House of Commons

Science and Technology Committee

5G market diversification and wider lessons for critical and emerging technologies

Second Report of Session 2019–21

Report, together with formal minutes relating to the report

Ordered by the House of Commons
to be printed 21 January 2021

HC 450
Published on 4 February 2021
by authority of the House of Commons

Science and Technology Committee

The Science and Technology Committee is appointed by the House of Commons to examine the expenditure, administration and policy of the Government Office for Science and associated public bodies.

Current membership

Greg Clark MP (*Conservative, Tunbridge Wells*) (Chair)

Aaron Bell MP (*Conservative, Newcastle-under-Lyme*)

Dawn Butler MP (*Labour, Brent Central*)

Chris Clarkson MP (*Conservative, Heywood and Middleton*)

Katherine Fletcher MP (*Conservative, South Ribble*)

Andrew Griffith MP (*Conservative, Arundel and South Downs*)

Darren Jones MP (*Labour, Bristol North West*)

Mark Logan MP (*Conservative, Bolton North East*)

Carol Monaghan MP (*Scottish National Party, Glasgow North West*)

Graham Stringer MP (*Labour, Blackley and Broughton*)

Zarah Sultana MP (*Labour, Coventry South*)

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.

Publication

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

Evidence relating to this report is published on the inquiry publications page of the Committee's website.

Committee staff

The current staff of the Committee are: Masrur Ahmed (Second Clerk), Dr Harry Beeson (Committee Specialist), Dr Christopher Brown (Committee Specialist), Dr James Chandler (Committee Specialist), Emma Dobrzynski (Committee Operations Officer), Sonia Draper (Committee Operations Manager), Danielle Nash (Clerk), Robert Paddock (POST fellow), and Emily Pritchard (Senior Media and Communications Officer).

Contacts

All correspondence should be addressed to the Clerk of the Science and Technology Committee, House of Commons, London, SW1A 0AA. The telephone number for general inquiries is: 020 7219 2793; the Committee's e-mail address is: scitechcom@parliament.uk.

You can follow the Committee on Twitter using @CommonsSTC.

Contents

Summary

The fifth generation of mobile telecommunications technology started being deployed in the UK in 2019. These '5G' networks are intended to provide not only faster data transfer rates, but also faster responses, greater reliability and the ability to support greater densities of devices than previous generations. These capabilities are expected to offer significant new applications and consequent economic growth. The development and deployment of 5G has, however, coincided with increased scrutiny of potential security concerns related to the infrastructure and companies providing 5G networks.

Following US sanctions on Huawei, a telecommunications infrastructure equipment supplier, the UK's National Cyber Security Centre recommended that network operators should not use 5G access equipment supplied by Huawei after implementation of the sanctions. The Government subsequently introduced legislation that would forbid the use of 5G infrastructure equipment procured from Huawei after 31 December 2020. This would effectively leave the UK 5G radio access equipment market with just two major suppliers. Following a warning from the National Cyber Security Centre that "only having two suppliers into all national mobile networks reduces network resilience and security", the Government published a *5G Supply Chain Diversification Strategy* in November 2020 setting out measures aimed at diversifying the global telecommunications supply chain.

Key findings

The Government's *5G Supply Chain Diversification Strategy* provides an overview of the Government's intentions for addressing the current lack of vendors in the UK's 5G infrastructure equipment market. In our opinion, it does not, however, provide detail on how the £250 million initially allocated to it will be used or set out clear milestones or timeframes for achieving the Government's goals. Given the scale of the challenge and the urgency of the threat, we recommend that the Government should publish, within three months, a more detailed action plan including these details (paragraphs 9–14).

In the short term, the Government is seeking to diversify the UK market by attracting existing vendors from other markets. In addition to considering the case for transitioning away from 2G and 3G technologies—which is not a short-term solution—we conclude that the Government should propose measures within the next six months to address network operators' preference for vendors to offer older generation technologies with their 5G equipment. For example, the Government should consider incentivising or mandating standalone 5G deployments and/or the use of protocols such as the Open X2 interface (paragraphs 15–23).

In this Report, we find that the Government is right to support the development and adoption of open standards and increased interoperability as a potential means of diversifying the telecommunications equipment vendor market. We also conclude that it is right to identify Open RAN as a prominent approach to achieving this, but not the only one. However, neither the success of Open RAN or any related efforts, nor the positive impact on overall telecommunications security if these efforts are successful,

is guaranteed. The Government must not, therefore, assume that open standards and interoperability will inevitably be adopted nor that they will have the desired effect, and should pursue a range of measures designed to support market diversification and increase security (paragraphs 24–33).

Measures to support research and development form a major part of the Government's diversification strategy. We heard strong support for its proposals to establish testing facilities for new 5G infrastructure equipment. Nevertheless, the total funding of £250 million for initial implementation of the strategy is significantly smaller than the tens of billions of pounds invested annually in research and development by the main incumbent vendors. We recommend in this Report that the Government should aim to actively co-ordinate the research and development that it supports so that participants work towards clearly-defined long-term objectives. In addition to conducting security testing and validation, we also recommend that the Government should ensure that existing and newly-established facilities drive market diversification by stimulating collaboration and supporting the development and commercialisation of new technologies (paragraphs 34–52).

We were told in evidence that obstacles facing new 5G equipment vendors included challenges in scaling up production rapidly enough to meet network operator demand and the concentration of intellectual property rights in the hands of established vendors. We call on the Government to align its strategy for diversifying the 5G vendor market with its support for rolling out 5G network coverage. The Government should also provide more details on how it intends to address the barriers brought about by intellectual property rights, and update us on early progress made against this goal (paragraphs 53–60).

Although network operators stand to benefit from a more diverse vendor market, we heard that it may not be in their interest to purchase and use equipment from a wider range of vendors. The Government's diversification strategy does not sufficiently acknowledge this fact, and provides, we conclude, little detail of proposed measures to ensure that it will be in operators' interests to drive and maintain a diverse vendor market. Addressing this will require a combination of incentives, measures to reduce operator costs, and regulatory requirements. In order to provide certainty to the sector, we recommend that the Government should publish within three months of this Report the measures it is considering to incentivise and require network operators to diversify their suppliers (paragraphs 61–71).

The telecommunications regulator, Ofcom, has two principal duties: to further the interests of citizens in relation to communications matters; and to further the interests of consumers in relevant markets. Of these two principal duties, Ofcom has appeared, according to the evidence we received, to give less prominence to the first than the second. It must ensure that it pursues both of its principal duties and guarantees the security of the UK's telecommunications infrastructure as well as furthering the interests of consumers. We call on the Government to consider the case for updating its statement of strategic priorities for telecommunications (paragraphs 72–74).

The UK's telecommunications market accounts for a small proportion of the global market. International co-ordination will therefore be critical to the success of the

UK's diversification strategy. We recommend that the Government should seek to establish a dedicated, standing forum for international co-operation on diversifying the telecommunications market, encompassing as many like-minded countries as possible (paragraphs 75–80).

There is a strong risk that the urgent security challenges faced by the UK's telecommunications sector are indicative of a wider, and growing, geopolitical development. Throughout our inquiry, we heard of the prospect of a growing technological and regulatory divergence between China, and countries aligned with China, and other countries. In our opinion, the Government should not regard the problems posed by 5G as a one-off, but more likely illustrative of a wider challenge. The character of the UK's response, and that of other like-minded nations, will have profound implications for future decades and beyond. We urge the Government to address this seriously, comprehensively and without delay. We recommend that within twelve months, the Government should develop and publish a White Paper setting out its assessment of the current extent and future potential for global technological divergence, the anticipated consequences of such divergence and how it intends to address the challenges this poses. As part of this White Paper, the Government should identify the technologies that are likely to be of critical importance to the UK's prosperity and security over the next ten to twenty years and propose measures to seize associated opportunities and mitigate associated risks, addressing aspects including global supply chains, standards setting processes and domestic research and development capability (paragraphs 81–109).

1 Introduction

1. The development of mobile communications has been characterised by the periodic introduction of new 'generations' of technologies and industrial standards, with each generation offering new capabilities.[1] The fifth such generation ('5G') started to be rolled out in the UK in 2019.[2] Marcus Weldon, President of Bell Labs, emphasised to us that 5G was not designed just to be "4G-plus".[3] Professor Dimitra Simeonidou, Professor of High Performance Networks at the University of Bristol, explained that as well as delivering "higher capacity of connection" for "faster downloads", 5G provided "high reliability", "ultra-low latency" (a shorter delay between sending and receiving signals) and "great density machine-to-machine communication".[4] These properties are hoped to enable new applications, including:

- mobile augmented and virtual reality, for example for leisure, industrial and educational purposes;
- autonomous vehicles;
- remote health monitoring via wearable or implanted health devices, or environmental monitors installed in the home;
- 'smart' manufacturing processes, with connected production line machines transmitting real-time data on machine faults and safety issues; and
- 'smart cities' and the 'Internet of Things',[5] with dense networks of sensors and other wireless devices providing novel capabilities, such as responsive traffic management, street lighting or waste collection.[6]

Other, currently unforeseen, applications may also be developed over time.[7] The Government has said that 5G has more "potential to improve the way people live, work and travel, and to deliver significant benefits to the economy and industry" than "any previous generation of mobile networks".[8] Matthew Evans, Director of Markets at techUK, estimated that the economic impact of 5G could be "upwards of £100 billion in incremental GDP growth to 2030".[9]

2. There are currently three major suppliers of mobile and fixed access telecommunications infrastructure equipment in the UK, namely Nokia, Ericsson and

1 House of Commons Library, '5G', CBP 07883 (2019)
2 '5G: Finally, it's here in the UK—so what is it?', BBC News, accessed 5 October 2020
3 Q344
4 Q1
5 The 'Internet of Things' refers to the concept of widespread, digitally connected sensors and other devices used to monitor environments in real-time and implement appropriate actions in response, in order to improve services and efficiencies—see: Parliamentary Office of Science and Technology, 'Machine to Machine Communication', POSTnote 423 (2012)
6 Qq1, 11–13 and 15—see also: Parliamentary Office of Science and Technology, '5G technology', POSTbrief 32 (2019)
7 Qq14 and 280
8 Ministry of Housing, Communities and Local Government and Department for Digital, Culture, Media and Sport, 'Proposed reforms to permitted development rights to support the deployment of 5G and extend mobile coverage' (2019), para 10
9 Q2—see also: Future Communications Challenge Group, 'UK strategy and plan for 5G & Digitisation—driving economic growth and productivity' (2017)

Huawei.[10] With regards to network security, Huawei has been classified as a high-risk vendor by the National Cyber Security Centre because, in combination with other relevant criteria, it is a "Chinese company that could, under China's National Intelligence Law of 2017, be ordered to act in a way that is harmful to the UK" and because the National Cyber Security Centre has concluded that the "Chinese State (and associated actors) have carried out and will continue to carry out cyber attacks against the UK and our interests".[11] Consequently, the Government decided in January 2020 that Huawei (and any other high-risk vendors) would be excluded from supplying equipment to sensitive 'core' parts of 5G and gigabit-capable networks,[12] and capped at supplying 35% of the equipment used in non-sensitive parts of these networks.[13] Although these conditions were initially advisory, the Government said that it would "seek to legislate at the earliest opportunity to put in place the powers necessary to implement this tough new telecoms security framework".[14]

3. On 15 May 2020, the US Department of Commerce announced new sanctions aimed at restricting Huawei's ability to use US technology and software to design and manufacture its semiconductors abroad.[15] Professor Ciaran Martin, former Chief Executive Officer of the National Cyber Security Centre, explained to us that these sanctions "effectively exclud[e] Huawei from purchasing anything with US intellectual property in it, particularly microchips from all over the world".[16] He added that this had demonstrated the "power of the US legal system and sanctions system", and suggested that—given the long timescales for managing telecommunications security—the UK should seek to adopt its strategy independently of the US administration in power at any moment.[17] In its assessment of the consequences of the US sanctions for telecommunications network security in the UK, the National Cyber Security Centre concluded that they:

- would limit the ability of Huawei to send its equipment to the Huawei Cyber Security Evaluation Centre for analysis, preventing the "functioning of the UK's security mitigation strategy with Huawei";
- could require Huawei to devote significant engineering focus on designing replacements for restricted components, reducing the company's ability to address ongoing cybersecurity issues; and

10 Department for Digital, Culture, Media and Sport, 'UK Telecoms Supply Chain Review Report' (2019), paras 4.5–4.12

11 National Cyber Security Centre, 'NCSC advice on the use of equipment from high risk vendors in UK telecoms networks', published 28 January 2020, paras 9–10 and 13—the National Cyber Security Centre stated that "Huawei has always been considered higher risk by the UK government and a risk mitigation strategy has been in place since they first began to supply the UK".

12 The 'core' of a 5G network refers to the more sensitive parts of the network, which are typically responsible for identifying users, controlling where information in the network flows, determining what services users receive and managing billing—see: National Cyber Security Centre, 'Security, complexity and Huawei; protecting the UK's telecoms networks', published 22 February 2019

13 'New plans to safeguard country's telecoms network and pave way for fast, reliable and secure connectivity', Department for Digital, Culture, Media and Sport, accessed 28 September 2020

14 'New plans to safeguard country's telecoms network and pave way for fast, reliable and secure connectivity', Department for Digital, Culture, Media and Sport, accessed 28 September 2020

15 'Commerce Addresses Huawei's Efforts to Undermine Entity List, Restricts Products Designed and Produced with U.S. Technologies', US Department of Commerce, accessed 1 October 2020—see also: Federal Register, vol 85 no. 97 (2020), pp29849–29863

16 Q315

17 Q335—see also: Qq266 and 358

- did not affect the support and maintenance of existing equipment, but indicated a "direction of travel" that might "limit Huawei's support for existing equipment" in the future.[18]

Based on these conclusions, the National Cyber Security Centre recommended that UK network operators should not use any 5G access equipment supplied by Huawei after implementation of the US sanctions. The Secretary of State for Digital, Culture, Media and Sport, Rt Hon Oliver Dowden MP, consequently told the House of Commons on 14 July 2020 that "from the end of this year, telecoms operators must not buy any 5G equipment from Huawei", and that "once the Telecoms Security Bill is passed it will be illegal for them to do so".[19]

4. As a result of these intended measures, the UK 5G access equipment market will have just two major suppliers, Nokia and Ericsson. The National Cyber Security Centre warned that "only having two suppliers into all national mobile networks reduces network resilience and security".[20] Dr Ian Levy, Technical Director of the National Cyber Security Centre, explained the security risks associated with having too few vendors in more detail:

> The first is strategic dependence. If you have only two vendors, and it is hard to switch between them and anyone else, you are reliant on them for everything. If one of them goes out of business or starts to do interesting commercial practices, you have a resilience risk for the long-term security and resilience of the network. The second is a systemic risk, in that it is very hard to build resilient networks—we are talking about the systems, rather than individual components—with just two vendors for the whole of the UK. Obviously, if there is a vulnerability or a failure in a particular piece of equipment, that is much more impactful in the UK if you have only that piece of equipment and one other type. It also means that you reduce innovation, competition, security pressure, feature pressure and so on, so you end up with quite a stagnant market.[21]

Dr Levy indicated that the Government should aim to have "at least three" vendors in the near term, and that over time it should aim for a wide variety of vendors supplying software and "maybe five, six, seven" radio access equipment vendors.[22]

5. Recognising the risks associated with too few vendors, the Government has published a strategy for diversifying the telecommunications vendor market.[23] The Secretary of State for Digital, Culture, Media and Sport, Oliver Dowden MP, has said that this strategy, in combination with strengthened regulation of network security,[24] would "lay the foundations for a world-class telecoms security framework".[25]

18 'Summary of the NCSC analysis of May 2020 US sanction', National Cyber Security Centre, accessed 1 October 2020
19 HC Deb, 14 July 2020, col 1375
20 'Summary of the NCSC analysis of May 2020 US sanction', National Cyber Security Centre, accessed 1 October 2020
21 Q428—see also: Vodafone UK (UKT0002)
22 Q429
23 Department for Digital, Culture, Media and Sport, '5G Supply Chain Diversification Strategy' (2020)
24 Telecommunications (Security) Bill [Bill 216 (2019–2021)]
25 Department for Digital, Culture, Media and Sport, '5G Supply Chain Diversification Strategy' (2020)

Our inquiry

6. We launched our inquiry on 9 April 2020 with a call for evidence on UK telecommunications infrastructure and the UK's domestic capability.[26] We published 37 written submissions and took oral evidence from 23 witnesses, including mobile network operators, telecommunications equipment vendors, the Chair of the Government's Telecoms Diversification Taskforce and the Secretary of State for Digital, Medial, Culture and Sport, Oliver Dowden MP. To assist us with our work, we appointed James Sullivan, Head of Cyber Research at the Royal United Services Institute, as a Specialist Adviser for our inquiry.[27] We are grateful to everyone who contributed to our inquiry.

