with the US and that, once the UK policy changes, that Five Eyes can present a united front.[214] Wider international policy on 5G, for example within the European Union or NATO, has been more mixed. It was reported in February that Germany had stopped short of banning Huawei from its network.[215] France has introduced a 'de facto ban' on Huawei 5G it by 2028.[216] Outside of these groupings, India has reportedly given orders to telecoms companies barring them from using Chinese vendors for future investments.[217] The map below provides an overview of global positions on allowing Huawei into the 5G network, as of 29 July 2020.[218]

Graphic 6: Use of Huawei across the world



86. The Henry Jackson Society, a foreign policy think tank based in London, made the point that if Australia can "black-ball" Huawei as its 5G provider, then the UK can certainly do the same without undue concern about the

213 Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p19; Reuters, 17 November 2019, UPDATE 2-Spark New Zealand keeps Huawei on preferred suppliers list, but leads 5G rollout with Nokia
214 Senator Tom Cotton, United States Senate (Q58)
215 Financial Times, Guy Chazan, 11 February 2020, Germany's CDU stops short of Huawei ban in 5G rollout
216 The Telegraph, James Cook, 22 July 2020, France introduces 'de facto ban' on Huawei 5G kit by 2028
217 IISS, August 2020, India's non-alignment in the telecommunications sector; Financial Times, Stephanie Findlay, 27 August 2020, India's Huawei snub prompts new crisis for Chinese telecoms group
218 New Statesman, Michael Goodier, 29 July 2020, The definitive list of where every country stands on Huawei

consequences.[219] However, Emily Taylor told us that the situation in the US and Australia, which have enacted outright bans of Huawei and ZTE, is very different from that in the UK. The US and Australia enacted bans in 2012 and so their existing infrastructure is not nearly as dependent on Huawei as the UK's. Therefore, they are, Emily Taylor argues, freer to manoeuvre.[220]

87. The NCSC told us that 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, suggesting that their decisions arose from geopolitical concerns with China.[221]

88. Before the most recent set of restrictions were announced Senator Tom Cotton told us that China was attempting to drive a high-tech wedge between the UK and US through the use of Huawei.[222] He explained the UK's previous policy would have created tensions in the ability to share the most sensitive kinds of intelligence as legislation passed last year in the US calls for their intelligence agencies to consider the extent to which partner nations have Chinese-sourced technology in their networks.[223] Ahead of a visit to the UK the US Secretary of State Mike Pompeo told reporters in January that the UK had a chance to "relook" at the decision, stressing the US needed to be sure its allies had "trusted" information networks.[224] In February Robert Strayer, the US deputy assistant for cyber and communications, warned that allowing Huawei in would threaten intelligence sharing between the US and UK.[225]

China was attempting to drive a high-tech wedge between the UK and US

Evidence from Naomi McGill, Director of Research & Development at Harlette Capital Ltd, and Consultant at Cable Free - Wireless Excellence Limited, highlighted tensions also arising between the UK and Australia following the January decision, which Declan James Ganley, CEO at Rivada Networks, also noted.[226] Dr Robert Dover outlined the political risk arising from the UK's previous policy:

> The political risk is that the current US Administration carries through with its threats to throttle back or cut off the supply of various types of intelligence product (be it signals, communications, or imagery intelligence), as a response to the threat it perceives or as a penalty for the failure of the UK to comply with its assessment. In turn we could suppose

219 Sir Richard Dearlove in Henry Jackson Society, Bob Seely MP, Dr Peter Varnish OBE and Dr John Hemmings, May 2019, Defending Our Data: Huawei, 5G and the Five Eyes, p.9
220 Emily Taylor, CEO, Oxford Information Labs (Q12)
221 Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p19
222 Senator Tom Cotton, United States Senate (Q48)
223 Senator Tom Cotton, United States Senate (Q59)
224 BBC News, 30 January 2020, Huawei: Pompeo urges UK to 'relook' at decision ahead of UK visit
225 BBC News, Rory Cellan-Jones, 21 February 2020, Huawei: US cyber-boss tells UK to 'think again' on Huawei
226 Written evidence submitted by Naomi McGill (SFG0002), p11; Written evidence submitted by Declan James Ganley (SFG0013), p6

> that the Australian government is likely to be supportive of any American move in this regard, because the Chinese security state is the largest state-actor threat in their region. A change of US Administration in November is unlikely to row back from these measures, because of the reputational risk of being seen as 'soft' on security policy.[227]

Emily Taylor told us that it is difficult to know to what extent the previous policy allowing Huawei to continue in the UK's 5G networks has impacted on the Five Eyes relationship. She explained, however, that it is the first instance she is aware of, where one member of the Five Eyes is "essentially threatening" another over decisions about purchasing equipment with "pretty consistent and overt statements" being made by high-level members of the US Administration.[228]

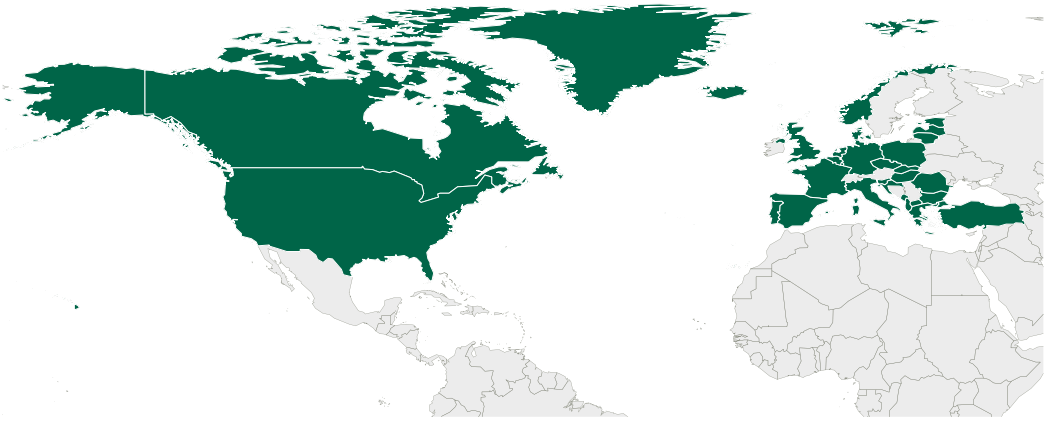
89. These tensions and announcements from allied Governments could have had a stark impact on operability within Five Eyes but also within organisations such as NATO as well, argues Dr Robert Dover.[229] NATO, which Senator Tom Cotton described as the most successful military alliance in world history, could be impacted by the UK's 5G policy.[230] Dr Steven Conlon highlights the risk to NATO also quoting NATO Secretary General Jens Stoltenberg, who said that the alliance took the threat from Huawei "very seriously".[231] Stoltenberg says that the Alliance is consulting widely to gain further understanding of the full extent of the potential threat from Huawei.[232] More recently the NATO Secretary General said the UK's review of 5G security is important:

> I trust that the UK government will design their networks in ways that protect the networks and make sure that the UK has secure 5G networks.[233]

In January 2019, the Polish Government told the EU and NATO to co-ordinate their stance on Huawei after one of Huawei's staff was arrested in Warsaw on suspicion of spying.[234]

227 Written Evidence submitted by Dr Robert Dover, University of Leicester (SFG0008), p2–3
228 Emily Taylor, CEO, Oxford Information Labs (Q25)
229 Written Evidence submitted by Dr Robert Dover, University of Leicester (SFG0008), p3
230 Senator Tom Cotton, United States Senate (Q75)
231 Written evidence submitted by Dr Steven Conlon (SFG0015), p13; Defence News, 15 March 2019, NATO weighing Huawei spying risks to member countries
232 Written evidence submitted by Dr Steven Conlon (SFG0015)
233 Reuters, 10 June 2020, NATO chief says on Huawei: UK review of 5G security is important
234 The Times, Marc Bennetts, 14 January 2019, Nato and EU 'must unite' over Huawei

Graphic 7: NATO member states



90. Both the Defence and Culture Secretaries told us that there had been no change in the level and detail of the intelligence sharing between the Five Eyes during the UK's debate on Huawei's involvement in 5G.[235] The Defence Secretary confirmed this again and added specifically that there had been no diminution in intelligence exchanges between the UK and Australia.[236] The Culture Secretary told us that the US sees the issue of Huawei through a geopolitical prism and that "It has made its position abundantly clear to us".[237]

91. The Government has had to balance its own technical considerations with pressures from allies such as the United States. The UK's closest allies, including the United States and Australia, originally embarked on a policy at odds to that of the UK. This had the potential to damage the UK's close intelligence, security and defence relationship with them, although reassurances have been given by Ministers that this was not the case.

92. The framing of the issue by the United States as a technical concern about the presence of Huawei in our networks has generated disagreement between the two Governments, given the contrasting conclusions of technical experts on either side of the Atlantic.

93. In the end, the Government decision was taken because of the technical considerations resulting from sanctions; however the Government should have considered the potential damage to key alliances enough of a risk to begin to remove Huawei from the UK's 5G network before the US sanctions were imposed.

235 The Rt Hon. Ben Wallace MP, Secretary of State for Defence and The Rt Hon. Oliver Dowden CBE MP, Secretary of State for Digital, Culture, Media and Sport (Q226)
236 The Rt Hon. Ben Wallace MP, Secretary of State for Defence (Q239–241)
237 The Rt Hon. Oliver Dowden CBE MP, Secretary of State for Digital, Culture, Media and Sport (Q236)

Huawei and the Chinese state

94. Huawei was founded in 1987 in Shenzhen, southern China, by Ren Zhengfei. It started making communications equipment for mobile phone networks and is now a global company, employing 180,000 workers. Huawei is the world's second-largest smartphone supplier after Samsung, with 18% of the market.[238] It employs 1,600 people in the UK with research centres in Edinburgh, Bristol, Cambridge and Ipswich and with a proposed £1 billion research centre at Sawston. The firm has also sponsored work at several universities including Imperial College London, Southampton and Surrey.[239]

Ownership and links to the Chinese Communist Party

95. Some witnesses told us that Huawei is closely linked to the Chinese state and Chinese Communist Party. André Pienaar said that Huawei is entirely different from the other players in the telecoms market due to the extent to which it is embedded in the Chinese state.[240] Congressman Mike Turner took the view that in China there is no division between its commercial sector, its government sector and the Communist party.[241]

96. André Pienaar illustrated the links between the founder of Huawei, Ren Zhengfei, a former engineer in the People's Liberation Army, and the Chinese Communist Party. André Pienaar told us that Ren Zhengfei has been a member of the party since 1978 and was someone on whom the Politburo of the Chinese Communist Party relies for the future of the party.[242] Huawei, however, said that Ren Zhengfei's membership of the People's Liberation Army and Chinese Communist Party are not relevant: "When Ren Zhengfei was a young man, you needed to be a Communist Party member to have any position of responsibility."[243]