Aims of this Report

7. The National Cyber Security Centre has made clear the urgency of addressing the lack of vendor diversity and the risks posed by the UK having two vendors.[28] In this Report we make a number of recommendations which require urgent action to address the lack of diversity in the 5G infrastructure market. Our urgent recommendations include, but are not limited to:

- **The need to learn from others internationally so that we do not fall behind**: actions to address this should include the UK evaluating initiatives by other countries such as the deployment of Open RAN and steps taken to diversify the vendor market (paragraphs 31–33);
- **The need to invest in research and development**: the £250 million allocated by the Government for 5G vendor diversification—in comparison to the tens of billions of pounds spent on research and development by incumbent vendors—underlines the scale of the challenge in achieving diversification (paragraphs 37–44);
- **The need for greater international collaboration and action**, particularly in the context of a potentially growing technological and regulatory divergence between the West and China, the Government needs to look to establish a forum for international collaboration (paragraphs 75–80); and
- **The need to avoid the UK getting into a similar situation in the future**: we call on the Government to develop a National Critical Technologies Strategy (Chapter 3).

Specifically:

- in Chapter 2, we review the major barriers to entry for companies seeking to enter the UK telecommunications vendor market, and assess the extent to which the Government's *5G Supply Chain Diversification Strategy* addresses these barriers; and

26 House of Commons Science and Technology Committee, 'Science and Technology Committee launches three new inquiries', published 9 April 2020

27 James Sullivan declared his interests on 9 July 2020: full-time salaried member of staff at the Royal United Services Institute.

28 National Cyber Security Centre, 'Summary of the NCSC analysis of May 2020 US sanction', published 14 July 2020 and Q428

- in Chapter 3 we seek to draw lessons from the UK's recent experience in the telecommunications sector to identify what the Government can do to avoid similar problems with other technologies and sectors.

2 The 5G Supply Chain Diversification Strategy

8. This Chapter discusses the long-term factors that led to the concentration of vendors in the UK telecommunications market today, as well as the current barriers to companies trying to enter the UK's market. It identifies which proposals in the Government's *5G Supply Chain Diversification Strategy* might address these barriers, how adequate they might be, and what other measures were suggested during our inquiry. Finally, it considers other important features for a successful diversification strategy, including alignment with 5G roll-outs and international co-operation.

The Government's diversification strategy

9. The Government's *5G Supply Chain Diversification Strategy* sets out twelve broad proposed actions for diversifying the UK's telecommunications equipment vendor market, broken down into three broad 'strands':

- supporting incumbent suppliers to ensure their resilience and ability to supply the market in the near term, while supporting their transition into the emerging market structure;
- attracting new suppliers into the UK market to build resilience and competition, prioritising deployments that are in line with the Government's longer-term vision for the market; and
- accelerating open-interface solutions and deployment so that the UK is not reliant on any single vendor and begins to realise the Government's long-term vision for a more open and innovative market.[29]

Prior to the full strategy's publication, Professor Ciaran Martin, former Chief Executive Officer of the National Cyber Security Centre, told us that the Government had identified the "right three pillars" and that the outlined strategy was "definitely […] the right strategy".[30] Following the strategy's publication, Mobile UK, the trade association for the UK's mobile network operators, described it as a "very positive development for the sector and the wider UK economy" but said that it "must be given time to bear fruit".[31]

10. The details of the Government's diversification strategy are assessed in the remainder of this Chapter. It is worth noting, however, that the Government concedes that its strategy represents a "long term plan" and that the "supply market in the UK will be dependent on Nokia and Ericsson for the foreseeable future".[32] Indeed, the Secretary of State for Digital, Culture, Media and Sport, Oliver Dowden MP, committed to us only that the effects of diversification would start to be seen by the end of this Parliament.[33] This timeframe, and the strategy's recent publication, sit in the context of a warning from the then Intelligence and Security Committee in 2013 that:

29 Department for Digital, Culture, Media and Sport, '5G Supply Chain Diversification Strategy' (2020), para 3.7
30 Q323
31 Mobile UK, 'Mobile UK Welcomes New 5G Supply Chain Diversification Strategy', published 30 November 2020
32 Department for Digital, Culture, Media and Sport, '5G Supply Chain Diversification Strategy' (2020), paras 1.6 and 3.5
33 Q285—see also: HC Deb, 10 March 2020, cols 168–216

> [The] Government must be clear what its strategy is when it comes to deployment of equipment—particularly where this has been developed or manufactured by foreign companies—within the UK's critical national infrastructure and have effective processes in place for considering these issues.[34]

In its report on Huawei's involvement in BT's network infrastructure, the then Intelligence and Security Committee found that "officials chose not to refer [BT's notification that it intended to install Huawei's equipment] to Ministers, or even inform them, until 2006, a year after the contract had been signed" and concluded that the "process for considering national security issues at that time was insufficiently robust".[35]

11. The origins of the recent diversification strategy lie in the then UK Government's *Telecoms Supply Chain Review* in 2018,[36] which first led to the stated objective of diversifying the UK's telecommunications vendor market.[37] Dr Ian Levy, Technical Director at the National Cyber Security Centre, told us in October 2020 that the "market conditions" and "technology conditions" for driving diversification were less suitable for intervention "until a year ago", but accepted that the Government nevertheless "could have" started considering interventions sooner than it has.[38] For example, as discussed later in this Chapter, one potential measure that could have been considered was to introduce minimum vendor diversity requirements on network operators (see paragraph 68), but this would require a sufficient number of vendors to exist in the market.[39] While there are now only three major vendors for 5G and shortly there will be two, the UK market had over ten vendors in 2010 prior to consolidation lasting the previous ten to twenty years.[40] In advance of the publication of the Government's diversification strategy, Amy Karam, a Fellow of the Canadian Global Affairs Institute, described the Government's strategy as a "catch-up strategy".[41]

12. Several witnesses contrasted China's approach to industrial policy for telecommunications with those of Western countries. Professor Martin explained to us that China was a "big single-nation state of 1.5 billion people with central planning" that could "do things that multiple disparate democratic countries cannot in terms of long-term planning".[42] Amy Karam similarly told us that China had been "very driven" and used "assertive policy" to work towards "big goals".[43] Acknowledging that China "played on terms we do not play on", she nevertheless suggested that the West had to "shift the mindset from free markets to how we help national security with economic security policies":

34 Intelligence and Security Committee, 'Foreign involvement in the Critical National Infrastructure' (2013), para 3
35 Intelligence and Security Committee, 'Foreign involvement in the Critical National Infrastructure' (2013), paras 13 and 16
36 Department for Digital, Culture, Media and Sport, 'Telecoms Supply Chain Review: Terms of Reference' (2018)
37 Department for Digital, Culture, Media and Sport, 'UK Telecoms Supply Chain Review Report' (2019) and Department for Digital, Culture, Media and Sport, '5G Supply Chain Diversification Strategy' (2020)
38 Q472
39 For example, see: Qq328 and 430–431
40 See: Spirent plc (UKT0001); Parallel Wireless and Isotek Microwave (UKT0013); Institution of Engineering and Technology (UKT0036) and Qq45, 219, 315 and 342
41 Q218
42 Q340
43 Q225

> Industrial policy has not been a very attractive term [in the West]; maybe we should do industrial policy 2.0 in order to foster the closer Government-private sector relationship that is really necessary. Where China succeeded was in that tight coupling. The Chinese Government helped catapult Huawei to a global leader because they facilitated that growth.[44]

Parallel Wireless and Isotek Microwave explained that over the same period that China had invested hundreds of billions of pounds into microelectronics innovation, the West had reduced its investment in this area.[45] These observations, combined with the timescales for diversification projected by the Government, point to the scale of the challenge.

13. While the Government's diversification strategy provides an overview of the measures that it intends to use to diversify the 5G infrastructure equipment vendor market, the strategy does not detail how the £250 million that it has been initially allocated will be used and does not set out an action plan with clear milestones or timeframes for achieving the Government's goals. Making these points to the Public Bill Committee for the Telecommunications (Security) Bill in January 2021, Matthew Evans, Director of Markets at techUK, described it as a "strategy and not a complete plan", and highlighted that "we do not yet know how the £250 million is going to be spent".[46] DLA Piper, a global law firm, has similarly commented that there was "currently little published guidance on who can specifically access the proposed £250 million funding".[47]

14. **The Government's '5G Supply Chain Diversification Strategy' provides an overview of the Government's intentions for addressing the current lack of vendors in the UK's 5G infrastructure equipment market. The Government itself acknowledges that this will take time. Although the decision to forbid the use of 5G equipment procured from Huawei after 2020 was made following US sanctions announced in May 2020, the potential threat from telecommunications infrastructure supplied by foreign vendors and the concentration in the UK's vendor market have been known for many years. It is therefore disappointing that the Government and its predecessors have not already developed and started implementing a strategy for diversifying the UK's telecommunications infrastructure supply chain. *Given the scale of the challenge and the urgency of the threat, the Government should publish, within three months, a more detailed action plan for implementing its diversification strategy. This should include a breakdown of how the initial budget will be spent and a series of milestones with target dates for completion.***

Barriers to market entry

15. A range of challenges facing companies trying to enter the UK's telecommunications vendor market was raised during our inquiry, including:

- a lack of interoperability between equipment from different vendors;[48]

44 Q221
45 Parallel Wireless and Isotek Microwave (UKT0013)
46 Oral evidence taken before the Public Bill Committee for the Telecommunications (Security) Bill on 14 January 2021, PBC (Bill 216) 2019–2021, Qq31 and 37
47 DLA Piper, 'UK Government publishes its 5G Supply Chain Diversification Strategy', published 2 December 2020)
48 For example, see: Vodafone UK (UKT0002); Samsung Electronics UK (UKT0008), section 2; techUK (UKT0020); UK Photonics Leadership Group (UKT0026); Compound Semiconductor Applications Catapult (UKT0032)

- operators' aversion to risk leading them to prefer established vendors;[49]
- the high levels of investment in research and development required to compete with established vendors;[50]
- the scale of telecommunications networks, requiring new vendors to provide large volumes of equipment soon after they go to market;[51] and
- the possession of necessary intellectual property by incumbent vendors.[52]

The Government identified a similar list of barriers to market entry in its diversification strategy.[53] Although the strategy set out a range of proposals intended to drive market diversification, it did not explicitly link each of these proposals to specific barriers to entry. In the following sections, we consider each barrier and examine the extent to which they are addressed by the Government's proposals.

Interoperability

16. Representatives of Samsung, Vodafone and BT all told us that the greatest barrier for vendors established in other markets trying to enter the UK market was the UK network operators' requirement for new 5G equipment to work alongside existing 2G, 3G and 4G equipment.[54] Howard Watson, Chief Technology and Information Officer at BT Group, informed us that 50% of BT's customers use 2G and 3G networks.[55] Andrea Dona, Head of Networks at Vodafone, said that Vodafone was in a similar position and that this meant that new equipment had to work alongside older generation equipment.[56] Samsung argued that this presented a "barrier to any new entrants that have not already been manufacturing the old 2G and 3G equipment (developed back in the 1990s), whereas it is an inbuilt advance to those vendors who were manufacturing back in that era":

> Samsung, for instance, does not make 2G and 3G network products. To do so now would mean investing in the development of old technology and then providing it free of charge, taking away research and development investment from areas where innovation is justified, like 5G and 6G.[57]

17. Recognising this challenge, the second strand of the Government's diversification strategy included work to "set out a clear roadmap for the long term use and provision of 2G, 3G and 4G network services in the UK—including consideration of options to sunset or streamline provision".[58] Discussing a possible transition away from older generation technologies, Dr Yih-Choung Teh, Group Director for Strategy and Research at Ofcom,

49 For example, see: Spirent plc (UKT0001); National Physical Laboratory (UKT0007), para 7; BT Group (UKT0019), para 19; techUK (UKT0020) and Q464
50 For example, see: Spirent plc (UKT0001); Samsung Electronics UK (UKT0008); BT Group (UKT0019), para 7; Internet Service Providers' Association (UKT0023), para 8; Digital Catapult (UKT0037) and Q450
51 For example, see: UK Photonics Leadership Group (UKT0026); Digital Catapult (UKT0037) and Q402
52 For example, see: National Physical Laboratory (UKT0007), para 22 and Q359—see also: oral evidence taken before the Defence Committee on 28 July 2020, HC 201, Q277
53 Department for Digital, Culture, Media and Sport, '5G Supply Chain Diversification Strategy' (2020), para 2.12
54 Qq123 and 143
55 Q143
56 Q143
57 Samsung Electronics UK (UKT0008), section 2
58 Department for Digital, Culture, Media and Sport, '5G Supply Chain Diversification Strategy' (2020), para 3.12

told us that this was a "very live question", which "operators are very keen to work on".[59] However, he cautioned that making progress on this would take "quite a lot of time" because of the "various legal and commercial questions in that migration", the scale of "logistical things that you have to co-ordinate", and the consideration of end-use cases that depended on older generation technologies, including consumer phones, business-to-business applications and critical national infrastructure applications such as smart metering and emergency communications.[60] Dr Teh did not expand on any potential solutions to any of these issues, suggesting that Ofcom did not yet have a well-developed approach in mind for managing transitions away from legacy technologies.

18. Making the case for shorter-term measures to address the challenge of interoperability with older generations of technology, Samsung identified two options:

- swapping out old 4G equipment for new equipment combining 4G and 5G capability, while preserving existing 2G and 3G equipment; and
- using the 'Open X2' interface to enable 5G equipment from one vendor to be overlaid on 4G equipment from another vendor.[61]

19. Samsung told us that it was in the process of deploying the first option in Canada and New Zealand, but that this was more difficult in the UK because network operators had mostly installed infrastructure combining 2G, 3G and 4G equipment together.[62] This could be overcome, we heard, with 'standalone' deployments of 5G networks, which do not require an underlying 4G network to work, but UK operators were currently deploying non-standalone deployments, which do require the 4G network.[63] Representatives from BT Group and Vodafone outlined three main reasons why they had opted for non-standalone deployment models for their initial roll-outs of 5G:

- the industrial roadmap for 5G envisioned a transition from 4G to non-standalone 5G followed by standalone 5G, meaning that non-standalone 5G standards were developed first;
- standalone networks require larger bands of continuous spectrum (spectrum refers to the different radio frequencies that each company is allowed to use to provide their networks);[64] and
- they perceive there to be fewer vendors offering standalone-compatible equipment.[65]

techUK agreed that non-standalone networks were cheaper and quicker to set up, but warned that they "reinforce the interoperability challenges that exist in certain regions between telecommunications vendors".[66] Dr Yih-Choung Teh, Group Director for Strategy and Research at Ofcom, told us that ultimately, UK operators would start deploying

59 Q458
60 Qq457–458
61 Samsung Electronics UK (UKT0029)
62 Samsung Electronics UK (UKT0008) and (UKT0029)
63 techUK (UKT0020) and Q3—see also: National Cyber Security Centre, 'Security, complexity and Huawei; protecting the UK's telecoms networks', published 22 February 2019
64 For a more detailed explanation, see: Parliamentary Office of Science and Technology, 'Radio spectrum management', POSTnote 292 (2007)
65 Qq189–190 and 193–196
66 techUK (UKT0020)

standalone 5G networks because "if you want to access the benefits and features that 5G offers us—for example, ultra-low latency—that needs to be built on a standalone 5G core".[67] Mr Watson, representing BT Group, suggested that this could start in 2021 at the earliest, although Professor Dimitra Simeonidou, Professor of High Performance Networks at the University of Bristol, suggested that it could be "three to four years at least" until full roll-outs of standalone 5G were possible.[68] The Secretary of State for Digital, Culture, Media and Sport, Oliver Dowden MP, indicated to us in July that he had an "open mind" with regards to introducing requirements on operators to deploy standalone 5G networks.[69]

20. With regards to the second of its proposed options, Samsung said that it had already used the Open X2 interface to deploy equipment in the Republic of Korea.[70] However, techUK, a trade association for the digital technology sector, told us that "compared to several other countries the UK has fewer open interfaces between 4G and 5G" and agreed that "some market players see this as a barrier to multi-vendor integration".[71] Dr Ian Levy, Technical Director at the National Cyber Security Centre, told us that adopting the Open X2 interface was not a "particularly hard technical problem" but was a "much harder commercial incentive problem":

> If you think about what you are asking, you are saying to, for the sake of argument, Huawei, 'tell us exactly how your 4G to 5G interface works so that we can take away your market'. That is effectively what you are asking them to do. Remember that both sides of the X2 interface have to co-operate, so whoever's 4G platform you are trying to plug the Samsung thing into has to co-operate as well. There is a real commercial incentive question around that.[72]

Dr Levy suggested that this was the "sort of thing that we have to address as we go forward in diversification and interoperability, so that there is a sensible set of incentives for every party in the system".

21. Although the Government's diversification strategy refers to the increased use of open interfaces, it mostly presented this as a longer-term solution.[73] Correspondingly, its proposed actions for encouraging open interfaces, such as establishing testing facilities and building capability in standards setting, largely focus on developing new technologies and stimulating a new ecosystem over the longer-term.[74] There were no proposed measures that addressed the commercial challenges raised by Dr Levy.

22. **The Government is seeking to attract existing vendors to the UK market in order to diversify the telecommunications vendor market in the short-term. One of the major barriers faced by such companies is the requirement of British network operators for**

67 Q459
68 Qq14 and 193
69 Qq282–283
70 Samsung Electronics UK (UKT0029)
71 techUK (UKT0020)
72 Q459
73 Department for Digital, Culture, Media and Sport, '5G Supply Chain Diversification Strategy' (2020), paras 2.17, 2.22, 2.25–2.29, 2.31, 3.1 and 3.7
74 Department for Digital, Culture, Media and Sport, '5G Supply Chain Diversification Strategy' (2020), paras 3.17–3.23

continued provision of older generations of network technology. The main proposal in the Government's diversification strategy to address this—to consider a transition away from these older technologies—is not a short-term solution.

23. ***In addition to considering the case for transitioning away from 2G and 3G technologies, the Government should propose measures within the next six months that could facilitate market entry by existing vendors in the near-term. It should consider options for addressing the barrier of operators' preference for vendors to offer older generation technologies with their 5G equipment, such as incentivising or mandating standalone 5G deployments and/or the use of protocols such as the Open X2 interface.***

24. In the longer-term, the Government hopes to deliver a telecommunications market with distributed, disaggregated supply chains and widespread use of open interfaces and standards that allow different vendors to provide different components of an overall system.[75] Dr Levy, Technical Director at the National Cyber Security Centre, explained that the Government wanted to achieve the same "modularisation and interoperability" in the telecommunications market as is found currently with the Internet, where "you can have an IBM laptop or an Apple laptop, and they both work on the Internet in the same way".[76] This vision is strongly associated—by the Government and by other stakeholders—with the 'Open RAN' movement (see Box 1), although the Government' strategy was careful to clarify that Open RAN was just one possible route to open standards and increased interoperability.[77]

Box 1: Open RAN

Open RAN stands for 'open radio access network'. The Telecoms Infra Project, a membership body working on Open RAN, explained that the radio access network (RAN) equipment comprises the "masts, antennas and associated parts that mobile network operators use to connect wirelessly with mobile devices like smartphones". The Open RAN Policy Coalition, an industry membership group promoting Open RAN explains that in a "traditional RAN system, the radio, hardware and software are proprietary", meaning that "nearly all the equipment comes from one supplier and operators are unable to, for example, deploy a network using radios from one vendor with hardware and software from another vendor". In contrast, Open RAN "allows networks to be built using subcomponents from a variety of vendors":

> The key concept of Open RAN is 'opening' the protocols and interfaces between the various subcomponents (radios, hardware and software) in the RAN […] By opening and standardising these interfaces (among others in the network), and incentivising implementation of the same, we move to an environment where networks can be deployed with a more modular design without being dependent upon a single vendor.

Andrea Dona, Head of Networks at Vodafone, told us that Open RAN makes it easier for companies to enter the market, because they only have to supply one component of the RAN setup, rather than the entire system.

Source: Telecom Infra Project (UKT0018), Q182 and Open RAN Policy Coalition, 'What is Open RAN?' (2020)

75 Department for Digital, Culture, Media and Sport, '5G Supply Chain Diversification Strategy' (2020), paras 2.17 and 2.23–2.31

76 Q429

77 Department for Digital, Culture, Media and Sport, '5G Supply Chain Diversification Strategy' (2020), para 2.31

25. We heard strong support for wider use of open standards and greater interoperability during our inquiry.[78] For example, techUK told us that interoperability "allows operators to buy equipment from different vendors as certain elements of telecom networks are separated out", which "opens the door for smaller vendors".[79] The Digital Catapult argued that a "more open and disaggregated supply chain across the key network components" would lead to networks supplied by a "multi-vendor chain for the different segments", rather than the "largely end-to-end single provider situation like today".[80] Dr Ian Levy, Technical Director at the National Cyber Security Centre, further observed that interoperability and openness would facilitate greater scrutiny of equipment by external security researchers:

> If I want to do security research on a base station [today], it is going to cost me about £1 million to spin it up. That changes as you move to much more software and virtualisation. I can run a base station on my laptop to do security research. So you get a very positive effect of security researchers globally looking at this equipment and helping vendors make it better, just like we have done in commodity IT for the last 10 years.[81]

Mavenir similarly argued that Open RAN would allow "multiple independent parties to continuously test the security of the network elements and the system".[82]

26. Although many of those supporting open standards and interoperability presented Open RAN as the major or only way to achieve this, Marcus Weldon, President of Bell Labs and Chief Technology Officer at Nokia, echoed the Government's caution and told us that that Open RAN was only "one option" for achieving better interoperability.[83] He argued that governments should promote the concept of open standards rather than supporting specific organisations or movements trying to achieve it (without focusing on Open RAN, the Internet Service Providers Association similarly said that the Government should "define principles rather than prescriptive measures to allow those regulated the flexibility to meet the principles in the format that is most relevant to their business and risk assessment").[84] Woojune Kim, Executive Vice-President of Samsung, additionally noted that "Open RAN can be interpreted in a lot of ways".[85]

27. We also heard of some potential risks with increased interoperability and use of open standards. BT Group warned us that although "new approaches, such as Open RAN, offer the potential" for wider adoption of open standards, it considered that it was "as yet unclear whether these will be successful".[86] Many others warned that it would take several years before it could be ready for widespread adoption.[87] Others have warned that

78 For example, see: Spirent plc (UKT0001); Vodafone UK (UKT0002); Dr Dimitris Kaltakis (UKT0004); Huawei Technologies (UKT0005); Samsung Electronics UK (UKT0008); techUK (UKT0020); UK Photonics Leadership Group (UKT0026); Compound Semiconductor Applications Catapult (UKT0032); Juniper Networks (UKT0033); Digital Catapult (UKT0037); Mavenir (UKT0038) and Qq221, 328, 421 and 460

79 techUK (UKT0020)

80 Digital Catapult (UKT0037)

81 Q463

82 Mavenir (UKT0038)

83 Q348—see also: Q460

84 Q348 and Internet Services Providers' Association (UKT0023), para 10

85 Q125

86 BT Group (UKT0019), para 21

87 For example, see: Vodafone UK (UKT0002); BT Group (UKT0019), paras 22–23; techUK (UKT0020); Samsung Electronics UK (UKT0029); Juniper Networks (UKT0033) and Q246—see also: oral evidence taken before the Defence Committee on 28 July 2020, HC 201, Q299

the Open RAN movement, or any other similar approach, could end up being dominated by incumbent vendors.[88] Further, even if open standards and greater interoperability are achieved, there is no guarantee that the companies selling network equipment components will not share the same attributes as high-risk vendors.[89]

28. Some have highlighted that it is also important that moves towards open standards and interoperability improve the overall security of 5G networks, not just the diversity of equipment vendors.[90] Dr Levy acknowledged that "with any complicated technical standard, there are always risks", and that Open RAN or similar initiatives could "potentially" pose risks to overall security.[91] For example, the Wilson Center, a non-partisan US-based think tank, has argued that the "greater the diversity of vendors in a network, the more complex the ecosystem" and that "mixing and matching hardware and software introduces new opportunities for vulnerabilities and unanticipated failures".[92]

29. **The Government is right to support the development and adoption of open standards and increased interoperability as a potential means of diversifying the telecommunications equipment vendor market. It is also right to identify Open RAN as a prominent approach to achieving this, but not the only one. However, neither the success of Open RAN or any related efforts, nor the positive impact on overall telecommunications security if these efforts are successful, is guaranteed.**

30. ***The Government should support Open RAN and other efforts to drive the adoption of open standards and greater interoperability. While the success of Open RAN is not guaranteed, the Government should encourage the deployment of Open RAN to ensure that the UK is not behind others in deploying this technology. However, it must continually ensure that support for these efforts is consistent not only with increasing vendor diversity but also with improving the overall security of the UK's telecommunications networks. Further, the Government must not assume that open standards and interoperability will inevitably be adopted nor that they will have the desired effect, and should pursue a range of measures designed to support market diversification and increase security.***

31. Despite the uncertainty and timeframes commonly associated with Open RAN, Rakuten Mobile, a Japanese mobile network operator, reported launching the world's first commercial Open RAN network in 2020.[93] Tareq Amin, Chief Technology Officer at Rakuten Mobile, told us that this approach had already enabled Rakuten Mobile to diversify the vendors that it used in its 5G network.[94] Lord Livingston, Chair of the Government's Telecoms Diversification Taskforce, noted that Open RAN network deployments were also being pursued in India and in the USA.[95]

88 Iain Morris, 'Open RAN is vulnerable to an Ericsson, Nokia takeover', published 10 June 2020 and Caroline Gabriel, 'There are high hurdles to leap before operators get a truly open RAN', published 11 September 2020

89 Iain Morris, 'Open RAN Won't Stop China, Dotards', published 30 January 2020

90 Cisco, 'Security in Open RAN Networks', published 22 September 2020

91 Q461

92 Wilson Center, 'Open RAN and 5G: Looking Beyond the National Security Hype' (2020)—see also: Ericsson, 'Security considerations of Open RAN' (2020)

93 Q278—see also: Rakuten Mobile, 'Rakuten Mobile Announces Full-Scale Commercial Launch; Unveils Enhanced 'Rakuten UN-LIMIT 2.0' Service Plan', published 8 April 2020 and Rakuten Mobile, 'Rakuten Mobile Launches 5G Service with New Plan, Same Monthly Fee: Rakuten UN-LIMIT V', published 30 September 2020

94 Q416

95 Q404

32. Asked why Rakuten Mobile had managed to launch an Open RAN network when no British network operator had done so, Dr Yih-Choung Teh, Group Director for Strategy and Research at Ofcom, assured us that it was not due to any regulatory constraints.[96] Instead, he suggested that Rakuten had benefited from being a "brand-new player" that could "build from a greenfield site versus being an incumbent with a bunch of legacy technologies that you are going to be very keen to make sure you interface with".[97] Dr Ian Levy, Technical Director at the National Cyber Security Centre, agreed that Rakuten had benefited from a "virgin spectrum, virgin network and a complete greenfield site", and observed that there was not, in his opinion, a "huge amount of money in the UK telecoms sector at the moment", which he said might deter operators from pursuing similar roll-outs here (this point is revisited later in this Report).[98]

33. **The first live networks using Open RAN are being deployed, with one having launched in Japan last year. *The Government should evaluate these initiatives and report regularly on what lessons can be learned from foreign experiences to inform the UK's strategy for diversifying the vendor market and improving telecommunications security, with an initial report within the next six months.***

Reliability

34. We heard during our inquiry that network operators required very high reliability from the equipment they procured and therefore preferred vendors with a proven track record and with whom they had an established relationship.[99] BT Group explained that the complex process of testing and integrating new equipment into existing networks to ensure reliable operation was "considerably more involved when introducing a completely new supplier" than when using an established vendor:

> Any new supplier would need to demonstrate, to a very high degree of surety, the capabilities of their equipment to perform effectively in a live network environment, potentially interworking with multiple versions of existing equipment and network variations. Such testing and confirmation takes considerable time and resource from both the supplier and the network operator as customer.[100]

The Government similarly observed the impact of "operator risk aversion", which it said made operators "less willing to purchase from new, less known vendors with less mature products" such that "track record and established relationships with operators reinforce incumbent suppliers' market positions".[101]

96 Q454
97 Q454
98 Q456
99 For example, see: Spirent plc (UKT0001); BT Group (UKT0019), paras 9, 19 and 23; techUK (UKT0020); Internet Service Providers' Association (UKT0023), para 7
100 BT Group (UKT0019), para 19
101 Department for Digital, Culture, Media and Sport, '5G Supply Chain Diversification Strategy' (2020), para 2.12

35. The Government's *5G Supply Chain Diversification Strategy* outlined two principal proposals to address this barrier:

- the development and introduction of "appropriate regulatory adjustments regarding performance and resilience requirements", to minimise the disincentive to network operators of integrating new suppliers into their networks; and
- the establishment of testing facilities and related trials, to "create a dynamic and vibrant proving ground in the UK for operators and suppliers to test and demonstrate the performance and capabilities of interoperable solutions", including a National Telecoms Lab to "create a unique testing environment for operators and suppliers to match their requirements and specifications to assess the technical performance and security of equipment in representative networks", which the Government hopes will be "particularly beneficial for new and emerging suppliers, offering them a unique opportunity to demonstrate their viability".[102]

Although more details will be required, these proposals align with recommendations from many of the contributors to our inquiry.[103] The National Physical Laboratory warned us, however, that testing facilities would have to be large-scale to provide adequate testing of equipment prior to deployment.[104]

36. **We heard evidence during our inquiry supporting the Government's assessment that network operators' preference for vendors with proven track records acts as a barrier to potential market entrants. The Government's proposals to establish testing and validation facilities, and to reduce regulatory disincentives for network operators to integrate new vendors into their networks, align with the recommendations for addressing this barrier made by many of the contributors to our inquiry. *Following consultation with industrial and other stakeholders, the Government should report on the required scale and specification of the National Telecoms Lab, to ensure that network operators trust the equipment that it validates for integration into their networks.***

Research and development

37. The scale of investment into research and development required to enter the telecommunications vendor market was raised by a variety of contributors to our inquiry.[105] BT Group told us that the development of 5G and related technologies had required "significant investment in research, development, manufacturing and global standards", with the result that a "key barrier to any new entrant to this market […] would be the scale of investment necessary to develop, deliver and continually evolve equipment in this market".[106] The Government's diversification strategy similarly found that the "high levels

102 Department for Digital, Culture, Media and Sport, '5G Supply Chain Diversification Strategy' (2020), paras 3.12–3.13, 3.16, and 3.18–3.20

103 For example, see: Spirent plc (UKT0001); National Physical Laboratory (UKT0007), paras 7, 15 and 20; techUK (UKT0020); UK Photonics Leadership Group (UKT0026); Institution of Engineering and Technology (UKT0036); Digital Catapult (UKT0037) and Qq325, 328 and 330

104 National Physical Laboratory (UKT0007), para 7

105 For example, see: Spirent plc (UKT0001); Samsung Electronics UK (UKT0008); BT Group (UKT0019), paras 7, 14 and 18; techUK (UKT0020); Internet Service Providers' Association (UKT0023), para 8; Rushmere Technology Limited (UKT0025), para 7; Digital Catapult (UKT0037)

106 BT Group (UKT0019), para 18

of research and development investment required to compete in the RAN equipment market […] acts as a barrier to entry for prospective vendors that are unable to access the capital and resources required for such investment".[107]

38. Support for research and development was a major focus of the Government's proposals for diversifying the telecommunications vendor market.[108] The diversification strategy's proposals included:

- the establishment of a National Telecoms Lab to "independently test network equipment security, resilience and performance";
- the establishment of the SmartRAN Open Network Interoperability Centre, to "demonstrate and foster an open disaggregated network ecosystem in the UK"; and
- other measures intended to establish a "UK wide research and development ecosystem to accelerate and pull forward the development of interoperable technologies", such as funding for a variety of trials of new technologies and network architectures (including Open RAN) as well as initiatives bringing network operators, established vendors and new vendors together to collaborate on research and development.[109]