97. Huawei Technologies' evidence argues that Huawei's annual reports, audited by KPMG, show that Huawei is a private company wholly owned by its employees.[244] But Professor Christopher Balding, Associate Professor at Fulbright University and an Associate Fellow at the Henry Jackson Society, writes that Huawei is "effectively owned by a political public organisation of an adversarial state".[245] He explains the complexity of Huawei's ownership structure with ownership lying with the Huawei Investment Holding Trade Union which, as it is part of the All China

It is fundamentally false and misleading to claim that Huawei is a private enterprise

238 BBC News, Tim Bowler, 14 July 2020, Huawei: Why is it being banned from the UK's 5G network?
239 BBC News, Leo Kelion, 14 July 2020, Huawei: What does the ban mean for you?
240 André Pienaar, CEO and Founder, C5 Capital (Q7)
241 Congressman Mike Turner, US House of Representatives (Q109)
242 André Pienaar, CEO and Founder, C5 Capital (Q14)
243 BBC News, Tim Bowler, 14 July 2020, Huawei: Why is it being banned from the UK's 5G network?
244 Written evidence submitted by Huawei Technologies (SFG0010), p2
245 Written evidence submitted by Prof. Christopher Balding, Associate Professor, Fulbright University and an Associate Fellow at the Henry Jackson Society (SFG0012), p2

Federation of Trade Unions, is part of a highly-political and state managed institution. Professor Balding concludes that "It is fundamentally false and misleading to claim that Huawei is a private enterprise".[246]

98. The Culture Secretary told us that the Government was aware that large private companies in China often have links to the Chinese Communist Party and this was one of the factors that led to Huawei being designated as a HRV.[247]

Chinese subsidies

99. André Pienaar told us that it is calculated that the Chinese Government have financed the growth of Huawei with some $75 billion over the past three years to enable it to achieve the kind of market dominance it currently has.[248] Evidence from the University of Strathclyde and Mike Rogers, CEO at 5G Action Now and former Chair of the US House of Representatives Intelligence Committee, highlighted that subsidies from the Chinese government explain the company's rapid growth by undercutting competitors.[249] André Pienaar said that Huawei's dominant position as the leading network solution provider in terms of market share is very much premised on the fact that, with the subsidies they are receiving from the Chinese state, they can sell their hardware equipment at a "ridiculously low price point".[250] Huawei Technologies, however, disagree with this and submitted evidence which claims that Huawei does not gain an unfair market advantage through the receipt of state aid or other special funds from the Chinese government.[251]

The National Intelligence Law

100. Professor Balding also expressed concerns about Huawei's links to Chinese intelligence agencies, which matches wider concerns about China's National Intelligence Law 2017 which is mentioned in the HCSEC's annual reports and discussed earlier in this report.[252] Dr Roslyn Layton, Vice President at Strand Consult, argues that while the technical vulnerabilities of equipment produced by Huawei are considerable and present opportunities for theft, surveillance, espionage, and sabotage, China's legal framework alone is reason enough to prohibit the use of technology made by Chinese state owned and affiliated enterprises in UK networks.[253]

246 Written evidence submitted by Prof. Christopher Balding, Associate Professor, Fulbright University and an Associate Fellow at the Henry Jackson Society (SFG0012), p2–3
247 The Rt Hon. Oliver Dowden CBE MP, Secretary of State for Digital, Culture, Media and Sport (Q253)
248 André Pienaar, CEO and Founder, C5 Capital (Q14)
249 Written evidence submitted by the University of Strathclyde (SFG0019), p3; Wall Street Journal, Chuin-Wei Yap, 25 December 2019, State Support Helped Fuel Huawei's Global Rise; Mike Rogers, Chairman, 5G Action Now (Q89)
250 André Pienaar, CEO and Founder, C5 Capital (Q19)
251 Written evidence submitted by Huawei Technologies (SFG0010), p2
252 Written evidence submitted by Prof. Christopher Balding, Associate Professor, Fulbright University and an Associate Fellow at the Henry Jackson Society (SFG0012), p3
253 Written evidence submitted by Roslyn Layton (SFG0017), p2

101. John W Strand and Dr Steven Conlon argue that the law means that any Chinese citizen working for Huawei is obliged to engage in espionage on behalf of the Chinese Communist Party.[254] Professor Balding highlights that based upon a database of employee résumés Huawei employees state that they act on behalf of the Ministry of State Security within Huawei, with other employees working simultaneously for research units of the People's Liberation Army: Professor Balding believes that these units are probably managing cyber warfare. He argues that this demonstrates that Huawei is actively engaged in a variety of intelligence, security, and intellectual property activities that are publicly denied by the company.[255] Dr Conlon argues that there is already some evidence that Huawei staff are willing to follow instructions from the Chinese state security services stating that staff members have been linked to espionage allegations, with Australian Intelligence reporting in 2018 that Huawei personnel provided "access codes to infiltrate a foreign network".[256]

Huawei is actively engaged in a variety of intelligence, security, and intellectual property activities

102. The NCSC told us that successive Governments have assumed that any company based in China could be fully compelled to act under the direction of the Chinese state.[257] This interpretation matches with that of André Pienaar who told us that the law is applicable abroad and in the UK to Chinese companies.[258]

103. It is clear that Huawei is strongly linked to the Chinese state and the Chinese Communist Party, despite its statements to the contrary. This is evidenced by its ownership model and the subsidies it has received. Additionally, Huawei's apparent willingness to support China's intelligence agencies and the 2017 National Intelligence Law are further cause for concern. Having a company so closely tied to a state and political organisation sometimes at odds with UK interests should be a point of concern and the decision to remove Huawei from our networks is further supported by these links.

104. Concern about Huawei is therefore based on clear evidence of collusion between the company and the Chinese Communist Party apparatus. It is important that the West does not succumb to ill-informed anti-China hysteria and recognises the mutual benefits of Chinese involvement in our economy. *The UK, and allies, should ensure that decisions taken around the*

254 Written evidence submitted by John W Strand (SFG0016), p3; Written evidence submitted by Dr Steven Conlon (SFG0015), p2

255 Written evidence submitted by Prof. Christopher Balding, Associate Professor, Fulbright University and an Associate Fellow at the Henry Jackson Society (SFG0012), p3; The Telegraph, Robert Mendick, 5 July 2019, Huawei staff CVs reveal alleged links to Chinese intelligence agencies

256 Written evidence submitted by Dr Steven Conlon (SFG0015), p2; ZDNet, 5 November 2018, Huawei denies foreign network hack reports

257 Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p10

258 André Pienaar, CEO and Founder, C5 Capital (Q19)

involvement of Chinese companies are taken in an evidence-based manner, and only when risk is demonstrable should decisions around removal be made.

The Chinese state's reaction to the removal of Huawei

105. The University of Strathclyde cites the director of the Global Public Policy Institute, Thorsten Benner, who believes the UK's January decision, of restrictions on Huawei but not its removal, was made due to fear of retaliation from China. He pointed to the Chinese ambassador stating in an interview that exclusion would lead to worsening economic and political relations. According to the University of Strathclyde, Thorsten Benner believes that Chinese threats to the UK over worsening economic and political relations were seen as more salient to the UK than US threats.[259] These threats are based on China's strong involvement in many sectors of the UK economy. An article from RUSI highlighted the depth of the UK-China economic relationship, both in trade and in investment flows.[260] This economic involvement includes other critical infrastructure projects with China's state railway company reportedly in talks to build the HS2 high-speed rail line and China having a minority share in Hinkley Point Nuclear Plant and Sizewell C Nuclear Plant. China General Nuclear Power Corporation also, reportedly, hopes to build a nuclear reactor at Bradwell in Essex.[261]

106. Congressman Mike Turner told us that once the UK took up the issue of whether Huawei should be in the 5G system, China began to threaten the UK in terms of pulling out in other areas and he argued that this shows that, in China's view, this is not just a commercial transaction.[262] He later told us that the Chinese government has been suggesting that, if the UK does not concede to Huawei, they will take action in other areas to punish the UK.[263] Just prior to the July announcement of the removal of Huawei, China Daily, an English-language daily newspaper owned by the Communist Party of China, released an editorial warning that the "UK will pay the price if it carries out [the] decision to exclude Huawei". The editorial warned that:

UK will pay the price if it carries out decision to exclude Huawei

259 Written evidence submitted by the University of Strathclyde (SFG0019), p8; Foreign Policy, Thorsten Benner, 31 January 2020, Britain Knows It's Selling Out Its National Security to Huawei
260 RUSI, Andrew Cainey and Veerle Nouwens, 12 June 2020, Assessing the UK–China Commercial Relationship
261 BBC News, 15 February 2020, HS2: UK in talks with China over construction of high-speed line; BBC News, 21 October 2015, Hinkley Point nuclear agreement reached; BBC News, 16 October 2015, Security fears over China nuclear power deal
262 Congressman Mike Turner, US House of Representatives (Q109)
263 Congressman Mike Turner, US House of Representatives (Q142)

> If true, this would be a very costly policy reversal that would cause an all-lose scenario for all stakeholders, and one whose ramifications would undoubtedly ripple far beyond technological concerns.[264]

The Times reported that the Chinese ambassador to the UK had privately "fired a warning shot" at the Government, telling business leaders that abandoning Huawei could undermine plans for Chinese companies to build nuclear power plants and the HS2 high-speed rail network.[265] China's ambassador later reportedly warned that trade between the UK and China could be at risk if the government removed Huawei from the 5G network.[266] This was followed by warnings from HSBC that it could face reprisals in China if Huawei is banned from the UK's 5G network.[267] Following the decision to remove Huawei by 2027, the Times reported that Beijing threatened retaliation against British companies in China with remarks from Zhao Lijian, the foreign ministry spokesperson in Beijing, threatening the prospects of UK companies in China such as BP, Diageo, GlaxoSmithKline, InterContinental Hotels and Jaguar Land Rover.[268] The US Secretary of State released a statement labelling these moves "coercive bullying tactics" from the Chinese Communist Party, arguing that:

> Beijing's aggressive behavior shows why countries should avoid economic overreliance on China and should guard their critical infrastructure from CCP influence … The United States stands ready to assist our friends in the U.K. with any needs they have, from building secure and reliable nuclear power plants to developing trusted 5G solutions that protect their citizens' privacy.[269]

107. Franklin C. Miller highlighted that these economic threats to the UK in retaliation for actions against Chinese interests are not unique:

> China threatens and employs economic blackmail against Governments whose actions it disapproves of. In the past week, we saw it cut off tourism to South Korea in retaliation for the US missile defence system. We have seen it cut off rare earth metals to Japan in retaliation for territorial dispute. It is cutting off imports of Australian products because Canberra had the temerity to suggest an international study into the origins of Covid. Now it is making threats against the UK, Denmark and Germany regarding Huawei.[270]

264 China Daily, 24 May 2020, UK will pay price if it carries out decision to exclude Huawei: China Daily editorial
265 The Times, Tim Shipman, 7 June 2020, China threatens to pull plug on new British nuclear plants
266 The Times, Catherine Philp and Lucy Fisher, 6 July 2020, China hints at trade boycott if UK ditches Huawei from 5G; The Times, Catherine Philp, Lucy Fisher and Francis Elliot, 7 July 2020, Ditch Huawei and trade will suffer, warns China
267 The Telegraph, Christopher Willliams, Lucy Burton and Edward Malnick, 6 June 2020, HSBC warns Downing Street on Chinese reprisals over Huawei
268 The Times, Steven Swinford, Lucy Fisher and Didi Tang, 15 July 2020, China threatens to make British companies pay for Huawei ban
269 US Department of State, 9 June 2020, On China's Attempted Coercion of the United Kingdom
270 Franklin C. Miller, Principal, The Scowcroft Group (Q150)

Dr Steven Conlon highlighted other examples to show that China is willing to threaten economic consequences on countries that ban or significantly limit Huawei's access to 5G deployment contracts. He cites examples from Australia, Canada and Denmark, amongst others, and argues that this further underscores the close political links between the Chinese Communist Party and Huawei.[271] An article from the Observer Research Foundation also argued that the Chinese state is using economic threats to increase the presence of its telecom providers:

> The Chinese state's actions themselves are evidence of the "politicisation" of 5G. India's ambassador to Beijing was reportedly summoned by the Chinese Ministry of Foreign Affairs and told categorically to pressure his government to allow Huawei to participate in 5G trials, with the threat of "reverse sanctions" against firms. China's ambassador to Germany similarly threatened "consequences" should Germany exclude Huawei from its market.[272]

108. Following concerns about China using economic blackmail there have been reports that MPs are pressuring the Government to remove Chinese companies from involvement in nuclear power.[273]

109. Pressure has been exerted by China on the UK Government to retain the presence of Huawei in its 5G infrastructure through both covert and overt threats. More recently, following the Government's announcement for the long-term withdrawal of Huawei from its 5G network, China has threatened to withdraw from the UK's economy, including in critical infrastructure such as nuclear.

110. Ending China's involvement in the UK's critical infrastructure would be a radical step with huge implications for the UK's economy. *If threats by the Chinese state to withdraw from the UK's critical industries continue and worsen, the Government should carefully consider China's future presence in critical sectors of the economy. The Government should make provision in its proposed National Security and Investment Bill to give it the power to intervene and stop investments in critical industries should threats or risks be present.*

Working with allies on 5G provision

111. Huawei Technologies' evidence notes that the UK currently has no sovereign industrial capability in 5G equipment.[274] TechUK add that there is no

271 Written evidence submitted by Dr Steven Conlon (SFG0015), p8
272 Observer Research Foundation, Trisha Ray, 10 June 2020, D10 or Bust? Finding purpose in the 5G club of democracies
273 Financial Times, Helen Warrell, George Parker, Demetri Sevastopulo, Yuan Yang, 15 July 2020, China lashes out at Boris Johnson over Huawei ban
274 Written evidence submitted by Huawei Technologies (SFG0010), p7

sovereign industrial capability within the Five Eyes group.[275] Even non-Chinese vendors such as Ericsson and Nokia do much of their manufacturing there and industrial capability is therefore concentrated in China. Nokia and Ericsson also have significant R&D and manufacturing operations in China and supply parts of China's own telecoms networks.[276] The NCSC's evidence quoted Matt Beale, then Vodafone's Director of Technology and Strategy, who told the Prague 5G conference in May 2019, "There is one supply chain for telecommunications, and it all runs through China."[277]

There is one supply chain for telecommunications, and it all runs through China

Some have expressed surprise at the lack of industrial capacity from UK allies, in particular the United States. André Pienaar explained that this is because the US has focused significantly on its software economy because of a policy belief that lower cost manufacturing in China is attractive and this has allowed China to make significant gains in its technology supply network.[278] Howard Watson concurred with this assessment saying that the UK, along with many other countries such as the US, have lost the manufacturing part of the supply chain.[279]

112. Much of the evidence received argued that it is vital that the UK and its close allies create and maintain industrial capability in this field.[280] The University of Strathclyde told us:

> It is incredibly important that the UK, both separately, as well as with its international allies, creates capability in this field. The phrase "creates" is specifically and deliberately used, as the UK has lost a lot of its historical industrial capability in telecoms.[281]

TRL Technology, a UK-based technology company, told us that in order to enable true operational freedom without reliance on HRVs it is critical that the UK and its allies maintain the ability to produce and operate their own equipment and services. They added that the UK has many sovereign companies that could produce some or all of the 5G capability and argued that this would have the effect of generating prosperity in jobs and services around the development, deployment and export of trusted and assured 5G technology. This, they add, could be made more attractive by a joint Five Eyes proposition that would open up the markets of those countries and beyond to NATO and other partners.[282] TechUK told us that the UK has a number of highly respected companies with

275 Written evidence submitted by techUK (SFG0020), p8; Written evidence submitted by Huawei Technologies (SFG0010), p7
276 Written evidence submitted by Huawei Technologies (SFG0010), p5; Written evidence submitted by Professor J A McDermid, University of York (SFG0025), p2
277 Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p13
278 André Pienaar, CEO and Founder, C5 Capital (Q33)
279 Howard Watson, Chief Technology and Information Officer, BT Group (Q300)
280 Written evidence submitted by Mr Declan James Ganley (SFG0013), p7; Written evidence submitted by TRL Technology (SFG0014), p5–6; Written evidence submitted by the University of Strathclyde (SFG0019), p15–17
281 Written evidence submitted by the University of Strathclyde (SFG0019), p15
282 Written evidence submitted by TRL Technology (SFG0014), p5–6

deep cyber security expertise which can and should be used to maintain and develop independent 5G capability for the UK, working alongside specialists like the NCSC.[283]

113. On proposed joint working with allies around the diversification of the supply chain, the University of Strathclyde's evidence states that there is a clear opportunity for the UK to partner with willing allies around the diversification of the supply chain but that care should be taken to ensure that the UK would itself be able to export and sell this technology on an international stage, along with its allies, rather than merely be a passive participant unable to exploit the work.[284] Political calls have been made for the creation of a new forum extending beyond the Five Eyes network to include Japan, South Korea and possibly India, Germany and France, in part focussed on developing alternative suppliers of 5G equipment.[285]

114. In May 2020 it was reported that Downing Street was making plans for an alliance of ten democracies to create alternative suppliers of 5G equipment and other technologies to avoid relying on China. The UK Government has reportedly approached Washington about a club of democratic partners based on the G7 (United States, Italy, Germany, United Kingdom, Japan, Canada, France) plus Australia, South Korea and India. Working with international partners to pioneer a wider selection of future technologies is reportedly part of the Prime Minister's plan for reducing reliance on HRVs with an option being explored for members to channel investment to technology companies based in member states.[286]

115. Analysis from the Observer Research Foundation, a research foundation based in India, argues that the '5G club of democracies' or D10 seems to have struck a chord in Washington.[287] Senator Tom Cotton told us that the UK should join together with the United States and other powerful free nations and work together on a 5G solution that does not empower Chinese intelligence.[288] On the proposed "D10 alliance" outlined above the Senator said that it would have the productive capabilities and the innovative and entrepreneurial spirit to develop 5G technologies, both software and hardware "that will far surpass in quality, performance and price anything that China produces".[289] Congressman Turner indicated support for a "community of democracies" working in this area.[290] Franklin C. Miller told us that the US Secretary of State said that the US is ready

283 Written evidence submitted by techUK (SFG0020), p8
284 Written evidence submitted by the University of Strathclyde (SFG0019), p17
285 The Guardian, Patrick Wintour, 14 May 2020, Chinese threat prompts calls for UK to toughen company takeover laws
286 The Times, Lucy Fisher, 29 May 2020, Downing Street plans new 5G club of democracies; The Times, Lucy Fisher, 31 May 2020, British tech firms could get state help to rival Huawei
287 Observer Research Foundation, Trisha Ray, 10 June 2020, D10 or Bust? Finding purpose in the 5G club of democracies
288 Senator Tom Cotton, United States Senate (Q48)
289 Senator Tom Cotton, United States Senate (Q80)
290 Congressman Mike Turner, US House of Representatives (Q132–133)

to assist the UK with developing 5G solutions and that he would urge the UK Government to take that offer up and to press the American Administration for concrete action with the democracy group of 10.[291]

116. Brigadier General Robert Spalding told us that he would advocate a bulk buy of radios, with the UK and allies coordinating on their purchase, and that it would be good if Five Eyes got together and stimulated production through that. He explained that if you were to stimulate a large buy for the five members, "you would have a pool of radios that you could potentially really use to maximise your replace".[292] Mike Rogers told us he agreed with this assessment and said:

> I would argue again, if we all came together, as the Five Eyes, and said, "Here's the security standard for anybody that competes in any one of the Five Eye countries," that bloc would lead to the bulk purchasing that the General talked about, and it would prevent Huawei and ZTE making the argument—because we know what they are doing; they are going to make the trade argument with our friends in Britain; they are going to argue, "There is a cost to this; if we can't get in your market, we are going to find ways to punish you." My argument is, okay, we will get around that, by agreeing, as the Five Eyes partners, "This is the security standard." And by the way, that standard will be adopted by others, because they will know the care and concern that we would go through to make sure we got it right.[293]

Congressman Mike Turner told us that there should be a call for a NATO standard on telecoms throughout our nations.[294] Brigadier General Robert Spalding told us that between Five Eyes, NATO and Japan there would be a very strong buying coalition for a secure 5G network.[295]

117. The Government told us of their intention to work with Five Eyes allies and other partners to develop new supply chain capacity.[296] The Culture Secretary told us that to achieve the Government's goal of diversifying the market it could not act unilaterally and that the Government was working with other partners across the world, not just Five Eyes but the G7 and other countries such as India, South Korea and Japan.[297]

118. However, analysis from the Observer Research Foundation suggested that the exact purpose of the grouping remains hazy, with some analysts speculating that it would either fund a new market entrant to serve as an alternative, or