39. Several contributors to our inquiry discussed the funding available for research and development,[110] with some directly making the case for increased funding.[111] The Government committed £250 million to the initial implementation of its diversification strategy in the 2020 Spending Review.[112] This is significantly smaller than the sums that established vendors invest in research and development, with several contributors to our inquiry noting that Huawei alone spends around $20 billion on research and development every year.[113] It also appears to be smaller than the sums spent on existing facilities, with Dr Dritan Kaleshi, Head of 5G Technology at the Digital Catapult, telling us that the Catapult's facilities had cost £1.5 billion.[114] BT Group and techUK advocated targeting public funds on Open RAN projects,[115] which ultimately were a prominent feature of the Government's strategy.[116]

40. Parallel Wireless and Isotek Microwave argued that the Government should support investment in research and development rather than spending on replacing Huawei equipment, and recommended that it establish a £1 billion 'moonshot' research

107 Department for Digital, Culture, Media and Sport, '5G Supply Chain Diversification Strategy' (2020), para 2.12
108 Department for Digital, Culture, Media and Sport, '5G Supply Chain Diversification Strategy' (2020), paras 3.8–3.24
109 Department for Digital, Culture, Media and Sport, '5G Supply Chain Diversification Strategy' (2020), paras 3.18–3.20
110 For example, see: Spirent plc (UKT0001); Parallel Wireless and Isotek Microwave (UKT0013); Telecom Infra Project (UKT0018); techUK (UKT0020); Internet Service Providers' Association (UKT0023), para 10; Compound Semiconductor Applications Catapult (UKT0032); Mavenir (UKT0038) and Qq338 and 349
111 See: Parallel Wireless and Isotek Microwave (UKT0013); Telecom Infra Project (UKT0018) and Q50
112 HM Treasury, 'Spending Review 2020' (2020), para 6.86 and Department for Digital, Culture, Media and Sport, '5G Supply Chain Diversification Strategy' (2020), para 5.4
113 For example, see: Huawei Technologies (UKT0005); National Physical Laboratory (UKT0007), para 22 and Q450
114 Q249. The Digital Catapult has since informed the Committee that the figure is £1.5 million.
115 BT Group (UKT0019), para 24 and techUK (UKT0020)
116 Department for Digital, Culture, Media and Sport, '5G Supply Chain Diversification Strategy' (2020), paras 3.16 and 3.18–3.19

programme.[117] Several submissions advocated matched funding for research and development.[118] The Compound Semiconductor Applications Catapult suggested that a "percentage of licence revenues could be directed to accelerate UK research and development"—Ofcom is expected to raise at least £1.1 billion through auctioning the licences for 5G spectrum allocations in January 2021.[119]

41. Many recommended better co-ordination of research and development across academia and industry towards clearly-defined, long-term goals, with some—such as the Digital Catapult and Parallel Wireless and Isotek Microwave—recommending that the new research centres should develop defined research objectives and publish technological roadmaps.[120] The Internet Service Providers' Association suggested that the "Government leading on a co-ordinated approach to research and development" might be a "better use of resources" than seeking to add to existing industrial funding.[121] Indeed, the National Physical Laboratory informed us that their industrial partners complained of a "lack of visibility of academic research activity":

> There is a need for better two-way communication between our larger telecommunications providers and our smaller and medium sized businesses. Larger telecommunications providers have said that they have had difficulty in accessing smaller companies and being able to find out what they have to offer. The smaller companies state it is not clear what the larger telecommunications companies' requirements are, or their future plans—so it is difficult for them to anticipate and then meet their needs.[122]

The Digital Catapult similarly told us that existing initiatives to co-ordinate public and private research "remain fragmented".[123]

42. The Government's diversification strategy made several references to developing strategies for technological development and supporting collaboration between research efforts, including:

- working with trusted incumbent suppliers to "shap[e] relevant research and development activity" and "[align] technological roadmaps", to make their supply chains more resilient;[124]
- "plugfests" bringing together operators and suppliers to test and demonstrate equipment in representative networks;[125] and

117 Parallel Wireless and Isotek Microwave (UKT0013)
118 For example, see: Parallel Wireless and Isotek Microwave (UKT0013); Internet Service Providers' Association (UKT0023), para 10;
119 Compound Semiconductor Applications Catapult (UKT0032) and Ofcom, 'Award of the 700 MHz and 3.6–3.8 GHz spectrum bands' (2020), para 5.4
120 For example, see: National Physical Laboratory (UKT0007), para 17; Parallel Wireless and Isotek Microwave (UKT0013); BT Group (UKT0019), para 24; techUK (UKT0020); British Standards Institution (UKT0021), para 12; Internet Service Providers' Association (UKT0023), para 10; Institution of Engineering and Technology (UKT0036); Digital Catapult (UKT0037); Mavenir (UKT0038) and Qq228, 247 and 329
121 Internet Service Providers' Association (UKT0023), para 10
122 See: National Physical Laboratory (UKT0007), paras 7 and 11; Digital Catapult (UKT0037)
123 Digital Catapult (UKT0037)
124 Department for Digital, Culture, Media and Sport, '5G Supply Chain Diversification Strategy' (2020), para 3.10
125 Department for Digital, Culture, Media and Sport, '5G Supply Chain Diversification Strategy' (2020), para 3.18

- using the new SmartRAN Open Network Interoperability Centre as a "platform for existing and emerging suppliers to come together to test and demonstrate interoperable solutions", with the aim of building a "better understanding of technology readiness and maturity and challenges of Open RAN, to inform technology roadmaps and strategies".[126]

However, the strategy refers repeatedly to establishing a research and development "ecosystem", which implies an intention to foster a natural evolution of networks of collaborating stakeholders rather than the adoption of a more strategic approach driving co-ordination between stakeholders working towards well-defined long-term objectives.

43. **Measures to support research and development form a major part of the Government's '5G Supply Chain Diversification Strategy'. Nevertheless, the total funding of £250 million for initial implementation of the strategy is significantly smaller than the tens of billions of pounds invested annually in research and development by the main incumbent vendors. Co-ordination with existing academic and commercial research and development, with clear long-term objectives, will therefore be critical. The Government's reference to establishing a research and development "ecosystem" instead implies, however, a less strategic approach.**

44. ***The collaborative research and development networks that the Government seeks to develop to support diversification of the telecommunications market should encompass relevant groups at universities and research institutes as well as small- and medium-sized enterprises and large companies. The Government should aim to actively co-ordinate the research and development that it supports so that participants work towards clearly-defined long-term objectives. Existing and newly-established public research facilities should be set up to support this goal.***

45. A major component of the Government's proposed support for research and development appears to be the establishment of a range of new testing facilities, including the National Telecoms Lab and the SmartRAN Open Network Interoperability Centre. We heard broad support for the establishment of national testing facilities during our inquiry,[127] with contributors identifying a range of benefits they could provide, including:

- enabling market entrants to demonstrate the reliability of their equipment to network operators;[128]
- strengthening the UK's ability to contribute to the development of standards by enabling interoperability to be tested and developed;[129]
- providing shared facilities for smaller-scale companies and research groups with fewer resources;[130] and

126 Department for Digital, Culture, Media and Sport, '5G Supply Chain Diversification Strategy' (2020), para 3.19
127 For example, see: Spirent plc (UKT0001); National Physical Laboratory (UKT0007), paras 10 and 15; Institution of Engineering and Technology (UKT0036); Digital Catapult (UKT0037); Mavenir (UKT0038) and Qq16, 19–20, 30, 184–185, 328 and 330
128 For example, see: Spirent plc (UKT0001); BT Group (UKT0019), para 24; UK Photonics Leadership Group (UKT0026); Digital Catapult (UKT0037)
129 For example, see: Digital Catapult (UKT0037)
130 For example, see: National Physical Laboratory (UKT0007), para 20; BT Group (UKT0019), para 24; Digital Catapult (UKT0037)

- acting as a focal point to support collaboration and skills development.[131]

Discussing the last of these points, several witnesses, including Lord Livingston, Chair of the Government's Telecoms Diversification Taskforce, highlighted the importance of 'systems integrators' that co-ordinate and combine the components supplied by different vendors to offer a complete system to network operators.[132] This tied in with another barrier to market entry identified by the Government, namely the "outsourcing strategies of operators", which it said had led operators to increasingly rely on the "procurement of end-to-end services, which can only be offered by incumbent suppliers".[133]

46. Although a publicly-funded test centre is unlikely to be able to fully replace the system integrator role usually performed by companies such as Cisco or Fujitsu,[134] Dr Kaleshi suggested that the Digital Catapult was nevertheless providing some of this role in its existing facilities:

> In our 5G testbed […] we have deliberately gone down a non-vendor specific route, so we mix and match from different suppliers and we do the integration ourselves, which gives us the flexibility to engage very early on. It is a good playground for exploring these things very early on.[135]

Diane Rinaldo, Executive Director of the Open RAN Policy Coalition, argued that the UK's future facilities should also aim to provide this systems integrator role.[136] The UK Photonics Leadership Group has similarly recommended that the Government "provide dedicated collaborative research and development support to bring network, nascent equipment and component suppliers together to innovate and demonstrate UK network equipment solutions".[137] The Digital Catapult suggested that a focus on systems integration could accelerate the diversification achieved by the Government's strategy, while both the Catapult and the Institution of Engineering and Technology told us that systems integration was a strength of the UK's.[138]

47. The Government's diversification strategy stated that the National Telecoms Lab will act as a "hub for telecoms research and development activity across the UK" and will support efforts to "de-risk, enable and accelerate diversification".[139] It is not, however, clear that the Lab's focus extends to any of the roles illustrated above beyond testing reliability and validating equipment.[140] Dr Dritan Kaleshi, Head of 5G Technology at the Digital Catapult, told us, prior to the publication of the diversification strategy, that it appeared to him that the "National Telecoms Lab, as discussed at the moment, is primarily a facility to address the ability to do cybersecurity testing".[141] BT Group similarly told us that it perceived the National Telecoms Lab to be focused on the "testing of security of new equipment for the UK market" rather than supporting technology development,

131 For example, see: BT Group (UKT0019), para 24 and Qq46 and 49
132 Qq50, 382 and 402—see also: Department for Digital, Culture, Media and Sport, '5G Supply Chain Diversification Strategy' (2020), para 4.9
133 Department for Digital, Culture, Media and Sport, '5G Supply Chain Diversification Strategy' (2020), para 2.12
134 Q382
135 Q249
136 Qq382–383
137 UK Photonics Leadership Group, 'Connecting the UK—Made in the UK' (2020)
138 Institution of Engineering and Technology (UKT0036) and Digital Catapult (UKT0037)
139 Department for Digital, Culture, Media and Sport, '5G Supply Chain Diversification Strategy' (2020), para 3.20
140 For example, see: BT Group (UKT0019), para 24 and Qq239 and 464
141 Q239

collaboration or deployment.[142] This leaves the SmartRAN Open Network Interoperability Centre to fulfil the remaining roles to support diversification. Although its stated remit does match these roles more closely, it is not clear how significant the Centre is intended to be, given that the strategy describes the National Telecoms Lab as the "heart of [the research and development] ecosystem".[143]

48. **There is strong support for the establishment of common testing facilities for new 5G infrastructure equipment, to provide a variety of services that could help to drive diversification. The National Telecoms Lab—which appears to be the main facility proposed by the diversification strategy—seems, however, to be focused heavily on security testing and validation alone.**

49. ***In addition to conducting security testing and validation, the Government should ensure that the research and testing facilities established through the diversification strategy also drive market diversification by stimulating collaboration and supporting the development and commercialisation of new technologies.***

50. Beyond the role of any new facilities, we also heard that the Government should aim for them to complement existing facilities. Dr Kaleshi noted that new facilities did "not necessarily have to be placed in one location" and argued that since the relevant expertise was already "distributed across the country", testing facilities could use a "federated hub and spoke model" connecting existing centres of excellence.[144] The National Physical Laboratory similarly called for the "establishment of a national scale, converged test network research and development environment combining existing and new physical and virtual testbeds for communications hardware and software".[145]

51. Marcus Weldon, President of Bell Labs and Chief Technology Officer at Nokia, additionally warned that Open RAN would be "running on webscale infrastructure in a cloud-native way", using a process called "continuous integration continuous delivery", which he suggested could cause practical issues for potential testing facilities:

> Invariably, to go back to my point about continuous integration continuous delivery, you will have to retest every day, or every week or every month, against all the known vulnerabilities and the new vulnerabilities […] In the new world order of dynamically cloud-native networks, it will be too hard to know what to test. There could be a false sense of security in assuming that a testing centre is validating something. In fact, perhaps it could create a vulnerability because everyone would know what the test configuration was and they would bypass it.[146]

52. **Testing facilities do not need to be situated in one physical location.** ***The Government should ensure that any new testing facilities complement existing facilities, and are designed with potential developments in 5G technology in mind to guard against future redundancy.***

142 BT Group (UKT0019), para 24
143 Department for Digital, Culture, Media and Sport, '5G Supply Chain Diversification Strategy' (2020), paras 3.19–3.20
144 Q240
145 National Physical Laboratory (UKT0007), para 15
146 Qq349–350

Scalability

53. The UK Photonics Leadership Group told us that "one of the main challenges" for new companies aiming to supply radio access equipment was the "ability to rapidly ramp production volumes".[147] The Government's diversification strategy similarly identified the preference of network operators to procure from large-scale vendors as a barrier to market entry and noted that "new market entrants find it challenging to grow without the large-scale opportunities that are needed in order to offset the high initial cost of market entry and ongoing research and development costs".[148] We note the parallels between this challenge of developing large-scale manufacturing capability for radio access equipment and measures taken by the Government to address similar challenges faced by UK-based companies in other sectors, such as in the manufacturing of covid-19 vaccines and batteries for electric vehicles.[149]

54. Although the proposals detailed in the Government's diversification strategy to address the challenge of scaling were limited to support for small-scale demonstration projects, the strategy did state that the Government would "seek to support the incubation and scale-up of homegrown suppliers building on the foundations that exist across our universities and in regional advanced technology hubs".[150] It said that this "work will be closely linked to the government's broader growth and productivity agenda that will be set out in the Industrial Strategy".[151] Addressing the challenge of scaling production specifically, the UK Photonics Leadership Group recommended to us that the Government should support the establishment of "pilot lines to help develop manufacturing expertise".[152] It suggested that a "number of countries", especially in Europe, had already done so to address this challenge.[153] The Digital Catapult also told us that market entrants would require "significant support in the early stages of the development" to scale up their output.[154]

55. Several submissions to our inquiry highlighted that roll-outs of 5G networks could present opportunities to support market entrants to scale up production.[155] For example, the Internet Service Providers' Association suggested that "incentives could be put in place to encourage diversification of the supply chain where public money is funding roll out".[156] In particular, we heard that smaller scale 5G deployments, in specific environments such as factories, campuses or along transport routes, could provide initial markets for new entrants to supply as they grew.[157] Juniper Networks, a network component supplier, noted

147 UK Photonics Leadership Group (UKT0026)—see also: National Physical Laboratory (UKT0007), para 22; BT Group (UKT0019), para 18; Digital Catapult (UKT0037) and oral evidence taken before the Defence Committee on 28 July 2020, HC 201, Q300

148 Department for Digital, Culture, Media and Sport, '5G Supply Chain Diversification Strategy' (2020), para 2.12

149 For example, see: Department for Business, Energy and Industrial Strategy, 'Vaccines Manufacturing and Innovation Centre to open 12 months ahead of schedule', published 17 May 2020 and UK Battery Industrialisation Centre, 'Who We Are', accessed 7 January 2020

150 Department for Digital, Culture, Media and Sport, '5G Supply Chain Diversification Strategy' (2020), paras 3.8–3.24 and 4.10–4.12

151 Department for Digital, Culture, Media and Sport, '5G Supply Chain Diversification Strategy' (2020), para 4.11

152 UK Photonics Leadership Group (UKT0026)

153 UK Photonics Leadership Group, 'Connecting the UK—Made in the UK' (2020)

154 Digital Catapult (UKT0037)

155 For example, see: Parallel Wireless and Isotek Microwave (UKT0013); BT Group (UKT0019), para 24; techUK (UKT0020); Internet Service Providers' Association (UKT0023), para 14; Juniper Networks (UKT0033); Institution of Engineering and Technology (UKT0036)

156 Internet Service Providers' Association (UKT0023), para 14

157 For example, see: Juniper Networks (UKT0033); Institution of Engineering and Technology (UKT0036); Digital Catapult (UKT0037) and Qq347, 353, 406–407 and 459

that the Government could support such deployments and use any funding it provided to stipulate support for diversification, such as the use of open standards.[158] Marcus Weldon, President of Bell Labs and Chief Technology Officer at Nokia, added that spectrum policy could also encourage these small-scale 5G deployments.[159]

56. **New vendors of 5G telecommunications equipment face challenges in scaling up their production rapidly enough to meet network operator demand and compete with incumbent vendors. Although the Government's diversification strategy identifies this barrier to market entry, it defers details of any significant measures to address it until publication of a refresh to the Industrial Strategy. There appear to be good opportunities for the Government to support new market entry at the same time as driving deployment of 5G in the UK, but the diversification strategy fails to set out measures to achieve this.**

57. ***The Government should align its strategy for diversifying the 5G vendor market with its support for rolling out 5G network coverage. Wherever the Government provides funds for expanding 5G coverage, it should look for opportunities to simultaneously support vendor diversification, for example by requiring the use of open standards. The Government should identify opportunities to support new market entrants scale their production by supporting the deployment of novel small-scale 5G deployments. It should provide details of planned measures to support diversification and expand 5G coverage in its Industrial Strategy.***

Intellectual property

58. The Government's diversification strategy identifies the "concentration of Standard Essential Patents[160] and intellectual property portfolios amongst market leading suppliers" as a barrier to new market entrants that can struggle to access the licenses for that intellectual property as easily as incumbent vendors.[161] Scott Petty, Chief Technology Officer of Vodafone UK, highlighted this problem to the Defence Sub-Committee, and noted that Huawei owned "much of the intellectual property and intellectual property rights that [are] required to deploy 5G in the way that it is today".[162]

59. Having identified intellectual property rights as a potential barrier to market entry, the Government's diversification strategy stated the Government's intention to work with "industry bodies, intellectual property licensors and licensees and others to optimise the licensing regime for telecoms standards to enable modularisation of networks".[163] It laid out the Government's ambition for this work to "remove barriers to entry for new market entrants by ensuring fair and equal access to intellectual property and licenses", but it did not provide much detail on what this work might involve or how the Government might achieve these goals.