291 Franklin C. Miller, Principal, Scowcroft Group (Q150)
292 Brigadier General (ret.) Robert Spalding, Senior Fellow, Hudson Institute (Q98)
293 Mike Rogers, Chairman, 5G Action Now (Q98)
294 Congressman Mike Turner, US House of Representatives (Q118–119)
295 Brigadier General (ret.) Robert Spalding, Senior Fellow, Hudson Institute (Q100)
296 Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p4
297 The Rt Hon. Oliver Dowden CBE MP, Secretary of State for Digital, Culture, Media and Sport (Q217)

fund existing 5G providers within the D10, neither of which will provide workable solutions in the short-term. The Observer Research Foundation also argues that the D10 has very little in common regarding 5G policymaking and ecosystem:

> The United States is in the process of comprehensively removing Huawei and ZTE from its 5G ecosystem, along with Australia and Japan, with the UK likely following suit. Meanwhile France has only excluded Huawei from its core network, and India, Germany, Italy, Canada and South Korea are allowing Chinese vendors to participate in 5G trials, despite US pressure.[298]

119. The Government told us that they will work with Five Eyes allies and other partners to develop new supply chain capacity within this Parliament and we await detailed proposals coming before the House.[299]

120. It is evident that the UK's lack of industrial capacity in telecommunications is not unique, with China dominating the industry. In order to combat this dominance, we support the principle of proposals for forming a D10 alliance of democracies to provide alternatives to Chinese technology: however, it is not yet clear what the purpose of this alliance is. *Following consultation with allies, the Government should set out exactly what the role of this alliance would be and seek to make progress as quickly as possible on formulating joint 5G policy. The Government should explore opportunities for joint network security standard setting across Five Eyes and perhaps more widely, through a D10 or NATO. It should also develop a programme to create necessary industrial capacity.*

121. We recognise that a D10 alliance could become more than just an alliance to provide alternatives to Chinese technology. *For security reasons beyond the remit of this inquiry we recommend that the Government takes steps to engage a D10 alliance of the most complete kind.*

Global standards

122. Ericsson told us that global standards are fundamental to 5G.[300] The NCSC wrote that 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.[301] BT Group told us that industry forums and international standard-setting bodies continue to define and refine the technical specifications for 5G security, drawing on global

298 Observer Research Foundation, Trisha Ray, 10 June 2020, D10 or Bust? Finding purpose in the 5G club of democracies
299 Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p9
300 Written evidence submitted by Ericsson (SFG0023), p2
301 Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p17

collaboration of chipset manufacturers, network equipment vendors, subscriber equipment manufacturers, operators and the suppliers of new technologies such as virtualisation.[302]

123. The '3rd Generation Partnership Program' (3GPP) brings together members of regional standards organisations to define the single, global standards. The NCSC told us that 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 and are Chinese organisations. 440 are affiliated through the European Telecoms Standards Institute although not all are European and 54 are affiliated through the Alliance for Telecoms Industry Solutions and are mainly US and Canadian. The NCSC told us that 3GPP finished the first 5G standard in June 2018, a success that they said was hailed by the world's telecoms companies.[303]

124. TRL Technology argued that the Government should take a proactive stance in international standards bodies to ensure that future standards are benign and not capable of malicious use.[304] Dr Conlon argued therefore that it is vital that the UK works with vendors, academics and international agencies to ensure that policies, standards and procurement strategies that reinforce vendor diversity, transparency and accountability are introduced, including a review of representation at these bodies.[305] André Pienaar told us that it is very important for Britain to continue to be a world leader and help to set international standards for key areas of technology in the correct international fora.[306] Dr Steven Conlon explained that global 5G standards impact the security of all networks and argued that China currently monopolises the 5G standards bodies.[307] He articulates concerns that the 5G standard bodies are dominated by Chinese companies, supported by China-sponsored affiliated countries, and cites a Wall Street Journal article:

The Government should take a proactive stance in international standards bodies

> Representatives from Chinese companies now hold 10 of the 57 chairman and vice chairman positions on decision-making panels at 3GPP.[308]

Emily Taylor told us that China is extremely active in technical standards, particularly through the United Nations, and is putting significant recourses into multiple study groups. She argued that:

302 Written evidence submitted by BT Group (SFG0022), p2
303 Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p18; 3GPP, 14 June 2018, Rel-15 success spans 3GPP groups
304 Written evidence submitted by TRL Technology (SFG0014), p4
305 Written evidence submitted by Dr Steven Conlon (SFG0015), p4
306 André Pienaar, CEO and Founder, C5 Capital (Q45)
307 Written evidence submitted by Dr Steven Conlon (SFG0015), p4
308 Written evidence submitted by Dr Steven Conlon (SFG0015), p15; Wall Street Journal, 30 March 2018, China's Huawei Is Determined to Lead the Way on 5G Despite U.S. Concerns

> It should also be a wakeup call to Western countries that have been relying on the market to sort these things out that that investment, that consistency, that level of participation in the technical standards bodies, particularly in the United Nations, has to be backed up by countries that have perhaps a different vision of the future networks and communication systems.[309]

Emily Taylor said that China is working on projects that would fundamentally alter the way the internet works, in ways that we can expect to benefit Chinese political ambitions.[310] More widely Senator Tom Cotton told us that China had worked effectively to undermine, and to insinuate itself into, the central decision-making places in international organisations.[311]

125. Senator Tom Cotton said that the Five Eyes nations, along with allies such as Japan and South Korea could help establish some new standards, whether they are technological standards or international policy standards.[312] The Scotland 5G Centre, the national hub for Scotland's 5G, argues that the Government can help address the diversity of the vendor ecosystem by "selecting suitable delegates to the standards bodies on behalf of the UK, who can prioritise and advance this work."[313]

126. Global standards are key to 5G and future telecommunications networks. China has been very active in the standard setting bodies whilst the UK and allies have stood back. This is not satisfactory. *The UK should take a leadership role in shaping global standards to ensure that the future of mobile networks, and global technology more widely, matches with our interests and those of our allies.*

309 Emily Taylor, CEO, Oxford Information Labs (Q29)
310 Emily Taylor, CEO, Oxford Information Labs (Q45)
311 Senator Tom Cotton, United States Senate (Q52)
312 Senator Tom Cotton, United States Senate (Q60)
313 Written evidence submitted by The Scotland 5G Centre (SFG0024), p3

Conclusions for the UK market

Timescales for the removal of Huawei

127. There has been significant debate about the timescales for the removal of Huawei, even prior to the Government's most recent announcement of the 2027 deadline. Prior to the decision being made, Gordon Corera noted that a long lead time for Huawei kit to be removed, of seven to ten years, would leave critics (such as the United States) unhappy but cause less disruption and therefore be more pleasing to operators. A three to five-year removal would please those concerned with Huawei's presence, he adds, but impose more costs on the networks.[314] Prior to the July announcement it was reported that the Government could announce restrictions that would have seen Huawei removed by 2023.[315] Senator Tom Cotton said that he had seen reports of this removal deadline, which he would welcome, adding that he would welcome it being done even earlier.[316] Congressman Mike Turner told us that a target to remove Huawei by 2023 was "an encouraging goal".[317]

128. The Financial Times reported that telecoms executives were frustrated at the prospect of a 2023 withdrawal with one quoted as saying that a 2023

314 BBC News, Gordon Corera, 13 July 2020, Huawei: UK prepares to change course on 5G kit supplier
315 The Times, Steven Swinford and Lucy Fisher, 26 May 2020, 'Impossible' to get rid of Huawei tech in telecom network by 2023
316 Senator Tom Cotton, United States Senate (Q82)
317 Congressman Mike Turner, US House of Representatives (Q130)

timeline was "too aggressive" for a full phase out.[318] A Times article said that BT and Vodafone were lobbying ministers against a decision to rip out Huawei hardware over a short timeframe, saying that would result in signal blackouts and claims for compensation running into hundreds of millions of pounds, because they would have to strip kit from about 19,000 mobile phone masts.[319] Howard Watson, of BT, told the Science and Technology Committee:

> I believe it is logistically impossible to get to zero in a three-year period. That would literally mean blackouts throughout the country for customers on 4G and 2G, as well as 5G, as we were building it in. We would definitely not recommend that we go down that route.[320]

Howard Watson told us that a 2023 date for complete removal would cause significant mobile network outages for 2G, 3G, 4G and 5G and argued that it is the wrong thing to do for the nation given the dependence on telecommunications networks.[321] He said that BT would need a minimum of five years, and ideally seven.[322] Andrea Dona, Head of Networks at Vodafone, similarly told the Science and Technology Committee that removal by 2023 would cause problems and that a five-year transition plan would be the minimum (therefore removal by 2025).[323]

129. Following the announcement of the 2027 deadline an article in the Times suggested that BT and Vodafone "breathed a sigh of relief" following the decision with shares in both companies rising following the decision.[324] On the timescale announced Scott Petty told us that Vodafone were happy with the decision on 2027 because it give them time to swap equipment without major disruption to their networks and enables them to have time to develop the OpenRAN ecosystem as an alternative supply.[325] Howard Watson told us that BT had a lot of conversations with Government about the possibility of it being done more quickly than 2027 and in all cases concluded that would cause significant network outage implications. He said that the measured approach for seven years means that it can be done in a controlled way without causing excessive amounts of network outages and within the guidance of the £500 million that was laid out by BT in January.[326]

130. When asked about the economic costs of various timeframes for Huawei's removal the Culture Secretary did not get drawn into specifics but told us that

318 The Financial Times, Jim Pickard and Nic Fildes, 23 May 2020, UK draws up 3-year plan to remove Huawei from 5G networks
319 The Times, Oliver Shah, 21 June 2020, Row over Huawei's planned £400m UK R&D centre
320 Science and Technology Committee, UK telecommunications infrastructure and the UK's domestic capacity, HC 450, Howard Watson, Chief Technology and Information Officer, BT Group (Q158)
321 Howard Watson, Chief Technology and Information Officer, BT Group (Q292)
322 Science and Technology Committee, UK telecommunications infrastructure and the UK's domestic capacity, HC 450, Howard Watson, Chief Technology and Information Officer, BT Group (Q160)
323 Science and Technology Committee, UK telecommunications infrastructure and the UK's domestic capacity, HC 450, Andrea Dona, Head of Networks, Vodafone (Q144–157)
324 The Times, Tom Howard, 15 July 2020, Later Huawei 5G deadline sounds good to Vodafone and BT
325 Scott Petty, Chief Technology Officer, Vodafone UK (Q271)
326 Howard Watson, Chief Technology and Information Officer, BT Group (Q271)

"the more restrictions you place on the free market, the greater the cost of doing so".[327] Government cyber security experts told us that a quicker removal could make the networks unreliable and pose financial concerns for operators, with a speedier removal than 2027, such as three years from now, described as "incredibly challenging".

131. The Government has faced pressure to remove Huawei more quickly than by 2027. The evidence we have received would suggest that a quicker timescale could result in signal blackouts, delay the 5G rollout significantly and cost both operators and the economy greatly. For the time being we consider the plan for a removal by 2027 to be a sensible decision. *Should pressure from allies for a speedier removal continue or should China's threats and global position change so significantly to warrant it, the Government should, however, consider whether a removal by 2025 is feasible and economically viable. The Government should also be alert to the fact that other factors may warrant an earlier removal despite the risk of costs or delays.*

132. The issues surrounding Huawei's removal and the UK's consolidated vendor ecosystem illustrate the need for a coherent long-term strategy for the UK's technical and technological ambitions. It is not clear to us that the Government has a cohesive strategy in this area. *The Government should learn lessons from debates around Huawei and seek to formulate a long-term plan for tech in the UK, this should include, for example, the Government's plan relating to OneWeb and the UK's removal from the Galileo satellite system.*

The economic impact on operators

133. BT Group's written evidence told us that the Government restrictions announced in January will cost them approximately £500m over a five-year period. They explain that these costs are created by a number of factors:

i. Most substantially (they argue) is the expense of swapping out existing Huawei equipment for those of another vendor. They explain that BT's 5G deployment is, in this first phase, focused on upgrading their existing 4G cell sites. Due to the current lack of vendor interoperability (which they expect to persist in the medium term), they have to use the same vendor for 5G as the underlying 4G technology–so in the vast majority of cases, they will also have to replace their existing 4G equipment;

ii. The expected increase in unit prices of 5G equipment from other global vendors as they respond to increased demand; and

327 The Rt Hon. Oliver Dowden CBE MP, Secretary of State for Digital, Culture, Media and Sport (Q224)

iii. The likely cost impact of negotiating access to sites with landlords who will be in a strong position to demand increased payments as our hard deadline for completing the transition is known publicly.[328]

Howard Watson told us that the interventions by Government in January and July will probably mean that BT's rollout of 5G will be "a year to a year and a half longer than it otherwise might have been".[329]

134. It was reported that the Government may assist operators financially because of these restrictions. Prior to the announcement in July The Telegraph reported that the Government was engaged in talks with MNOs regarding compensation for having to swap out Huawei equipment earlier than planned.[330] Later reports have suggested that MNOs are hoping to offset the added costs of removing Huawei by convincing the government to make it cheaper for them to buy the airwaves necessary to provide 5G services.[331] It has been reported that Vodafone want the 5G auction to be scrapped to cover the cost of replacing Huawei's equipment. Ofcom, the telecoms regulator, is due to conduct a competitive auction of new spectrum for 5G but the sale will not take place until November at the earliest because of the coronavirus pandemic.[332]

135. On the other hand, others argue that financial compensation is not necessary with evidence from the University of Strathclyde saying that the UK's network operators are profitable businesses, and that it is only right that they should bear the cost of making what they provide secure.[333] John W Strand argues that the costs arising from the January restrictions were not as significant as once predicted. He writes that BT estimates the impact of the Huawei ban to be only £100 million per year for the next 5 years, which compared to its total investment is a small amount. John W Strand also highlights that Vodafone noted similarly that the Huawei restrictions do not hurt its financial performance.[334]

136. Despite being a longer timeframe than some have called for, the Government's most recent restrictions on the use of Huawei in 5G networks will delay the 5G rollout and economically damage the UK and mobile network operators. *The UK Government should take necessary steps to minimise the delay and economic damage. The Government should consider providing compensation to operators, whether direct or indirect, whose networks are currently reliant on Huawei if the 2027 deadline is moved forward, in order to minimise costs to, and delays for, consumers. They should also consider legislation to give networks the right of access to sites.*

328 Written evidence submitted by BT Group (SFG0022), p4
329 Howard Watson, Chief Technology and Information Officer, BT Group (Q272)
330 The Telegraph, Hannah Boland, 2 June 2020, Inside the talks to end the UK's reliance on Huawei; Talks in Whitehall over potential 'compensation' for telecoms operators are understood to be underway
331 The Telgraph, James Cook, 14 July 2020, Telecoms firms seek cheaper 5G airwaves to meet £2bn cost of ripping out Huawei kit
332 Financial Times, Nic Fildes, 16 July 2020, Vodafone wants 5G auction to be scrapped after Huawei move
333 Written evidence submitted by the University of Strathclyde (SFG0019), p5
334 Written evidence submitted by John W Strand (SFG0016), p1–2

Diversifying the UK's consolidated vendor market

137. UK telecoms operators are currently heavily reliant on a small number of global companies for their RAN equipment, namely Huawei, Ericsson and Nokia.[335] Britain's reliance on just three suppliers, including Huawei, is "crazy," according to Dr Ian Levy:

> We need to diversify the market significantly in the UK so that we have a more robust supply base to enable the long-term security of the UK networks and to ensure we do not end up nationally dependent on any vendor.[336]

Improving diversity in the market is one of the Governments priorities for the future of telecommunications, and they are developing a targeted diversification strategy to address this market failure.[337] The TSCR sought to look at how the Government can create sustainable diversity in the telecoms supply chain and the Government's strategy can be categorised into three groups:

Britain's reliance on just three suppliers, including Huawei, is crazy

- Industry-led action: For example, the Telecom Infra Project has groups to help build interoperability (vRAN Fronthaul/F1 interface), cut some of the high R&D costs (OpenCellular and OpenRAN) and remove some of the operator costs for custom hardware (OpenRAN);
- Combined action: For example, Government support to vendors who operate strongly in one geography and aren't yet able to operate in another; and
- Government-led action: For example, the UK national telecoms lab that the NCSC intends to build with DCMS will help de-risk new entrants to the market by providing a standard test bed, allowing the Government to test and force better interoperability between vendors and ensure security is improving. The Government is looking at hybrid models with established public cloud providers with good security records to see if they can provide some of the mobile edge compute infrastructure. Work around spectrum and intellectual property will need an international approach.[338]

335 Written evidence submitted by BT Group (SFG0022), p5
336 National Cyber Security Centre, Dr Ian Levy, 9 March 2020, The future of telecoms in the UK
337 Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p6
338 National Cyber Security Centre, Dr Ian Levy, 9 March 2020, The future of telecoms in the UK

138. The Culture Secretary told us that the UK needs to correct the market failure and explained that the UK needed to start a process of diversification by:

i. Securing the existing two incumbent providers;

ii. Getting other vendors into the market. The Culture Secretary said that both Samsung and NEC are "obvious vendors" that they would like to get into the UK market; and

iii. Moving to more open radio access networks (OpenRAN).[339]

Evidence received was supportive of the Government's ambitions for a more diverse ecosystem of vendors.[340] Huawei told us that sustaining a three-vendor market or increasing to four vendors would be positive.[341] BT Group told us that a more diverse vendor base would be beneficial economically and in terms of quickening technological advances.[342]

Attracting other 5G vendors

139. One of the key pillars of the Government's diversification strategy will be to attract other scale players to the UK market.[343] Discussions for the introduction of new vendors have focussed on the South Korean company Samsung and Japanese companies NEC and Fujitsu. The NCSC told us that the UK Government is seeking to encourage them all to enter the UK market, although none currently operate at scale in Europe.[344]

140. Huawei Technologies' evidence recognises the possibility of Samsung providing an alternative supplier. They highlight that Samsung currently provides 5G telecoms equipment in South Korea, and some limited services in Japan and the US.[345] André Pienaar told us that Samsung has about 3% of the global share of telecommunications equipment network.[346] Samsung has stated its interest in entering the market for the UK 5G network, supplying the RAN. In written evidence to the Science and Technology Committee, Samsung commented:

> The UK Government has a stated objective of diversifying the 5G market to encourage new entrants. Samsung now wishes to help achieve that national goal by entering the 5G network market in the UK.[347]

339 The Rt Hon. Oliver Dowden CBE MP, Secretary of State for Digital, Culture, Media and Sport (Q217)
340 Written evidence submitted by techUK (SFG0020), p3, 5; Scott Petty, Chief Technology Officer, Vodafone UK (Q270); Written evidence submitted by James Sullivan, Head of Cyber Research, RUSI (SFG0027), p2; NIS Cooperation Group, 9 October 2019, EU coordinated risk assessment of the cybersecurity of 5G networks
341 Written evidence submitted by Huawei Technologies (SFG0010), p2–5
342 Written evidence submitted by BT Group (SFG0022), p5
343 Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p6–7
344 Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p25
345 Written evidence submitted by Huawei Technologies (SFG0010), p5
346 André Pienaar, CEO and Founder, C5 Capital (Q19)
347 Written evidence submitted by Samsung Electronics UK (UKT0008)

In evidence to the Science and Technology Committee, Samsung suggested it had also recently won "major network contracts in Canada and New Zealand, two countries with which the UK has a close relationship".[348]

Scott Petty from Vodafone told us that Samsung has a role to play, particularly in the OpenRAN ecosystem but that Samsung lacks the capabilities, particularly in 2G and 3G, to be deployed at scale.[349] The University of Strathclyde's evidence notes that Samsung has little or no footprint in the UK and Europe.[350] James Sullivan notes that this is because most of its equipment is designed for a different frequency than most European countries have allocated for 5G and 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.[351]

141. NEC is a Japanese vendor and was recently awarded a contract to supply part of Japan's 5G network. It has announced it is seeking to grow its market share from 0.7% to 20% by 2030 with its Chief Executive, Takashi Niino, commenting:

> In the wake of the Huawei issue, governments worldwide are considering what options are out there... There is a chance for NEC to be part of those options, a possibility that hardly existed in the past.[352]

Takashi Niino said the UK government reached out to NEC as part of a strategy to consider alternatives to Huawei equipment in the UK network.[353] It was reported that talks began in May of this year.[354] It was reported that another Japanese company, Fujistu, is also being considered as a potential alternative to Huawei in the UK.[355]

142. In June the Culture Secretary told us that the Minister for Digital Infrastructure, Matt Warman MP, has been having constructive discussions with NEC, Fujitsu and Samsung, who have all, he added, expressed an interest in entering the UK market. The Culture Secretary explained that:

> The challenge we need to overcome is how we ensure that this is a market they feel comfortable entering, given that they are not currently present and there is actually quite a high cost of entering a new market.[356]

348 Written evidence submitted by Samsung Electronics UK (UKT0008)
349 Scott Petty, Chief Technology Officer, Vodafone UK (Q298)
350 Written evidence submitted by the University of Strathclyde (SFG0019), p7
351 Written evidence submitted by James Sullivan, Head of Cyber Research, RUSI (SFG0027), p2
352 Financial Times, Kana Inagaki and Nic Fildes, 1 July 2020, NEC sees Huawei's woes as chance to crack 5G market
353 Financial Times, Kana Inagaki and Nic Fildes, 1 July 2020, NEC sees Huawei's woes as chance to crack 5G market
354 The Times, Lucy Fisher, 4 June 2020, Japanese company enters 5G talks as Huawei doubts grow
355 The Telegraph, James Cook, 20 July 2020, Britain consults Japan on how to fill Huawei vacuum
356 The Rt Hon. Oliver Dowden CBE MP, Secretary of State for Digital, Culture, Media and Sport (Q228)