158 Juniper Networks (UKT0033)

159 Qq347 and 354—see also: Vodafone, 'An Industrial 5G Spectrum Policy for Europe' (2019)

160 Standard Essential Patents are patents on technologies that are included in an industry standard, and therefore required for a supplier to be able to produce a product that meets those standards—see: European Commission, 'Standard Essential Patents' (2018)

161 Department for Digital, Culture, Media and Sport, '5G Supply Chain Diversification Strategy' (2020), para 2.12

162 Oral evidence taken before the Defence Committee on 28 July 2020, HC 201, Q277

163 Department for Digital, Culture, Media and Sport, '5G Supply Chain Diversification Strategy' (2020), para 3.23

60. **The Government identified the concentration of intellectual property rights in the hands of established vendors as a barrier to market entry. It commits in its diversification strategy to working with industry bodies to address this, although the proposed work is not described in great detail.** ***In its response to this Report, the Government should provide more details on how it intends to address the barriers brought about by intellectual property rights, and update us on early progress made against this goal.***

Motivating diversification and maintaining diversity

61. The previous section discussed the barriers that potential telecommunications equipment vendors might face in entering the UK market, and how they might be addressed. This section explores the measures that might be required to proactively drive diversification, as well as the need to maintain increased diversity once it is achieved.

62. Dr Mike Short, Chief Scientific Adviser at the Department for International Trade, emphasised the need for the Government to "work with the operators" to make sure that they would purchase equipment from potential market entrants.[164] Lord Livingston, Chair of the Government's Telecoms Diversification Taskforce, similarly told us that "getting the network operators in line will be important".[165] Addressing this point, Dr Yih-Choung Teh, Group Director for Strategy and Research at Ofcom, argued that network operators had a "very strong commercial incentive" to support diversification of the vendor market, and that this had been confirmed in his dealings with them.[166] Lord Livingston also told us that operators did "not like the fact that they have little choice" of vendors currently.[167] Indeed, Vodafone is undertaking significant work to support the development of Open RAN.[168]

63. Kip Meek, Director of Communications Chambers and the Wireless Infrastructure Group, warned, however, that although network operators would "apparently have an incentive to [have …] as diverse a supply chain as possible", they could face barriers in working towards this, especially in the short-term.[169] For example:

- potential market entrants might not be as competitive on costs as incumbents;
- network management could be complicated by having a wide range of vendors supplying components; and
- network operators may not be able to rely on the security and reliability of new vendors.

Marcus Weldon, Chief Technology Officer at Nokia, and Diane Rinaldo, Executive Director of the Open RAN Policy Coalition, both agreed that network operators preferred to liaise with just one point of contact responsible for large proportions of their network.[170] Howard Watson, Chief Technology and Information Officer at BT, confirmed that "having more than two suppliers across the 19,000 cell sites that I have […] is quite an operational

164 Q333
165 Q401
166 Q453
167 Q402
168 Vodafone UK (UKT0002) and Telecom Infra Project (UKT0018)
169 Q352
170 Qq357 and 382

burden" explaining that "it means that three lots of kit need to accompany every engineer as they maintain the network".[171] He explained that the "balance" operators had to make was between "diversity of choice" and "making the right operational decisions, to have limited deployment [from different vendors]".

64. One indication that operators may face challenges in driving diversification is the market consolidation that has taken place in the UK vendor market over previous years. Although there are only three major vendors in the UK now,[172] Professor Ciaran Martin, former Chief Executive Officer of the National Cyber Security Centre, informed us that there had been "around a dozen" ten years ago.[173] During our inquiry, we heard suggestions of a range of factors that may have driven market consolidation over the last ten to twenty years, including:

- the importance of economies of scale in manufacturing;[174]
- arguments from some of low profitability for network operators and therefore infrastructure equipment vendors (for example, Professor Martin told us that a "lot of the problems lie in the fact that the last two decades have been pretty miserable experiences for UK telecommunications operators");[175]
- the risk of expensive research projects not delivering successful innovations;[176]
- the convenience for network operators of managing a small number of suppliers;[177] and
- national policies supporting certain companies, making others uncompetitive.[178]

The Digital Catapult warned us that if diversification were achieved, it would be critical to avoid that developing into a "repeat of the situation we have today, emerging through consolidation of new vendors in the future".[179]

65. The Government identified similar drivers of consolidation in its strategy and warned that many of them were "likely to persist".[180] It argued that "this market failure calls for a sustained and concerted challenge of the status quo".[181] The strategy did not, however, provide detailed proposals to address many of the drivers for consolidation and did not acknowledge that operators experienced benefits as well as disadvantages from employing

171 Q206
172 Department for Digital, Culture, Media and Sport, '5G Supply Chain Diversification Strategy' (2020), para 2.8
173 Q315—see also: Spirent plc (UKT0001); Parallel Wireless and Isotek Microwave (UKT0013); UK Photonics Leadership Group (UKT0026); Juniper Networks (UKT0033); Institution of Engineering and Technology (UKT0036) and Qq24, 219, 397 and 450
174 For example, see: Spirent plc (UKT0001); Compound Semiconductor Applications Catapult (UKT0032) and Q450
175 For example, see: BT Group (UKT0019), para 15 and Qq221, 321, 342, 354, 397, 408 and 470
176 For example, see: BT Group (UKT0019), para 12
177 For example, see: Qq206, 357 and 382
178 For example, see: Juniper Networks (UKT0033) and Qq137–138, 221 and 225
179 Digital Catapult (UKT0037)
180 Department for Digital, Culture, Media and Sport, '5G Supply Chain Diversification Strategy' (2020), paras 2.12–2.14 and 3.2
181 Department for Digital, Culture, Media and Sport, '5G Supply Chain Diversification Strategy' (2020), paras 3.2–3.3

equipment from a small number of vendors.[182] Kip Meek, Director of Communications Chambers and the Wireless Infrastructure Group, told us that the Government could seek to influence the market in three different ways—funding, facilitation and regulation.[183]

66. Marcus Weldon, Chief Technology Officer at Nokia, noted the financial pressures network operators faced and told us that "we have to recognise that [network operators] may need some incentives" to help to drive vendor market diversification.[184] The Government's diversification strategy similarly noted that incentives for operators to pursue diversification would be a requirement for success.[185] However, the Government's proposals mostly focus on addressing barriers for operators—such as removing technical barriers, reviewing regulatory burdens and offsetting costs—rather than introducing measures to encourage operators to actively pursue diversification.[186] Where the strategy does refer to proposed incentives, it said only that the Government would "consider commercial incentives for mobile network operators".[187] Giving evidence to us in September, Dr Short suggested that "matching supply and demand" between operators and potential new vendors still needed a "bit more work".[188]

67. Several submissions to our inquiry recommended that the Government could also aim to introduce measures to improve the profitability of network operators, to enable them to invest more in diversification and innovation.[189] Dr Ian Levy, Technical Director at the National Cyber Security Centre, told us, for example, that he did not think there was a "huge amount of money in the UK telecoms sector at the moment":

> We have levied quite a lot of cost on [network operators] in various ways, and so investing in something such as standalone 5G in the way that Rakuten [in Japan] has done would be a big commercial risk for them at the moment while we are asking us to do all these other things as well.[190]

Samsung suggested that savings could be found in "spectrum prices, cell site rentals, civil works, transport network [and] energy" costs.[191] BT Group additionally suggested costs associated with meeting regulatory requirements.[192] The Government's support for a project exploring the viability of 'neutral host' deployments (where cell sites are shared between operators) could help to reduce overall site rental costs for operators.[193] In 2018, Ofcom advised the then Government that operators' operating costs could be reduced by giving them similar rights to other utilities (such as rights of access to landlord's properties)

182 Department for Digital, Culture, Media and Sport, '5G Supply Chain Diversification Strategy' (2020), paras 2.22 and 3.8–3.24
183 Q346—see also: Qq348–349
184 Q352
185 Department for Digital, Culture, Media and Sport, '5G Supply Chain Diversification Strategy' (2020), paras 2.22, 3.4 and 3.13
186 Department for Digital, Culture, Media and Sport, '5G Supply Chain Diversification Strategy' (2020), paras 3.8–3.24—para 2.22 refers to incentives for operators but provides no details of what these might consist of
187 Department for Digital, Culture, Media and Sport, '5G Supply Chain Diversification Strategy' (2020), para 3.12
188 Q333
189 For example, see: Samsung Electronics UK (UKT0008); BT Group (UKT0019), para 15; techUK (UKT0020) and Q456
190 Q456
191 Samsung Electronics UK (UKT0008)
192 BT Group (UKT0019), para 15
193 Department for Digital, Culture, Media and Sport, '5G Supply Chain Diversification Strategy' (2020), para 3.16—see also, for example: GSMA, 'Infrastructure Sharing: An Overview', accessed 6 January 2021 and Oughton *et al.*, 'The cost, coverage and rollout implications of 5G infrastructure in Britain', Telecommunications Policy, vol 42 (2018)

and by providing business rates relief on mobile mast deployments.[194] The latter measure could be made dependent on operators supporting diversification, for example integrating open interfaces in their equipment or making deployments open to other operators for shared use.[195]

68. Others recommended that the Government should introduce regulations requiring diversification. For example, the Compound Semiconductor Applications Catapult and the UK Photonics Leadership Group both advocated requirements on operators specifying a minimum proportion of equipment that should be designed or manufactured in the UK or in an allied country.[196] Amy Karam, a Fellow at the Canadian Global Affairs Institute, similarly suggested that the Government could set minimum proportions of equipment that should meet open standard and interoperability criteria.[197] Professor Ciaran Martin, former Chief Executive Officer at the National Cyber Security Centre, agreed that regulation would "have some role to play" in delivering diversification, but warned that the Government could "not conjure up a scale player just through regulation":

> At the moment, we could in theory demand through regulation more than two players, but we do not have two viable players selling if we exclude Huawei. The regulatory intent has to be matched by commercial reality. [Regulation] has a part to play, but it will not in and of itself create the conditions that we need for a more diverse market.[198]

Marcus Weldon, President of Bell Labs and Chief Technology Officer at Nokia, supported the idea of Government mandates, but argued that although these should involve "testable" requirements, they should be based on principles (such as "openness") rather than picking particular technologies for implementation (such as Open RAN).[199]

69. Whichever mix of incentives, policies and regulations are adopted, BT Group told us that it strongly encouraged the Government to provide "long term clarity and certainty" in pursuing diversification:

> Designing and building our networks requires sufficient lead times for effective implementation, including the need to meet any new regulatory, legal and/or public policy obligations. Avoiding changes in requirements over the short to medium term, requiring our network design and build plans to alter, is hugely inefficient and will put at risk network performance and resilience.[200]

Dr Tobias Feakin, the Australian Ambassador for Cyber Affairs and Critical Technology, similarly told us that Australian operators had benefited from the certainty provided by the Australian government's early decision to ban high-risk vendors from its 5G networks.[201]

194 Ofcom, 'Further options for improving mobile coverage' (2018), para 1.42
195 EE, 'EE Parliamentary briefing: Business Rates' (2014)
196 UK Photonics Leadership Group (UKT0026) and Compound Semiconductor Applications Catapult (UKT0032)
197 Q221
198 Q328
199 Q348
200 BT Group (UKT0019), para 9
201 Q410

Amy Karam suggested that mandates for diversity requirements be published to give operators good warning.[202] This could be comparable to roadmap of different stages for removing high-risk vendors published by the Government.[203]

70. **Long-standing factors have driven consolidation in the telecommunications vendor market over many years, so it is critical that the Government adopts measures to maintain market diversity as well as to drive the initial diversification. Network operators will be integral to achieving both aims. Although operators stand to benefit from a more diverse vendor market, it may not be in their interest to purchase and use equipment from a wider range of vendors. The Government's diversification strategy does not sufficiently acknowledge this fact, and provides little detail of proposed measures to ensure that it will be in network operators' interest to drive and maintain a diverse vendor market.**

71. ***The Government cannot rely solely on removing barriers to market entry to diversify the telecommunications vendor market, but must also ensure that network operators actively pursue diversification and act to maintain the diversity achieved. This will require a combination of incentives, measures to reduce operator costs, and regulatory requirements. For example, the Government could introduce business rate relief on mobile mast deployments. In order to provide certainty to the sector, the Government should publish within three months of this Report the measures it is considering to incentivise and require network operators to diversify their suppliers, with an indicative timetable for implementation.***

72. Discussing regulation, Professor Martin added that he felt that the UK had "under-regulated security" in telecommunications.[204] Dr Ian Levy, Technical Director at the National Cyber Security Centre, similarly told us that the "regulatory system has been all about consumer prices", which had benefited consumers but left the network operators with "less and less capital reserves".[205] Marcus Weldon suggested that the telecommunications market had focused so heavily on consumer costs and experience that there had been a "devaluation of the fundamental infrastructure piece".[206] This is despite the two principal duties of the regulator, Ofcom, being:

- to further the interests of citizens in relation to communications matters; and
- to further the interests of consumers in relevant markets, where appropriate by promoting competition.[207]

The inclusion of the first duty alongside the second implies an expectation for Ofcom to act beyond simply reducing costs for consumers, but also to, for example, promote network security. Indeed, Ofcom has specific responsibilities to ensure that "network providers and service providers […] take technical and organisational measures appropriately to manage risks to the security of public electronic communications networks and public electronic communications services".[208] Dr Yih-Choung Teh, Group Director for Strategy

202 Q221
203 Department for Digital, Culture, Media and Sport, 'Roadmap to remove high risk vendors from telecoms network', published 30 November 2020
204 Q334
205 Q470
206 Q343
207 Communications Act 2003, section 3
208 Communications Act 2003, section 105A

and Research at the regulator, Ofcom, argued that the regulator did consider the "longer-term investment in the infrastructure that the country needs" as well as the "immediate static benefits of lower prices", but that there was a "trade off" to be made between them given the "finite amount of cash".[209] He added that one of the motivations for the new Telecoms Security Requirements was to provide Ofcom with greater powers to achieve the security outcomes it desired (see Box 2).[210]

Box 2: The Telecommunications (Security) Bill

The Government introduced the Telecommunications (Security) Bill to "introduce a new security framework for the UK telecoms sector to ensure that public telecommunications providers operate secure and resilient networks and services and manage their supply chains appropriately".

The Bill replaces the existing security requirements on network operators with new duties to take appropriate and proportionate measures to:

- identify security risks;
- reduce those risks; and
- prepare for dealing with potential security compromises.