The Culture Secretary explained that the Government is looking at things such as trade incentives for incoming vendors, financial incentives and how the Government can help them create scale.[357]

143. The NCSC told us that whilst the Government is seeking to encourage companies into the UK market and to set a technical environment that is conducive to new entrants it is unlikely that any new entrants to the RAN will be able to scale sufficiently to meet multiple national requirements within a 3 to 5 year period.[358]

The problem of non-interoperability and Open-RAN

144. Non-interoperable equipment is a significant issue for telecoms and contributes to 'vendor lock-in'. In order to deal with inter-operability issues André Pienaar told us that the future of telecommunications is in OpenRAN, virtualised networks where software replaces hardware which allows for greater inter-operability.[359] OpenRAN technology standardises the design and functionality of RAN hardware and software and allows operators to buy equipment from different vendors which opens the door for smaller vendors. The Telecom Infra Project explained that OpenRAN is non-proprietary removing the previous barriers to entry which were extremely high.[360]

145. Much of the evidence that we received praised OpenRAN as having the potential to diversify the supply chain in the future.[361] We were told that this will help tech SMEs, an area in which the UK is currently world leading.[362] Furthermore, we were told that OpenRAN will improve network security through a more transparent and accessible development process.[363]

146. However, BT Group's evidence told us that is it not yet clear whether OpenRAN will be successful.[364] James Sullivan's evidence suggested that initiatives such as OpenRAN face serious challenges as even if interoperability is feasible, it may not yet be economically viable.[365] The Economist, meanwhile, notes that OpenRAN will not solve all security problems and that its underlying standard is not yet mature.[366]

357 The Rt Hon. Oliver Dowden CBE MP, Secretary of State for Digital, Culture, Media and Sport (Q228)
358 Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p26
359 André Pienaar, CEO and Founder, C5 Capital (Q33)
360 Written evidence submitted by techUK (SFG0020), p7; Written evidence submitted by Telecom Infra Project (SFG0027), p3
361 Written evidence submitted by Dr Steven Conlon (SFG0015), p6; Written evidence submitted by David Hanke (SFG0021), p1;
362 André Pienaar, CEO and Founder, C5 Capital (Q34, Q40); Senator Tom Cotton, United States Senate (Q51)
363 Written evidence submitted by TRL Technology (SFG0014), p3; Written evidence submitted by Telecom Infra Project (SFG0027), p3
364 Written evidence submitted by BT Group (SFG0022), p5
365 Written evidence submitted by James Sullivan, Head of Cyber Research, RUSI (SFG0027), p3
366 The Economist, 8 April 2020, Open standards, not sanctions, are America's best weapon against Huawei

147. TechUK told us that industry is actively exploring this type of technology, with Emily Taylor telling us that Vodafone, in particular, has been investing in this technology.[367] Scott Petty confirmed this telling us that Vodafone has begun trialling OpenRAN technology in the UK in a number of rural sites and is working with Government and the other operators to drive scale in the OpenRAN environment to try to create an opportunity to create further diversification.[368] Scott Petty said that Vodafone believe that by 2023 they may be able to deploy at some scale in the rural parts of the network and by 2025 to deploy at scale in dense urban and suburban areas.[369] For BT, Howard Watson told us that they are probably looking at 2026 or 2027 before they could usefully deploy OpenRAN.[370]

148. The NCSC said that most small cell vendors are only just starting to scale their engineering and product portfolio and 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.[371] The Culture Secretary told us that, internationally, there is one current example of a network using OpenRAN.[372] This was launched on 8 April 2020 by Rakuten, a Japanese company.[373]

149. The Culture Secretary told us that the medium to long-term solution for diversification of 5G is driving OpenRAN and that the Government has taken measures in respect of that:

> First, we are launching flagship OpenRAN testbeds with MNOs. Clearly, that is going to be at a small scale to begin with. Secondly, we are looking to co-ordinate R&D funding with our other partners, particularly Five Eyes, because it would make sense if we co-ordinate between different specialisms within the different elements of an OpenRAN.[374]

He added that the Government are looking at what financial incentive they can create for operators to start adopting an OpenRAN system.[375] TechUK however, argue that the Government can spur this market by prioritising OpenRAN and similar initiatives in Government funded testbeds (such as its 5G Testbeds Programme) or subsidised rollouts.[376]

Make inter-operability through OpenRAN and similar initiatives a reality

The Telecom Infra Project told us that the UK should provide support for

367 Written evidence submitted by techUK (SFG0020), p7; Emily Taylor, CEO, Oxford Information Labs (Q38)
368 Scott Petty, Chief Technology Officer, Vodafone UK (Q270)
369 Scott Petty, Chief Technology Officer, Vodafone UK (Q296)
370 Howard Watson, Chief Technology and Information Officer, BT Group (Q299)
371 Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p25
372 The Rt Hon. Oliver Dowden CBE MP, Secretary of State for Digital, Culture, Media and Sport (Q229)
373 The Economist, 8 April 2020, Open standards, not sanctions, are America's best weapon against Huawei
374 The Rt Hon. Oliver Dowden CBE MP, Secretary of State for Digital, Culture, Media and Sport (Q221)
375 The Rt Hon. Oliver Dowden CBE MP, Secretary of State for Digital, Culture, Media and Sport (Q221)
376 Written evidence submitted by techUK (SFG0020), p7

innovative British companies in RAN and should consider ways to make it easier for mobile networks to procure from outside the established vendors.[377] BT Group's evidence was similar arguing that the Government should:

- Target public funding on a number of OpenRAN projects based in the UK with industry providing opportunities for commercial deployments e.g. via rural coverage programmes or dense urban small cell roll-out.
- Encourage major vendors who do not have a significant presence in the UK, such as Samsung, to invest in UK-focused product development that meets UK operators' specific requirements.
- Greater funding support, potentially through the DCMS 5G Testbeds and Trials programme, to develop a new Future Network Research Initiative (FNRI) to complement the proposed National Telecoms Lab (which will focus on the testing of security of new equipment for the UK market). The FNRI would provide the infrastructure to enable universities and companies to trial new approaches to network deployment and operation, collaborate to build to prove end-to-end solutions, test hardware and software in a scaled environment. This would help in overcoming the hurdles smaller vendors face in proving their products in the UK telecoms environment.[378]

The CEO of the NCSC told the Committee that there is £200 million for 5G testbeds and trials programme, some of which is going to things that will encourage OpenRAN.[379] Government cyber security experts told us about the intention to set up this proposed National Telecoms Lab, which will work to make inter-operability through OpenRAN and similar initiatives a reality, work to de-risk new entrants and to give security researchers access to networks so that they can help make networks more secure.

150. The UK market for vendors is far from satisfactory. Whilst this reflects a wider consolidated ecosystem of global 5G vendors action must now be taken to ensure that 5G is in a more secure position in the years to come.

151. *The Government should work with mobile network operators to bring in new suppliers to the UK, for example Samsung or NEC and also encourage the development of industrial capacity in the UK*. This will not only improve market diversity but make our networks more resilient and lessen the potential security risks by removing Huawei and therefore leaving the UK reliant on Nokia and Ericsson alone.

152. OpenRAN presents an opportunity to move away from the current consolidated vendor environment to one in which operators no longer

377 Written evidence submitted by Telecom Infra Project (SFG0027), p4
378 Written evidence submitted by BT Group (SFG0022), p5–6
379 Ciaran Martin, Chief Executive Officer, National Cyber Security Centre (Q229)

have to consider which vendor to source from. It will also improve network security in a number of other ways. Whilst it may not provide an immediate solution as the standard is not yet mature, it does present a long-term solution to the current situation. *The UK Government and mobile service operators should continue investment in OpenRAN technology and work to make the UK a global leader, not just in technological development, but also in production*.

Network security and the Telecoms Security Requirements

153. We received evidence to suggest Government should be responsible for setting security requirement for vendors and operators in telecoms.[380] Some evidence also suggested that the current regulatory regime is insufficient and does not adequately incentivise good cybersecurity practice.[381]

154. The Scotland 5G Centre told us that the Government should be working with technical experts across a wider range of stakeholders, including those outside Government, to form high-quality technical guidance that is broader, and more principles-focused, rather than based on specific concerns around certain vendors, as they argue the current guidance is.[382] It appears this is what the Government have sought to do with the TSCR and the proposed Telecoms Security Requirements (TSRs). In its TSCR the Government proposed that inadequacies in product security could be the result of vendors putting commercial concerns before security risks:

> The responsibility for the management of security and resilience risks for UK telecoms is currently shared between the Government, Ofcom and industry. Telecoms operators are responsible for assessing risks and taking appropriate measures to ensure the security and resilience of their networks. However, there can be tensions between commercial priorities and security concerns, particularly when these impact on costs and investment decisions.
>
> Equally, the business models of vendors do not always prioritise cyber security sufficiently. An extreme example of this can be seen in the conclusions of the 2019 HCSEC Oversight Board report. The flaws identified in the report are the result of practices that may have achieved good commercial outcomes but have resulted in poor cyber security.[383]

380 Written evidence submitted by TRL Technology (SFG0014), p4; Written evidence submitted by the University of Strathclyde (SFG0019), p5
381 Written evidence submitted by BT Group (SFG0022), p1–2; Emily Taylor, CEO, Oxford Information Labs (Q27, Q36)
382 Written evidence submitted by The Scotland 5G Centre (SFG0024), p2
383 Department for Digital, Culture, Media and Sport, July 2019, UK Telecoms Supply Chain Review Report

The response to the Telecoms Supply Chain Review

In response to the review's findings, the Government committed to establishing a new security framework for 5G, this would include:

New Telecoms Security Requirements (TSR): This new set of security requirements would aim to provide clarity to industry on what is required and "raise the height of the security bar" by requiring telecoms operators, overseen by Ofcom and Government, to design and manage their networks to meet new requirements.

Establishing an enhanced legislative framework for security in telecoms: The new requirements would be underpinned by legislation to "provide Ofcom with stronger powers to allow for the effective enforcement of the TSR and to establish stronger national security backstop powers for Government." This legislation is to be introduced "at the earliest opportunity".

Managing the security risks posed by vendors: The Review concluded that there should be a "three lines of defence" approach to managing the risks posed by vendors:

- Require operators to subject vendors to rigorous oversight through procurement and contract management. This involves operators requiring all their vendors to adhere to the new TSR;
- Require operators to work closely with vendors, supported by Government, to ensure effective assurance testing for equipment, systems and software, and support ongoing verification arrangements; and
- Impose additional controls on the presence of certain types of vendors which pose significantly greater security and resilience risks to UK telecoms. In considering what those controls should be, it is necessary to address the identified security risks, whilst seeking to minimise the costs to industry and the wider economy.384

384 Department for Digital, Culture, Media and Sport, July 2019, UK Telecoms Supply Chain Review Report, p.6–7

155. BT Group told us that whilst cyber security is a top priority, from an operator's perspective the current regulatory framework does not adequately incentivise the security of networks.[385] Emily Taylor told us that the market has not delivered good cyber-security practices through the ecosystem and that is a "major problem". She explained that the market actually rewards companies for being less secure and as long as those market conditions persist it will always be possible for hostile state actors to compromise our systems.[386] She later explained that the market rewards getting out to market quickly, doing things cheaply and having lots of features over security.[387] This matched with what we were told by government cyber security experts who told us that the current regulatory system is not sufficient for the future as it doesn't incentivise security for networks. The evidence we received indicated widespread support from industry for the conclusions of the TSCR and the proposed TSRs.[388] Huawei Technologies, for example, told us that the TSRs will make the UK the most strongly regulated communications market in the world.[389]

156. The Culture Secretary told us that the current regime sits under the Communications Act where the burden was on telecoms providers to determine their own security in which they had no obligation.[390] He added that, currently, Government advice to operators is in the form of guidance, which companies are not obliged to follow.[391] Government cyber security experts told us that Ofcom is only responsible for ensuring that the networks are available and can only fine the regulator if they have a service outage or significant failure. Government cyber security experts told us that if responsibility changes in line with the planned Telecom Security Bill Ofcom will gain much more power to become a cyber security regulator as well as a market regulator.

157. The NCSC told us that the overall implementation of the TSRs, coupled with the secondary issue of HRV (which now seems to have been somewhat settled), matters most for the security of 5G. Without the TSR framework, the NCSC add, they cannot be confident about the security of UK 5G networks.[392] In June the Culture Secretary told us that they will be bringing forward the Telecoms Security Bill "shortly". He told us that it will place a range of obligations on telecoms companies, shifting the burden so "it is now

385 Written evidence submitted by BT Group (SFG0022), p1–2
386 Emily Taylor, CEO, Oxford Information Labs (Q27)
387 Emily Taylor, CEO, Oxford Information Labs (Q36)
388 Written evidence submitted by techUK (SFG0020), p4; Written evidence submitted by Huawei Technologies (SFG0010), p1–6; Howard Watson, Chief Technology and Information Officer, BT Group (Q290); Scott Petty, Chief Technology Officer, Vodafone UK (Q290)
389 Written evidence submitted by Huawei Technologies (SFG0010), p1
390 The Rt Hon. Oliver Dowden CBE MP, Secretary of State for Digital, Culture, Media and Sport (Q188)
391 The Rt Hon. Oliver Dowden CBE MP, Secretary of State for Digital, Culture, Media and Sport (Q189)
392 Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p16

essentially the Government saying what they need to do to ensure the network is secure".[393] He also told us that the purpose of the Bill is to put government advice to vendors on security on a statutory footing to ensure that they are required to follow it.[394] He added that the Bill will not differentiate between the different levels of telecommunications network, whether 3G, 4G or 5G.[395] Describing the likely structure of the proposed Bill itself the Culture Secretary said:

> In terms of broad structure, there will be overarching duties in the legislation. We will then produce specific codes in terms of security. The purpose of producing those specific codes under it is to give us the flexibility so that this legislation is futureproof, so that we can keep up with further developments.[396]

Government cyber security experts told us that the new primary legislation is required alongside a code of practice. The Government initially told us that they were seeking to introduce legislation to implement the new telecoms security framework before the summer recess, this did not happen.[397]

158. The current regulatory situation for network security is outdated and unsatisfactory. The Telecoms Security Bill is required to bring regulations up to date and allow Government to compel operators to act in the interests of security. The current situation has led to commercial concerns trumping those of national security. *The Government should not allow a situation where short-term commercial considerations are placed ahead of those for national security and defence. The Telecoms Security Bill is necessary in order to enhance the Government's and Government bodies' regulatory powers and should be published as soon as possible.*

159. The House was promised a Telecoms Security Bill before the summer recess. This did not happen. There must be no further delay. *The Government should introduce the Telecoms Security Bill before 31 December 2020.*

393 The Rt Hon. Oliver Dowden CBE MP, Secretary of State for Digital, Culture, Media and Sport (Q188)
394 The Rt Hon. Oliver Dowden CBE MP, Secretary of State for Digital, Culture, Media and Sport (Q189)
395 The Rt Hon. Oliver Dowden CBE MP, Secretary of State for Digital, Culture, Media and Sport (Q189)
396 The Rt Hon. Oliver Dowden CBE MP, Secretary of State for Digital, Culture, Media and Sport (Q200)
397 Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Ministry of Defence (SFG0026), p4

Conclusions and recommendations

1. 5G will transform lives across the world by facilitating the Internet of Things. Whilst this is undoubtedly a positive development, 5G will increase our reliance on mobile connectivity, and this represents a security risk whether from 'espionage, sabotage or system failure'. Many more items will be connected to the internet through 5G meaning a greater surface for illicit actions. This represents a risk to individuals as well as to defence and government. (Paragraph 18)

2. We share the Government's objective that the UK remains at the forefront of the 5G rollout as we move into the next technological era. It is imperative that the UK is amongst the first countries to benefit from the technological advances that 5G will bring. *The Government's ambitions for the rollout of 5G are laudable and cybersecurity policy should take into account the strategic value of the UK maintaining its position as a global market leader in this technology.* (Paragraph 25)

3. It is clear that the UK vendor market for 5G kit is not diverse enough. Even with the inclusion of Huawei the market was "sub-optimal" and the Government's decision to remove Huawei completely from 5G by 2027 poses a risk that could potentially result in an even less diverse market, which could bring security and resilience concerns of its own. (Paragraph 33)

4. This inquiry was launched in the context of a lively debate on the security of the UK's 5G network in Parliament and across the country from late 2019 and through 2020 with a focus on the presence in our network of high-risk vendors, particularly Huawei. A significant Government announcement took place in January with restrictions placed on high-risk vendors followed by stricter rules announced in July, with Huawei to be removed from the UK's 5G network by 2027. The UK Government has had to balance technical considerations with wider geopolitical considerations when formulating its 5G policy. (Paragraph 52)

5. There is evidence that the UK, and our allies, face many malicious cyber-attacks both from rogue individuals and state-sponsored attacks from states such as Russia and China. These attacks are diverse in their nature and in their aims. Some attacks aim to steal individual data and state secrets whilst others seek to bring down the network in its entirety. (Paragraph 58)

6. It is important that the Government continues to call out cyber-attacks from adversaries on the international stage and works to find a deterrent to counter them. *There is currently a lack of global rules regulating international cyber-attacks and the Government should work with allies to formulate a system to provide accountability for perpetrators. The Government should clarify why it is not deploying a cyberattack capability to deter aggressors.* (Paragraph 59)

7. There is no doubt that Huawei's designation as a high-risk vendor is justified. The Huawei Cyber Security Evaluation Centre has consistently reported on its low-quality products and concerning approach to software development, which has resulted in increased risk to UK operators and networks. The presence of Huawei in the UK's 5G networks therefore poses a significant security risk to individuals and to our Government. Whilst Huawei is a market leading company, we do not believe it to be higher in quality or more functional than its rivals, Nokia and Ericsson. (Paragraph 67)

8. The establishment of the Huawei Cyber Security Evaluation Centre has resulted in the UK leading the world in understanding Huawei's equipment. *Despite the planned withdrawal of Huawei from our 5G networks, the Huawei Cyber Security Evaluation Centre should continue to operate to assess Huawei equipment in other areas of our telecommunications. The Government should consider assessing all equipment vendors in a similar fashion, given the vulnerabilities of all equipment.* (Paragraph 68)

9. Advice to Government was clear, that the presence of Huawei in the UK's networks was a manageable risk. The UK has one of the most active and effective cyber-security regimes in the world, and, from our public and private conversations with Government, we are confident that GCHQ and the NCSC are able to appropriately manage any increased risk posed by the presence of Huawei or other high-risk vendors in the UK's 5G. (Paragraph 72)

10. Furthermore, whilst the risk remained manageable, it is important to remember the benefits in having a greater number of vendors involved in 5G network provision, despite the designation as high-risk, as this improves overall network resilience should a single vendor fail. (Paragraph 73)

11. Prior to the US sanctions announced in May, the risk of Huawei products remaining in the UK's 5G networks was, according to the Government, significant but manageable through monitoring and regulation. The situation changed when Huawei was deprived of reliable chip manufacturing capabilities. Following these sanctions, as discussed in the Government's July announcement, it became much more difficult to

guarantee and measure the quality of Huawei products. In principle, the Government has made the correct technical decision to ban the purchase and presence of Huawei products in the future. (Paragraph 77)

12. We are content that Huawei has been, and continues to be, sufficiently distanced from sensitive defence and national security sites. The Defence Secretary has informed us that no Huawei 5G equipment is present on the defence estate and that sensitive communications are safe from compromise. *The Government should ensure that Huawei continues to be distanced from sensitive networks until the complete removal of its equipment from 5G by 2027.* (Paragraph 82)

13. Huawei's continued presence in commercial 5G networks does not impact on our ability to share sensitive information with partners. We have been told that Huawei is not present in our sensitive networks and that, due to encryption standards, even if adversaries were able to record information as it passes through systems, they would not be able to decipher it. (Paragraph 83)

14. The Government has had to balance its own technical considerations with pressures from allies such as the United States. The UK's closest allies, including the United States and Australia, originally embarked on a policy at odds to that of the UK. This had the potential to damage the UK's close intelligence, security and defence relationship with them, although reassurances have been given by Ministers that this was not the case. (Paragraph 91)

15. The framing of the issue by the United States as a technical concern about the presence of Huawei in our networks has generated disagreement between the two Governments, given the contrasting conclusions of technical experts on either side of the Atlantic. (Paragraph 92)

16. In the end, the Government decision was taken because of the technical considerations resulting from sanctions; however the Government should have considered the potential damage to key alliances enough of a risk to begin to remove Huawei from the UK's 5G network before the US sanctions were imposed. (Paragraph 93)

17. It is clear that Huawei is strongly linked to the Chinese state and the Chinese Communist Party, despite its statements to the contrary. This is evidenced by its ownership model and the subsidies it has received. Additionally, Huawei's apparent willingness to support China's intelligence agencies and the 2017 National Intelligence Law are further cause for concern. Having a company so closely tied to a state and political organisation sometimes at odds with UK interests should be a point of concern and the decision to remove Huawei from our networks is further supported by these links. (Paragraph 103)