The Bill gives the Secretary of State the ability to issue regulations requiring specific measures that network operators must take to achieve these aims, as well as codes of practice giving guidance on how operators are expected to achieve those aims. The Bill provides Ofcom with new powers to enforce this security framework, such as powers to assess compliance, direct network operators to take measures to improve security, and issue fines for non-compliance.

The Bill additionally introduces new powers for the Secretary of State to "designate" vendors that are felt to pose a threat to national security, and to introduce requirements on network operators with regards to their use of equipment from that vendor. For example, the Government intends to use this power to designate Huawei as a potential security risk and to prohibit the use of Huawei equipment purchased after 31 December 2020.

Source: Telecommunications (Security) Bill [Bill 216 (2019–2021)]; Explanatory Notes to the Telecommunications (Security) Bill [Bill 216 (2019–2021)—EN] and Department for Digital, Culture, Media and Sport, 'Huawei Draft Designated Vendor Direction' (2020)

73. The Digital Economy Act 2017 gave the Secretary of State the power to set out the Government's "strategic priorities" for telecommunications, to which Ofcom must "have regard" in carrying out its duties.[211] The Secretary of State published the Government's strategic priorities in 2019.[212] Although this statement included "secure and resilient telecoms infrastructure" as one of four strategic priority areas, this area was covered in just four paragraphs while the section on "furthering the interests of telecoms consumers" spanned fourteen paragraphs.[213] The section on security welcomed Ofcom's increasing capability in this space and highlighted the importance of Ofcom's role in securing 5G

209 Q471
210 Q474—see also: Telecommunications (Security) Bill [Bill 216 (2019–2021)]
211 Digital Economy Act 2017, section 98 and Communications Act 2003, sections 2A–2C
212 Department for Digital, Culture, Media and Sport, 'Statement of Strategic Priorities for telecommunications, the management of radio spectrum, and postal services' (2019)
213 Department for Digital, Culture, Media and Sport, 'Statement of Strategic Priorities for telecommunications, the management of radio spectrum, and postal services' (2019), paras 45–62

security, but did not set any clear priority actions.[214] In contrast, the section on consumer interests made seven recommendations to Ofcom.[215] In response, Ofcom listed securing networks as one of its priorities and noted its collaboration with the Government on the development of the Telecoms Security Requirements to be implemented by the Telecommunications (Security) Bill, but did not indicate any rebalancing of its focus on consumer pricing and network security.[216] Although the Government's statement of strategic priorities is not intended to be updated more frequently than every five years, there is provision for the Government to do this following a "significant change" in policy.[217]

74. **Of Ofcom's two principal duties, it has appeared to have given less prominence to "further[ing] the interests of citizens in relation to communications matters" than it has to "further[ing] the interests of consumers". *Ofcom must ensure that it pursues both of its principal duties and guarantees the security of the UK's telecommunications infrastructure as well as furthering the interests of consumers. The Government should consider the case for updating its statement of strategic priorities for telecommunications, to emphasise the importance of Ofcom's duties relating to telecommunications security.***

International co-operation

75. The importance of international co-ordination on diversification was emphasised by many contributors to our inquiry.[218] Lord Livingston, Chair of the Government's Telecoms Diversification Taskforce, explained that "no supplier, small or big, is going to create a world-beating product just for the UK, so it will be important to have a consistency of approach across a number of countries where they know that they can scale up".[219] Important areas for co-ordination included:

- **research and development**—to pool resources and make use of different areas of expertise;[220]
- **standards**—to ensure that global standards embed the values shared by the UK and its allies;[221]
- **adoption and deployment**—to provide large markets for new vendors;[222] and
- **policy**—to provide consistency and clarity for vendors operating across multiple countries.[223]

214 Department for Digital, Culture, Media and Sport, 'Statement of Strategic Priorities for telecommunications, the management of radio spectrum, and postal services' (2019), paras 59–62
215 Department for Digital, Culture, Media and Sport, 'Statement of Strategic Priorities for telecommunications, the management of radio spectrum, and postal services' (2019), paras 49, 53–58
216 Letter from Katie Pettifer, Director of Public Policy at Ofcom, to James Heath, Digital Infrastructure Director at the Department for Digital, Culture, Media and Sport, 25 November 2019, p6
217 Communications Act 2003, section 2A
218 For example, see: Parallel Wireless and Isotek Microwave (UKT0013); BT Group (UKT0019), para 37; Openreach (UKT0022), para 24; Internet Service Providers' Association (UKT0023), para 13; Telecom Infra Project (UKT0028); Digital Catapult (UKT0037); Mavenir (UKT0038), section 5 and Qq323, 348, 401, 423 and 432
219 Q401
220 For example, see: Rushmere Technology Limited (UKT0025), para 11 and Qq241, 401 and 423
221 For example, see: and Qq401, 423 and 435
222 For example, see: Parallel Wireless and Isotek Microwave (UKT0013) and Q432
223 For example, see: Internet Service Providers' Association (UKT0023), para 13 and Q401

76. The Government's diversification strategy acknowledged that the "UK market alone cannot drive or sustain meaningful change across the supply chain", and stated that "international partnership and collaboration will be fundamental to the success" of the strategy.[224] It did not, however, make any reference to the specific policies or ambitions of other countries, or how the proposals in the strategy compared or aligned with those of the UK's allies. Although we were made aware of a variety of initiatives being undertaken in other countries,[225] it was notable that Dr Feakin told us that the Australian government did not intend to intervene in its telecommunications market to drive the development or adoption of Open RAN.[226]

77. The diversification strategy indicated that the Government intends to pursue international collaboration through its existing diplomatic and trade networks.[227] Dr Mike Short, Chief Scientific Adviser at the Department for International Trade, assured us that the UK was "already starting to work with some of our allies, particularly the USA and Canada, in looking at what they are doing with their supply " and was "also working with allies in north-east Asia, whether Japan or South Korea, to see how we can learn lessons from some of the supplier choice factors that they use".[228] The Secretary of State for Digital, Culture, Media and Sport, Oliver Dowden MP, referred to the 'D10' countries comprising the G7 (the UK, Canada, France, Germany, Italy, Japan and the USA) plus Australia, India and South Korea, and told us that the Government was "having good discussions with all of them".[229] Professor Ciaran Martin, former Chief Executive Officer of the National Cyber Security Centre, welcomed this work, but suggested that governments currently "lack the sort of mechanisms" to provide the level of economic and trade policy co-ordinated required:

> I would welcome a standing intergovernmental mechanism among like-minded countries to keep an eye on this, to drive things and to have a look at Government level as to whether standards and markets are developing in the right way. At the moment, we are designed for national security agencies to talk to each other about stuff like this. National security agencies do not decide whether or not big telecoms operators are going to buy from a new scale player. Commercial entities do that, and that is the sort of thing that Governments need to think creatively about.[230]

Professor Martin specified that the 'Five Eyes' alliance was a "hugely important security alliance", but has "never co-ordinated economic and commercial policy" and was "not designed to do that".[231] Amy Karam, a Fellow of the Canadian Global Affairs Institute, similarly told us that although there was "definitely value in having the security commissions

224 Department for Digital, Culture, Media and Sport, '5G Supply Chain Diversification Strategy' (2020), paras 3.25–3.26
225 For example, see: Telecom Infra Project (UKT0028)
226 Q422
227 Department for Digital, Culture, Media and Sport, '5G Supply Chain Diversification Strategy' (2020), paras 3.25–3.31
228 Q337
229 Q305
230 Q337—see also: Q323
231 Q337

participate", other aspects and actors would also be important to achieving rapid and significant progress in the 5G vendor market.[232] The Digital Catapult reiterated Professor Martin's argument of the importance of mechanisms for sustained collaboration.[233]

78. We also heard of the importance of working with a wide range of international partners.[234] Dr Short noted the importance of countries in Europe, the Americas and north-east Asia for setting standards and co-ordinating spectrum allocations.[235] Ms Karam emphasised that "if we want to be a significant player globally in the long term—in five, 10, 15 or 20 years—we should not forget about emerging markets".[236] Democratic countries with large telecommunications markets, such as India and Brazil, have also been highlighted as important collaborators.[237] The diversification strategy states the Government's intention to work with a "wide range of international partners, including markets with advanced technology and manufacturing bases, those with the ability to drive change in the market through scale and emerging markets with potential for rapid growth".[238] The specific examples it gives of fora for collaboration, however—the 'Five Eyes' alliance and the G7—do not cover countries like India or Brazil, or emerging markets.

79. **The UK's telecommunications market accounts for a small proportion of the global market. International co-ordination will therefore be critical to the success of the UK's diversification strategy. The Government's 5G Supply Chain Diversification Strategy acknowledges this fact, and states the Government's ambition for international co-operation. However, the strategy provides little detail of plans for sustained co-ordination on industrial policy with a diverse range of countries.**

80. ***The Government should seek to establish a dedicated, standing forum for international co-operation on diversifying the telecommunications market, encompassing as many like-minded countries as possible and covering aspects including: research and development; adoption and deployment; standards; and overall strategy. This should not be based on existing intelligence-sharing coalitions. The Government should set out in its response to this Report, how it intends to achieve this, a timetable for establishing such a forum and what progress it has made to date.***

232 Q226
233 Digital Catapult (UKT0037)
234 For example, see: and Qq227 and 348
235 Qq330–332 and 337—see also: Q348
236 Q227—see also: Institution of Engineering and Technology (UKT0036), section 2
237 Q401—see also: Open RAN Policy Coalition, Submission to the US National Telecommunications and Information Administration on The National Strategy to Secure 5G Implementation Plan (2020), p14
238 Department for Digital, Culture, Media and Sport, '5G Supply Chain Diversification Strategy' (2020), para 3.28

3 A critical technologies strategy

81. The previous Chapter focused on the specific task of diversifying the UK's current telecommunications vendor market. In its *5G Supply Chain Diversification Strategy*, the Government expressed its hope that the strategy could also "provide future guidance for sectors dealing with similar risks to their critical infrastructure".[239] This Chapter examines the factors leading to the current situation in telecommunications and draws lessons from this that are of relevance to other technologies and sectors.

Context

82. Throughout our inquiry, several witnesses referred to a growing technological divergence between China and the West.[240] Professor Ciaran Martin, the former Chief Executive Officer of the National Cyber Security Centre, told us that "some form of greater polarisation […] is inevitable and already happening", identifying China's "increasing authoritarianism" and "US policy" as key factors driving polarisation (although he clarified that he did not think that "full polarisation" was "likely any time soon").[241] Dr Ian Levy, Technical Director at the National Cyber Security Centre, similarly said that he anticipated "two competing tech stacks in a number of spaces, including telecoms—one Western-driven, one China-driven".[242] Marcus Weldon, President of Bell Labs, added that he expected the "belt and road countries" to mostly align with China.[243]

83. Referring to telecommunications, Lord Livingston, Chair of the Government's Telecoms Diversification Taskforce, told us that divergence leading to Chinese-defined standards would have "definite economic consequences".[244] In September 2020, Mircea Geoană, the Deputy General of NATO, described the developing threat from new technologies as "one of the most rapidly evolving security challenges of our time":

> We are now competing with authoritarian regimes that misuse and abuse new technologies to destabilise us, and to manipulate and disrupt our free and democratic way of life. Countries that don't share our values, such as China and Russia, are investing heavily in technologies that help them increase control over their own citizens and exert influence in the world.[245]

Professor Martin has similarly described the emergence of China's technological prowess and its willingness to use this for geopolitical competition as a "Sputnik moment for the whole of the West":

> Published in 2015, [China's] Made in China 2025 strategy articulates a vision, backed by long-term planning and huge state subsidies, to establish China as a world leader in many of the key technologies of the future […] The solution [to this challenge] relies on reshaping dysfunctional markets

239 Department for Digital, Culture, Media and Sport, '5G Supply Chain Diversification Strategy' (2020), para 1.8
240 For example, see: Qq230, 340, 358, 395 and 432
241 Q340
242 Q432
243 Q358; see also: 'China's Massive Belt and Road Initiative', Council on Foreign Relations, accessed 17 November 2020
244 Q409
245 NATO, 'Speech by NATO Deputy Secretary General Mircea Geoană at the CYBERSEC GLOBAL 2020 virtual conference', made 28 September 2020

> to compete against a nation with one and a half billion potential consumers, deep pockets for subsidies, and no democratic accountability. Countering China requires a long-term, technically authoritative, well-funded, carefully regulated and properly incentivised strategy.[246]

This appears to go beyond the Government's £250 million strategy intended to diversify the UK's 5G vendor market.

84. Dr Tobias Feakin, the Australian Ambassador for Cyber Affairs and Critical Technology, told us that, in the Australian government's view, 5G was "one of the most, if not the most, important major infrastructure investment that [Australia] would be making over the next decade".[247] However, 5G is not the only technological development with the potential to significantly impact UK prosperity and security over the coming years. Technologies such as artificial intelligence, robotics, quantum technologies, biotechnologies, space technologies and low-carbon technologies are expected to be important drivers of economic growth; many also have applications directly relevant to defence and national security.[248]

85. **There is a strong risk that the urgent security challenges faced by the UK's telecommunications sector are indicative of a wider, and growing, geopolitical development. Throughout our inquiry, we have heard of the prospect of a growing technological and regulatory divergence between China, and countries aligned with China, and other countries. This is not restricted to telecommunications or even cyber security—artificial intelligence, quantum technologies and synthetic biology are just some examples of other emerging technology sectors that will be prominent in our future economy and security, and in which there is the potential for different technical and regulatory standards to apply. The Government should not regard the problems posed by 5G addressed in this Report as a one-off, but more likely illustrative of a wider challenge.**

86. ***The Government must treat the current issues in the UK's 5G vendor market as an indication of a much wider geopolitical, technological challenge. The character of the UK's response, and that of other like-minded nations, will have profound implications for future decades and beyond. We urge the Government to address this seriously, comprehensively and without delay. We recommend that within twelve months, the Government should develop and publish a White Paper setting out its assessment of the current extent of and future potential for global technological divergence, the anticipated consequences of such divergence and how it intends to address the challenges this poses.***

A national critical technologies strategy

87. As discussed earlier in this Report, the UK found itself in a position in which there were too few vendors to provide the desired level of security in its telecommunications networks, and in which the mechanism for managing the threat of a high-risk vendor was dependent upon the decisions of other countries. Lord Livingston, Chair of the Telecoms Diversification Taskforce, argued that one of the UK's flaws leading up to the

246 Professor Ciaran Martin, 'The 'tech'tonic plates begin to shift', published 21 December 2020
247 Q410
248 For example, see: Government Office for Science, 'Technology and Innovation Futures 2017' (2017); US White House, 'National Strategy for Critical and Emerging Technologies' (2020), Annex

current situation had been a lack of a "strategic look at the UK's position, whether that be standards or capability, or research and development".[249] Amy Karam, a Fellow of the Canadian Global Affairs Institute, similarly told us that the main challenge for Western countries, including the UK, had been the lack of "foresight or a longer-term view".[250]

88. The USA published a 'National Strategy for Critical and Emerging Technologies' in 2020.[251] This identified 20 technology areas of critical importance to economic growth and security, including "communication and networking technologies", and set out the US Government's intention to:

- support domestic research and development capability in these technology areas;
- accelerate the adoption of emerging critical technologies;
- secure supply chains;
- enhance international leadership in standards and governance; and
- protect domestic intellectual property, research knowledge and other relevant assets.