18. Concern about Huawei is therefore based on clear evidence of collusion between the company and the Chinese Communist Party apparatus. It is important that the West does not succumb to ill-informed anti-China hysteria and recognises the mutual benefits of Chinese involvement in our economy. The UK, and allies, should ensure that decisions taken around the involvement of Chinese companies are taken in an evidence-based manner, and only when risk is demonstrable should decisions around removal be made. *The UK, and allies, should ensure that decisions taken around the involvement of Chinese companies are taken in an evidence-based manner, and only when risk is demonstrable should decisions around removal be made.* (Paragraph 104)

19. Pressure has been exerted by China on the UK Government to retain the presence of Huawei in its 5G infrastructure through both covert and overt threats. More recently, following the Government's announcement for the long-term withdrawal of Huawei from its 5G network, China has threatened to withdraw from the UK's economy, including in critical infrastructure such as nuclear. (Paragraph 109)

20. Ending China's involvement in the UK's critical infrastructure would be a radical step with huge implications for the UK's economy. *If threats by the Chinese state to withdraw from the UK's critical industries continue and worsen, the Government should carefully consider China's future presence in critical sectors of the economy. The Government should make provision in its proposed National Security and Investment Bill to give it the power to intervene and stop investments in critical industries should threats or risks be present.* (Paragraph 110)

21. It is evident that the UK's lack of industrial capacity in telecommunications is not unique, with China dominating the industry. In order to combat this dominance, we support the principle of proposals for forming a D10 alliance of democracies to provide alternatives to Chinese technology: however, it is not yet clear what the purpose of this alliance is. Following consultation with allies, the Government should set out exactly what the role of this alliance would be and seek to make progress as quickly as possible on formulating joint 5G policy. The Government should explore opportunities for joint network security standard setting across Five Eyes and perhaps more widely, through a D10 or NATO. *Following consultation with allies, the Government should set out exactly what the role of this alliance would be and seek to make progress as quickly as possible on formulating joint 5G policy. The Government should explore opportunities for joint network security standard setting across Five Eyes and perhaps more widely, through a D10 or NATO. It should also develop a programme to create necessary industrial capacity.* (Paragraph 120)

22. We recognise that a D10 alliance could become more than just an alliance to provide alternatives to Chinese technology. For security reasons beyond the remit of this inquiry we recommend that the Government takes steps to engage a D10 alliance of the most complete kind. *For security reasons beyond the remit of this inquiry we recommend that the Government takes steps to engage a D10 alliance of the most complete kind.* (Paragraph 121)

23. Global standards are key to 5G and future telecommunications networks. China has been very active in the standard setting bodies whilst the UK and allies have stood back. This is not satisfactory. *The UK should take a leadership role in shaping global standards to ensure that the future of mobile networks, and global technology more widely, matches with our interests and those of our allies.* (Paragraph 126)

24. The Government has faced pressure to remove Huawei more quickly than by 2027. The evidence we have received would suggest that a quicker timescale could result in signal blackouts, delay the 5G rollout significantly and cost both operators and the economy greatly. For the time being we consider the plan for a removal by 2027 to be a sensible decision. *Should pressure from allies for a speedier removal continue or should China's threats and global position change so significantly to warrant it, the Government should, however, consider whether a removal by 2025 is feasible and economically viable. The Government should also be alert to the fact that other factors may warrant an earlier removal despite the risk of costs or delays.* (Paragraph 131)

25. The issues surrounding Huawei's removal and the UK's consolidated vendor ecosystem illustrate the need for a coherent long-term strategy for the UK's technical and technological ambitions. It is not clear to us that the Government has a cohesive strategy in this area. *The Government should learn lessons from debates around Huawei and seek to formulate a long-term plan for tech in the UK, this should include, for example, the Government's plan relating to OneWeb and the UK's removal from the Galileo satellite system.* (Paragraph 132)

26. Despite being a longer timeframe than some have called for, the Government's most recent restrictions on the use of Huawei in 5G networks will delay the 5G rollout and economically damage the UK and mobile network operators. *The UK Government should take necessary steps to minimise the delay and economic damage. The Government should consider providing compensation to operators, whether direct or indirect, whose networks are currently reliant on Huawei if the 2027 deadline is moved forward, in order to minimise costs to, and delays for, consumers. They should also consider legislation to give networks the right of access to sites.* (Paragraph 136)

27. The UK market for vendors is far from satisfactory. Whilst this reflects a wider consolidated ecosystem of global 5G vendors action must now be taken to ensure that 5G is in a more secure position in the years to come. (Paragraph 150)

28. *The Government should work with mobile network operators to bring in new suppliers to the UK, for example Samsung or NEC and also encourage the development of industrial capacity in the UK*. This will not only improve market diversity but make our networks more resilient and lessen the potential security risks by removing Huawei and therefore leaving the UK reliant on Nokia and Ericsson alone. (Paragraph 151)

29. OpenRAN presents an opportunity to move away from the current consolidated vendor environment to one in which operators no longer have to consider which vendor to source from. It will also improve network security in a number of other ways. Whilst it may not provide an immediate solution as the standard is not yet mature, it does present a long-term solution to the current situation. The UK Government and mobile service operators should continue investment in OpenRAN technology and work to make the UK a global leader, not just in technological development, but also in production. *The UK Government and mobile service operators should continue investment in OpenRAN technology and work to make the UK a global leader, not just in technological development, but also in production*. (Paragraph 152)

30. The current regulatory situation for network security is outdated and unsatisfactory. The Telecoms Security Bill is required to bring regulations up to date and allow Government to compel operators to act in the interests of security. The current situation has led to commercial concerns trumping those of national security. *The Government should not allow a situation where short-term commercial considerations are placed ahead of those for national security and defence. The Telecoms Security Bill is necessary in order to enhance the Government's and Government bodies' regulatory powers and should be published as soon as possible*. (Paragraph 158)

31. The House was promised a Telecoms Security Bill before the summer recess. This did not happen. There must be no further delay. *The Government should introduce the Telecoms Security Bill before 31 December 2020*. (Paragraph 159)

Sub-Committee Formal Minutes

Tuesday 22 September 2020

Members present:

Rt Hon Tobias Ellwood, in the Chair

Sarah Atherton

Richard Drax

Rt Hon Kevan Jones

Emma Lewell-Buck

Gavin Robinson

Rt Hon John Spellar

Derek Twigg

Minutes

Draft Report (*The Security of 5G*), proposed by the Chair, brought up and read.

Ordered, That the draft Report be read a second time, paragraph by paragraph.

Paragraphs 1 to 159 read and agreed to.

Summary agreed to.

Resolved, That the Report be the First Report of the Sub-Committee to the Committee in this session.

Ordered, That the Chair make the Report to the Committee.

Next meeting

[The Sub-Committee adjourned.

Committee Formal Minutes

Tuesday 22 September 2020

Members present:

Rt Hon Tobias Ellwood, in the Chair

Sarah Atherton

Richard Drax

Rt Hon Kevan Jones

Emma Lewell-Buck

Gavin Robinson

Rt Hon John Spellar

Derek Twigg

Minutes

Draft Report from the Sub-Committee *(The Security of 5G*), brought up and read.

Ordered, That the draft Report be read a second time, paragraph by paragraph.

Paragraphs 1 to 159 read and agreed to.

Summary agreed to.

Resolved, That the Report be the Second Report of the Committee to the House.

Ordered, That the Chair make the Report to the House.

Ordered, That embargoed copies of the Report be made available, in accordance with the provisions of Standing Order No. 134

Next meeting

[Adjourned till Tuesday 29 September at 1.45 pm

Witnesses

The following witnesses gave evidence. Transcripts can be viewed on the inquiry publications page of the Committee's website.

Tuesday 28 April 2020

First panel: Q1–47

Emily Taylor, CEO, Oxford Information Labs

André Pienaar, CEO and Founder, C5 Capital

Tuesday 02 June 2020

First panel: Q48–84

Tom Cotton, Senator, US Senate

Second panel: Q85–108

Mike Rogers, Chairman, 5G Action Now

Brigadier General (ret.) Robert Spalding, Senior Fellow, Hudson Institute

Tuesday 16 June 2020

First panel: Q109–149

Congressman Mike Turner, Congressman, US House of Representatives

Second panel: Q150–183

Franklin C. Miller, Principal, Scowcroft Group

Tuesday 30 June 2020

Q184–260

Rt Hon Ben Wallace MP, Secretary of State for Defence, Ministry of Defence

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

Ciaran Martin, CEO, National Cyber Security Centre

Tuesday 28 July 2020

Q261–306

Howard Watson, Chief Technology and Information Officer, BT Group

Scott Petty, Chief Technology Officer, Vodafone UK

Published written evidence

The following written evidence was received and can be viewed on the inquiry publications page of the Committee's website.

SFG numbers are generated by the evidence processing system and so may not be complete.

1. Balding, Professor Christopher (SFG0012)
2. BT Group (Mr Richard Wainer, Policy and Public Affairs Director, Networks) (SFG0022)
3. Conlon, Dr Steven (SFG0015)
4. Department for Digital, Culture, Media and Sport (Rt Hon Oliver Dowden, Secretary of State) (SFG0026)
5. Dover, Dr Robert (SFG0008)
6. Ericsson (Ms Patricia Dooley, Government and Industry Relations) (SFG0023)
7. Ganley, Mr Declan James (SFG0013)
8. Hanke, David (SFG0021)
9. Harlette Capital Ltd, and Cable Free - Wireless Excellence Limit (Miss Naomi McGill) (SFG0002)
10. Huawei Technologies (Mr Ashley Lumsden, Director of UK Government and Public Affairs) (SFG0010)
11. Layton, Dr Roslyn (SFG0017)
12. May, Lieutenant Commander RN (retired) Lester (SFG0004)
13. McDermid, Professor John (SFG0025)
14. Ministry of Defence (SFG0028)
15. Ministry of Defence (Rt Hon Ben Wallace, Secretary of State for Defence) (SFG0026)
16. Royal United Services Institute (RUSI) (James Sullivan, Head of Cyber Research) (SFG0011)
17. Scotland 5G Centre (Dr James Irvine, Security Researcher) (SFG0024)
18. Spalding, Dr Robert (SFG0001)

19. Strand, John (SFG0016)
20. techUK (Sophie Weston, Programme Manager - Communications Infrastructure) (SFG0020)
21. Telecom Infra Project (Mr Attilio Zani, Executive Director) (SFG0027)
22. TRL Technology Ltd (Mr Wade Bennett, Systems Solution Architect) (SFG0014)
23. University of Strathclyde (Dr Greig Paul, Lead Mobile Networks & Security Engineer) (SFG0019)