The USA is not the only country to be explicitly focusing on critical and emerging technologies. Australia appointed an inaugural ambassador for cyber affairs in 2017—our witness, Dr Feakin—and later expanded the role to encompass critical technology, to "reflect the central role that technology issues have in geopolitics".[252] The Australian Government subsequently launched a public consultation in April 2020 to feed into a new 'International Cyber and Critical Technology Engagement Strategy', covering issues including:

- which technological developments and applications present the greatest risk and/or opportunities;
- how cyberspace and critical technologies will shape the international strategic and geopolitical environment out to 2030; and
- what Australia's key international cyber and critical technology objectives should be.[253]

89. The UK has acted to achieve similar goals in some of the same areas addressed by the USA's strategy. For example, the Government introduced a National Security and Investment Bill, intended to strengthen the Government's powers to scrutinise, and intervene in, investments for the purposes of protecting national security.[254] It has also

249 Q399—although Lord Livingston did argue that the "notion that the UK could have prevented a situation where the whole world had gone to proprietary equipment from a small number of manufacturers is asking a bit much of UK markets": Q397

250 Q218

251 US White House, 'National Strategy for Critical and Emerging Technologies' (2020)

252 Australian Department of Foreign Affairs and Trade, 'Ambassador for Cyber Affairs and Critical Technology', accessed 23 November 2020

253 Australian Department of Foreign Affairs and Trade, 'Public Consultation: International Cyber and Critical Technology Engagement Strategy', accessed 23 November 2020

254 Department for Business, Energy and Industrial Strategy, 'National Security and Investment Bill' (2020)—see also: Department for Business, Energy and Industrial Strategy, 'National Security and Investment Bill: Explanatory Notes' (2020)

sought to achieve some of the other goals in specific sectors, for example through the National Quantum Technologies Programme or with the artificial intelligence sector deal.[255] However, it has not yet produced an equivalent over-arching strategy to identify critical technologies and develop measures to ensure the UK's prosperity and security as they emerge. Dr Mike Short, Chief Scientific Adviser at the Department for International Trade, told us that the UK needed to plan its "own strategy" for dealing with technological and regulatory divergence, addressing "several sectors and not just telecommunications".[256] We note that the Government's call for evidence for its *Integrated Review of Security, Defence, Foreign Policy and Development* referred to science and technology both as a driver for change in international relations and a means for managing potential security risks.[257]

90. ***As part of its White Paper on global technological divergence, the Government should develop a critical technologies strategy that identifies technologies that are likely to be of critical importance to the UK's prosperity and security over the next ten to twenty years. This strategy should assess the potential opportunities and risks of these technologies, and propose measures to seize those opportunities and mitigate those risks. It should align with other relevant strategies, such as the Integrated Review of Security, Defence, Foreign Policy and Development and the new Industrial Strategy.***

Supply chain security

91. The component of the USA's national strategy of most direct relevance to the issues discussed in the previous Chapter concerns supply chains. Although the telecommunications sector regulator, Ofcom, has responsibilities to protect the security of networks and services, this has been limited to the regulation of network operators and does not extend to equipment vendors.[258] The Government's diversification strategy now aims to increase the number of vendors supplying equipment to the UK's network operators, and the Telecommunications (Security) Bill is intended to provide new powers to improve network security, including consideration of equipment vendors.[259] Giving evidence to our predecessor Committee in June 2019, however, Professor Rahim Tafazolli, Head of the Institute for Communication Systems at the University of Surrey and now a member of the Government's Telecoms Diversification Taskforce, observed that regardless of the vendor, "most of the equipment comes from China on the hardware side".[260] Dr Levy explained to us that that the location of manufacturing was less important to the overall security risk of a product than the location of its hardware design, software development or testing, as these would be easier stages in the overall process to insert security vulnerabilities.[261] Nevertheless, he was clear that the National Cyber Security Centre would "absolutely wish to have a diverse supply base and manufacturing base across the telecoms sector".[262]

255 UK National Quantum Technologies Programme, 'Overview of programme', accessed 20 November 2020 and HM Government, 'Industrial Strategy: Artificial Intelligence Sector Deal' (2018)
256 Q336
257 Cabinet Office, 'Integrated Review: Call for Evidence' (2020)
258 Q450—see also: Communications Act 2003, sections 105A–105D
259 Telecommunications (Security) Bill, Clause 15 [Bill 216 (2019–2021)]
260 Oral evidence taken before the previous Science and Technology Committee on 10 June 2019, HC (2017–2019) 2200, Q43
261 Qq436–437
262 Q446

92. Manufacturing is, in turn, dependent upon access to raw materials. The EU and the USA have both published lists of 'critical materials', identified on the basis of their importance to national prosperity and security, the security of their supply chains and the availability of alternatives.[263] China is the main producer of 19 of the 30 critical materials identified by the EU (other principal producers for certain materials include the USA, South Africa and Brazil).[264] In 2019, the US Department of Commerce noted that the USA was "heavily dependent on foreign sources of critical minerals and on foreign supply chains resulting in the potential for strategic vulnerabilities to both [its] economy and military", and published a strategy for reducing US reliance on, and improving security of supply of, critical materials.[265] The EU updated a similar strategy in September 2020,[266] while the Australian government recently consulted on principles to apply to managing the supply chains of critical technologies.[267] Common actions covered by these strategies include:

- research and development for critical material recycling and exploration of alternative materials;
- the development of domestic material exploration and extraction;
- co-operation with international allies to strengthen and diversify supply chains; and
- assessment of supply chain risk and possible future risks, with planning to prepare for different scenarios.

A 2019 paper from the Parliamentary Office for Science and Technology noted that, in contrast, the UK Government did "not have a specific critical materials strategy".[268]

93. **The Government has only recently considered the consolidation of vendors in the UK's telecommunications market as a potential risk to national security, although it is a process that has taken place over ten to twenty years. One problem appears to have been the focus on the security of the network operators and not their supply chains, including when setting the role and powers of the regulator. Although the diversification strategy now addresses vendor diversity, it still does not consider the full supply chain. Whereas other nations and regions, including the USA, Australia and the European Union, have produced strategies addressing supply chain risk across all critical technology areas, the Government's diversification strategy addresses only 5G.**

94. ***In producing a national strategy for critical and emerging technologies, the Government should consider potential risks that could develop across their full supply chains.***

263 European Commission, 'Critical Raw Materials Resilience: Charting a Path towards greater Security and Sustainability' (2020) and US Department of the Interior, 'Final List of Critical Minerals 2018', Federal Register, Vol 83 No 97 (2018)

264 European Commission, 'Critical Raw Materials Resilience: Charting a Path towards greater Security and Sustainability' (2020), pp19–22

265 US Department of Commerce, 'A Federal Strategy to Ensure Secure and Reliable Supplies of Critical Minerals' (2019)

266 European Commission, 'Critical Raw Materials Resilience: Charting a Path towards greater Security and Sustainability' (2020)

267 Australian Government, 'Critical Technology Supply Chain Principles: A Call for Views' (2020)

268 Parliamentary Office for Science and Technology, 'Access to Critical Materials', POSTnote 609 (2019)

International standards

95. A potential technological divergence between China and the West was most frequently discussed with reference to standards, although the extent to which standards might diverge was not yet known.[269] The Secretary of State for Digital, Culture, Media and Sport, Oliver Dowden MP, told us that he "hope[d] that we will be able to have common standards across the entire globe".[270] In contrast, Dr Levy told us that some extent of divergence was "likely", although "whether they end up being completely separate standards or profiles of the same standard is to be seen".[271] Marcus Weldon, President of Bell Labs, told us that he had "not seen any bifurcation yet" in the "mainstream" standards for 5G, but that the "industrial segment already seems to be bifurcating".[272]

96. The Australian Strategic Policy Institute noted in 2019 that whereas the agreement of standards had once been "considered a very dry subject in which technical experts put their heads together and collaborate to get the best technical outcomes", it had recently become "politicised".[273] Dr Ian Levy, Technical Director at the National Cyber Security Centre, explained that countries with a strong influence over standards-setting processes could use this to support domestic companies and project their values:

> One potential outcome is you end up with whoever sets the standard ensuring that their commercial companies are best positioned to deliver that, so you end up skewing the market quite considerably. If you skew the market towards something that, for example, puts at the heart of its standard censorship of domestic traffic, that would then come for free in everything you bought, because that is what they are building.[274]

Whereas allowing standards to be largely determined by foreign companies and countries could therefore cede economic advantage and influence over the values embedded in technologies, allowing standards to diverge could increase costs and hinder innovation.[275]

97. Lord Livingston, Chair of the Government's Telecoms Diversification Taskforce, told us that for telecommunications, the "biggest influence on the standards bodies today probably is China and certain suppliers".[276] Other commentators, including at the Royal United Services Institute and the Information Technology and Innovation Foundation, have similarly reported growing Chinese influence over telecommunications and other standards bodies.[277] As the Secretary of State told us, it is "perfectly understandable that China, as an emergent and indeed emerged power, and a country with huge commercial interests around the world, wants to take its legitimate place at the table in shaping those standards".[278] There have, however, been concerns that Chinese companies have in some instances moved away from supporting proposed specifications on technical grounds

269 For example, see: Qq230, 337, 358, 388, 395, 409 and 432
270 Q308
271 Q432
272 Q358
273 Australian Strategic Policy Institute, 'Ensuring a trusted 5G ecosystem of vendors and technology' (2020), p8
274 Q434
275 For example, see: Digital Catapult (UKT0037) and oral evidence taken before the Defence Committee on 28 July 2020, HC 201, Q277
276 Q409
277 Veerle Nouwens, 'A Voice on the Stage, Not Just a Seat at the Table', Royal United Services Institute Newsbrief, published 24 July 2020 and Doug Brake, 'A U.S. National Strategy for 5G and Future Wireless Innovation', Information Technology and Innovation Foundation report, published 27 April 2020
278 Q307

alone.[279] Alluding to these concerns, Dr Levy told us that the UK must "make sure that the standards bodies are multilateral and appropriately driven to make sure that everybody gets a fair voice".[280] In any case, Lord Livingston argued that the "West has dropped the ball on standards", and referred to a "whole list of things about the UK's involvement in standards […] where we have frankly lost the position we had many years ago".[281] Dr Tobias Feakin, the Australian Ambassador for Cyber Affairs and Critical Technology, told us that "standards is gritty, time-consuming work, but I think there has been a grand awakening among like-minded countries that we need to be doing more".[282]

98. Recognising the importance of standards and the UK's diminishing influence over them, the Government's *5G Supply Chain Diversification Strategy* included "increasing UK presence and influence at standard setting bodies" as part of its proposals to drive diversification.[283] Noting that some standards-setting bodies were industry-led and some were run at a nation-state level, the strategy set out four main aspects of the proposed work:

- increasing representation at global standards-setting fora from British officials and British companies;
- increasing the input of British officials, companies and academics to standards-setting processes, for example new standards proposals;
- closer co-operation between the UK Government, industry and academia to increase the effectiveness of representation and participation; and
- more strategic co-ordination to ensure that the first three measures contribute to standards better-suited to the UK's overall, long-term interests.[284]

These measures, however, have been presented in the context of telecommunications alone. In contrast, Marcus Weldon, President of Bell Labs, told us that "it looks like China will be publishing something called China Standards 2035", with the aim of promoting "Chinese native standards for this industrial revolution".[285] This is expected to cover a wide range of technologies.[286] The Chinese government has also published strategies detailing its ambitions to gain influence over standards in specific sectors, such as artificial intelligence.[287]

99. **The setting of international standards is important for national economic competitivity and technical capability. The influence of British companies and officials in global standards-setting processes is diminishing. Although the '5G Supply Chain**

279 For example, see: Information Technology and Innovation Foundation, 'A U.S. National Strategy for 5G and Future Wireless Innovation' (2020) and Australian Strategic Policy Institute, 'Ensuring a trusted 5G ecosystem of vendors and technology' (2020)
280 Q433
281 Qq358 and 397
282 Q423
283 Department for Digital, Culture, Media and Sport, '5G Supply Chain Diversification Strategy' (2020)
284 Department for Digital, Culture, Media and Sport, '5G Supply Chain Diversification Strategy' (2020), paras 2.13 and 3.22
285 Q358
286 Federation of German Industries, 'Chinese Creative Drive: China Standards 2035', published 13 August 2020
287 Standardization Administration of China, 'Artificial Intelligence Standardization White Paper' (2018); translation by Center for Security and Emerging Technology, Georgetown University

Diversification Strategy' sets out the Government's intention to redress this in the telecommunications sector, it is not clear that there are similar plans for other important technological sectors.

100. ***In producing a national strategy for critical and emerging technologies, the Government should review the relevant global standards bodies, the objectivity of their processes and the relative influence of different countries. Similar to those measures outlined in its 5G supply chain diversification strategy, the Government should develop measures to build British capability and influence at standards-setting bodies for all critical technologies.***

Domestic capability

101. Many of the aims set out in the USA's strategy for critical and emerging technologies focus on strengthening what it refers to as the "United States national security innovation base", which it defines as the "American network of knowledge, capabilities, and people […] that turns ideas into innovations, transforms discoveries into successful commercial products and companies, and protects and enhances the American way of life".[288]

102. The economic and societal benefits to the UK of having a strong domestic capability for research and development in emerging critical technology sectors are evident. For example, Professor Dimitra Simeonidou, Professor of High Performance Networks at the University of Bristol, observed that "most of the other countries that have had faster take-up of 5G have a local vendor—for instance, South Korea with Samsung, or Japan with NEC".[289] The Government has explicitly recognised this and set out plans to strengthen the UK's science and innovation capability, including significant increases in funding.[290] Domestic capability in critical technologies also improves security by reducing the UK's dependency on foreign researchers, companies and governments. Professor Ciaran Martin, former Chief Executive Officer of the National Cyber Security Centre, added that technologies designed outside of the UK or its allies could not be scrutinised for security vulnerabilities in the same detail as domestic technologies.[291] Further to this, Dr Ian Levy, Technical Director at the National Cyber Security Centre, noted that the country in which a technology is developed shaped its capabilities:

> Software codifies values at the moment, so if you have Chinese companies providing the software or the hardware for everything that you do, you are implicitly going to get the Chinese values encoded in that.[292]

103. None of the leading telecommunications equipment vendors are British or based in countries belonging to the 'Five Eyes' or 'D10' alliances.[293] During our inquiry, we were made aware of several successful British companies further down the supply chain.[294]

288 US White House, 'National Strategy for Critical and Emerging Technologies' (2020)
289 Q6
290 HM Government, 'UK Research and Development Roadmap' (2020)
291 Q316
292 Q433
293 Department for Digital, Culture, Media and Sport, 'UK Telecoms Supply Chain Review Report' (2019), paras 4.5–4.12 and Q426—the 'Five Eyes' alliance is an intelligence sharing alliance comprising the UK, the USA, Australia, Canada and New Zealand, the 'D10' comprises the UK, Australia, Canada, France, Germany, India, Italy, Japan, South Korea and the USA
294 For example, see: UK Photonics Leadership Group (UKT0026); Digital Catapult (UKT0037); Mavenir (UKT0038), section 4 and Q236

However, the Digital Catapult told us that while the UK had strengths in academic research, there had been a "long standing decrease in public and private industrial research and development funding in telecommunications in the UK over the past 15 years or so".[295] It argued that it was "necessary to strengthen the industrial research and development capabilities in the UK". Options for achieving this have been discussed in more detail in Chapter 2.

104. Referring to telecommunications specifically, Lord Livingston told us that "working with other countries on research and development will be important" because although "we have some great technological base in the UK and great academics […] we most certainly do not have all of it".[296] Discussing the full breadth of critical and emerging technologies, the USA's strategy similarly recognised that it was "not feasible for the United States to lead in all aspects of every technology area".[297] Instead, it set out the country's aim to "maintain clear leadership in the highest priority critical and emerging technology areas and invite its allies and partners to join in those efforts", and to act as a "contributing peer with its allies and partners" in "high-priority critical and emerging technology areas".

105. **Domestic capability in the research, development and adoption of critical technologies is key not only to economic growth and technological progress, but also to national security. It reduces dependency on foreign suppliers and governments, and allows the UK greater scrutiny of technologies for potential vulnerabilities and greater influence over the technological capabilities developed. Managing potential risks from critical and emerging technologies by supporting domestic capability will require early identification of those technologies and assessment of the UK's existing capabilities, as well as the capability of the UK's allies.**

106. ***In producing a national strategy for critical and emerging technologies, the Government should assess the UK's domestic research and development capability for each technology area as well as the capability of its allies. As the Government looks to strengthen research and development in the UK, this assessment should be used to identify particular critical and emerging technology areas of strategic importance in which the UK's capability should be developed and strengthened. This support should not focus on academic research alone, but should also encompass research and innovation capability in businesses and other research institutions.***

107. Universities UK warned in October 2020 that "higher education institutions are subject to regular and targeted attempts by individuals and organisations from overseas seeking to improperly gain access to research and intellectual property".[298] It added that these "risks are increasingly dynamic and growing in complexity" due to the increasing "centrality of universities, science and technology to the future security and prosperity of the UK". It gave examples of several different types of risks, including:

- international collaborations with partners seeking to use the partnership to obtain sensitive information or "exploit the excellence of the UK higher education sector";

295 Digital Catapult (UKT0037)
296 Q401
297 US White House, 'National Strategy for Critical and Emerging Technologies' (2020)
298 Universities UK, 'Managing Risks in Internationalisation: Security Related Issues' (2020)

- cyberattacks seeking to steal intellectual property or data; and
- a lack of awareness among academics of export controls and other national security requirements.

Other organisations have raised similar concerns. The National Cyber Security Centre stated in 2019 that "nation states almost certainly target universities for the data and information they hold".[299] Prior to the Government's National Security and Investment Bill, it further noted that "if foreign direct investment were to come under greater scrutiny or restriction, it is a realistic possibility that the cyber threat to universities would increase, as nation states sought alternative ways to gain access to sensitive research and intellectual property".[300] In 2018, the Australian Strategic Policy Institute reported increasing numbers of researchers affiliated to China's People's Liberation Army collaborating with Western research groups on defence-related and dual-use technologies, sometimes while actively obscuring their links to the Chinese military. It argued that the risks of such collaboration could outweigh the benefits, by "helping a rival military develop its expertise and technology" and "harming the West's strategic advantage".[301]

108. Two of the priority actions identified by the USA's national strategy for critical and emerging technologies were:

- to "ensure that competitors do not use illicit means to acquire United States intellectual property, research, development, or technologies"; and
- to "protect the integrity of the research and development enterprise by fostering research security in academic institutions, laboratories, and industry, while balancing the valuable contributions of foreign researchers".[302]

Universities UK, the National Cyber Security Centre and the Centre for the Protection of National Infrastructure have all produced guidance for academic and business leaders to help them mitigate these risks.[303]

109. ***In producing a national strategy for critical and emerging technologies, the Government should consider the security of the universities, businesses and other institutions conducting research into these technologies. Although guidance for the sector has recently been developed, the Government should monitor its implementation and stand ready to work with institutions to address any remaining challenges as appropriate.***

299 National Cyber Security Centre, 'The cyber threat to Universities' (2019)
300 National Cyber Security Centre, 'The cyber threat to Universities' (2019)
301 Australian Strategic Policy Institute, 'Picking Flowers, Making Honey' (2018)
302 US White House, 'National Strategy for Critical and Emerging Technologies' (2020), p9
303 Universities UK, 'Managing Risks in Internationalisation: Security Related Issues' (2020), National Cyber Security Centre, 'Trusted Research—protecting your research' (2019) and Centre for the Protection of National Infrastructure, 'Trusted Research' (2019)

Conclusions and recommendations

The 5G Supply Chain Diversification Strategy

1. The Government's '5G Supply Chain Diversification Strategy' provides an overview of the Government's intentions for addressing the current lack of vendors in the UK's 5G infrastructure equipment market. The Government itself acknowledges that this will take time. Although the decision to forbid the use of 5G equipment procured from Huawei after 2020 was made following US sanctions announced in May 2020, the potential threat from telecommunications infrastructure supplied by foreign vendors and the concentration in the UK's vendor market have been known for many years. It is therefore disappointing that the Government and its predecessors have not already developed and started implementing a strategy for diversifying the UK's telecommunications infrastructure supply chain. *Given the scale of the challenge and the urgency of the threat, the Government should publish, within three months, a more detailed action plan for implementing its diversification strategy. This should include a breakdown of how the initial budget will be spent and a series of milestones with target dates for completion.* (Paragraph 14)

2. The Government is seeking to attract existing vendors to the UK market in order to diversify the telecommunications vendor market in the short-term. One of the major barriers faced by such companies is the requirement of British network operators for continued provision of older generations of network technology. The main proposal in the Government's diversification strategy to address this—to consider a transition away from these older technologies—is not a short-term solution. (Paragraph 22)

3. *In addition to considering the case for transitioning away from 2G and 3G technologies, the Government should propose measures within the next six months that could facilitate market entry by existing vendors in the near-term. It should consider options for addressing the barrier of operators' preference for vendors to offer older generation technologies with their 5G equipment, such as incentivising or mandating standalone 5G deployments and/or the use of protocols such as the Open X2 interface.* (Paragraph 23)

4. The Government is right to support the development and adoption of open standards and increased interoperability as a potential means of diversifying the telecommunications equipment vendor market. It is also right to identify Open RAN as a prominent approach to achieving this, but not the only one. However, neither the success of Open RAN or any related efforts, nor the positive impact on overall telecommunications security if these efforts are successful, is guaranteed. (Paragraph 29)

5. *The Government should support Open RAN and other efforts to drive the adoption of open standards and greater interoperability. While the success of Open RAN is not guaranteed, the Government should encourage the deployment of Open RAN to ensure that the UK is not behind others in deploying this technology. However, it must continually ensure that support for these efforts is consistent not only with increasing vendor diversity but also with improving the overall security of the UK's telecommunications networks. Further, the Government must not assume that open*

standards and interoperability will inevitably be adopted nor that they will have the desired effect, and should pursue a range of measures designed to support market diversification and increase security. (Paragraph 30)

6. The first live networks using Open RAN are being deployed, with one having launched in Japan last year. *The Government should evaluate these initiatives and report regularly on what lessons can be learned from foreign experiences to inform the UK's strategy for diversifying the vendor market and improving telecommunications security, with an initial report within the next six months.* (Paragraph 33)

7. We heard evidence during our inquiry supporting the Government's assessment that network operators' preference for vendors with proven track records acts as a barrier to potential market entrants. The Government's proposals to establish testing and validation facilities, and to reduce regulatory disincentives for network operators to integrate new vendors into their networks, align with the recommendations for addressing this barrier made by many of the contributors to our inquiry. *Following consultation with industrial and other stakeholders, the Government should report on the required scale and specification of the National Telecoms Lab, to ensure that network operators trust the equipment that it validates for integration into their networks.* (Paragraph 36)

8. Measures to support research and development form a major part of the Government's '5G Supply Chain Diversification Strategy'. Nevertheless, the total funding of £250 million for initial implementation of the strategy is significantly smaller than the tens of billions of pounds invested annually in research and development by the main incumbent vendors. Co-ordination with existing academic and commercial research and development, with clear long-term objectives, will therefore be critical. The Government's reference to establishing a research and development "ecosystem" instead implies, however, a less strategic approach. (Paragraph 43)

9. *The collaborative research and development networks that the Government seeks to develop to support diversification of the telecommunications market should encompass relevant groups at universities and research institutes as well as small- and medium-sized enterprises and large companies. The Government should aim to actively co-ordinate the research and development that it supports so that participants work towards clearly-defined long-term objectives. Existing and newly-established public research facilities should be set up to support this goal.* (Paragraph 44)

10. There is strong support for the establishment of common testing facilities for new 5G infrastructure equipment, to provide a variety of services that could help to drive diversification. The National Telecoms Lab—which appears to be the main facility proposed by the diversification strategy—seems, however, to be focused heavily on security testing and validation alone. (Paragraph 48)

11. *In addition to conducting security testing and validation, the Government should ensure that the research and testing facilities established through the diversification strategy also drive market diversification by stimulating collaboration and supporting the development and commercialisation of new technologies.* (Paragraph 49)

12. Testing facilities do not need to be situated in one physical location. *The Government should ensure that any new testing facilities complement existing facilities, and are designed with potential developments in 5G technology in mind to guard against future redundancy.* (Paragraph 52)

13. New vendors of 5G telecommunications equipment face challenges in scaling up their production rapidly enough to meet network operator demand and compete with incumbent vendors. Although the Government's diversification strategy identifies this barrier to market entry, it defers details of any significant measures to address it until publication of a refresh to the Industrial Strategy. There appear to be good opportunities for the Government to support new market entry at the same time as driving deployment of 5G in the UK, but the diversification strategy fails to set out measures to achieve this. (Paragraph 56)

14. *The Government should align its strategy for diversifying the 5G vendor market with its support for rolling out 5G network coverage. Wherever the Government provides funds for expanding 5G coverage, it should look for opportunities to simultaneously support vendor diversification, for example by requiring the use of open standards. The Government should identify opportunities to support new market entrants scale their production by supporting the deployment of novel small-scale 5G deployments. It should provide details of planned measures to support diversification and expand 5G coverage in its Industrial Strategy.* (Paragraph 57)

15. The Government identified the concentration of intellectual property rights in the hands of established vendors as a barrier to market entry. It commits in its diversification strategy to working with industry bodies to address this, although the proposed work is not described in great detail. *In its response to this Report, the Government should provide more details on how it intends to address the barriers brought about by intellectual property rights, and update us on early progress made against this goal.* (Paragraph 60)

16. Long-standing factors have driven consolidation in the telecommunications vendor market over many years, so it is critical that the Government adopts measures to maintain market diversity as well as to drive the initial diversification. Network operators will be integral to achieving both aims. Although operators stand to benefit from a more diverse vendor market, it may not be in their interest to purchase and use equipment from a wider range of vendors. The Government's diversification strategy does not sufficiently acknowledge this fact, and provides little detail of proposed measures to ensure that it will be in network operators' interest to drive and maintain a diverse vendor market. (Paragraph 70)

17. *The Government cannot rely solely on removing barriers to market entry to diversify the telecommunications vendor market, but must also ensure that network operators actively pursue diversification and act to maintain the diversity achieved. This will require a combination of incentives, measures to reduce operator costs, and regulatory requirements. For example, the Government could introduce business rate relief on mobile mast deployments. In order to provide certainty to the sector, the Government should publish within three months of this Report the measures it is considering to incentivise and require network operators to diversify their suppliers, with an indicative timetable for implementation.* (Paragraph 71)

18. Of Ofcom's two principal duties, it has appeared to have given less prominence to "further[ing] the interests of citizens in relation to communications matters" than it has to "further[ing] the interests of consumers". *Ofcom must ensure that it pursues both of its principal duties and guarantees the security of the UK's telecommunications infrastructure as well as furthering the interests of consumers. The Government should consider the case for updating its statement of strategic priorities for telecommunications, to emphasise the importance of Ofcom's duties relating to telecommunications security.* (Paragraph 74)

19. The UK's telecommunications market accounts for a small proportion of the global market. International co-ordination will therefore be critical to the success of the UK's diversification strategy. The Government's 5G Supply Chain Diversification Strategy acknowledges this fact, and states the Government's ambition for international co-operation. However, the strategy provides little detail of plans for sustained co-ordination on industrial policy with a diverse range of countries. (Paragraph 79)

20. *The Government should seek to establish a dedicated, standing forum for international co-operation on diversifying the telecommunications market, encompassing as many like-minded countries as possible and covering aspects including: research and development; adoption and deployment; standards; and overall strategy. This should not be based on existing intelligence-sharing coalitions. The Government should set out in its response to this Report, how it intends to achieve this, a timetable for establishing such a forum and what progress it has made to date.* (Paragraph 80)

A critical technologies strategy

21. There is a strong risk that the urgent security challenges faced by the UK's telecommunications sector are indicative of a wider, and growing, geopolitical development. Throughout our inquiry, we have heard of the prospect of a growing technological and regulatory divergence between China, and countries aligned with China, and other countries. This is not restricted to telecommunications or even cyber security—artificial intelligence, quantum technologies and synthetic biology are just some examples of other emerging technology sectors that will be prominent in our future economy and security, and in which there is the potential for different technical and regulatory standards to apply. The Government should not regard the problems posed by 5G addressed in this Report as a one-off, but more likely illustrative of a wider challenge. (Paragraph 85)

22. *The Government must treat the current issues in the UK's 5G vendor market as an indication of a much wider geopolitical, technological challenge. The character of the UK's response, and that of other like-minded nations, will have profound implications for future decades and beyond. We urge the Government to address this seriously, comprehensively and without delay. We recommend that within twelve months, the Government should develop and publish a White Paper setting out its assessment of the current extent of and future potential for global technological divergence, the anticipated consequences of such divergence and how it intends to address the challenges this poses.* (Paragraph 86)

23. *As part of its White Paper on global technological divergence, the Government should develop a critical technologies strategy that identifies technologies that are likely to be of critical importance to the UK's prosperity and security over the next ten to twenty years. This strategy should assess the potential opportunities and risks of these technologies, and propose measures to seize those opportunities and mitigate those risks. It should align with other relevant strategies, such as the Integrated Review of Security, Defence, Foreign Policy and Development and the new Industrial Strategy.* (Paragraph 90)

24. The Government has only recently considered the consolidation of vendors in the UK's telecommunications market as a potential risk to national security, although it is a process that has taken place over ten to twenty years. One problem appears to have been the focus on the security of the network operators and not their supply chains, including when setting the role and powers of the regulator. Although the diversification strategy now addresses vendor diversity, it still does not consider the full supply chain. Whereas other nations and regions, including the USA, Australia and the European Union, have produced strategies addressing supply chain risk across all critical technology areas, the Government's diversification strategy addresses only 5G. (Paragraph 93)

25. *In producing a national strategy for critical and emerging technologies, the Government should consider potential risks that could develop across their full supply chains.* (Paragraph 94)

26. The setting of international standards is important for national economic competitivity and technical capability. The influence of British companies and officials in global standards-setting processes is diminishing. Although the '5G Supply Chain Diversification Strategy' sets out the Government's intention to redress this in the telecommunications sector, it is not clear that there are similar plans for other important technological sectors. (Paragraph 99)

27. *In producing a national strategy for critical and emerging technologies, the Government should review the relevant global standards bodies, the objectivity of their processes and the relative influence of different countries. Similar to those measures outlined in its 5G supply chain diversification strategy, the Government should develop measures to build British capability and influence at standards-setting bodies for all critical technologies.* (Paragraph 100)

28. Domestic capability in the research, development and adoption of critical technologies is key not only to economic growth and technological progress, but also to national security. It reduces dependency on foreign suppliers and governments, and allows the UK greater scrutiny of technologies for potential vulnerabilities and greater influence over the technological capabilities developed. Managing potential risks from critical and emerging technologies by supporting domestic capability will require early identification of those technologies and assessment of the UK's existing capabilities, as well as the capability of the UK's allies. (Paragraph 105)

29. *In producing a national strategy for critical and emerging technologies, the Government should assess the UK's domestic research and development capability for each technology area as well as the capability of its allies. As the Government looks*

to strengthen research and development in the UK, this assessment should be used to identify particular critical and emerging technology areas of strategic importance in which the UK's capability should be developed and strengthened. This support should not focus on academic research alone, but should also encompass research and innovation capability in businesses and other research institutions. (Paragraph 106)

30. *In producing a national strategy for critical and emerging technologies, the Government should consider the security of the universities, businesses and other institutions conducting research into these technologies. Although guidance for the sector has recently been developed, the Government should monitor its implementation and stand ready to work with institutions to address any remaining challenges as appropriate.* (Paragraph 109)

Formal minutes

Thursday 21 January 2021

Members present:

Greg Clark in the Chair

Aaron Bell	Darren Jones
Dawn Butler	Mark Logan
Chris Clarkson	Carol Monaghan
Katherine Fletcher	Graham Stringer
Andrew Griffith	Zarah Sultana

Second Report of Session 2019–21: *5G market diversification and wider lessons for critical and emerging technologies.*

After consulting all Members of the Committee, the Chair was satisfied that the Report represented a decision of the majority of the Committee and reported it to the House. (Order of the House of 24 March 2020).

Witnesses

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

Wednesday 24 June 2020

Matthew Evans, Director (Markets), techUK; **Professor Dimitra Simeonidou**, Professor of High Performance Networks, University of Bristol — Q1–40

Attilio Zani, Executive Director, Telecom Infra Project — Q41–60

Thursday 9 July 2020

Woojune Kim, Executive Vice President, Samsung; **Andrea Dona**, Head of Networks, Vodafone UK; **Howard Watson**, Chief Technology and Information Officer, BT Group — Q61–121

Dr Yao Wenbing, Vice President Business Development and Partnerships, Huawei UK; **Mr Jeremy Thompson**, Vice President, Huawei UK; **Victor Zhang**, Vice President and Chief Representative, Huawei UK — Q122–206

Wednesday 22 July 2020

Amy Karam, Global Strategist, Fellow, Canadian Global Affairs Institute; **Dr Dritan Kaleshi**, Head of Technology (5G), Digital Catapult — Q207–249

Rt Hon Oliver Dowden MP, Secretary of State for Digital, Culture, Media and Sport — Q250–314

Wednesday 30 September 2020

Professor Ciaran Martin, Professor, University of Oxford; **Dr Mike Short**, Chief Scientific Adviser, Department for International Trade — Q315–341

Marcus Weldon, President, Bell Labs; **Kip Meek**, Director, Communications Chambers and the Wireless Infrastructure Group — Q342–363

Diane Rinaldo, Executive Director, Open RAN Policy Coalition — Q364–387

Wednesday 28 October 2020

The Lord Livingston of Parkhead, Chair, Telecoms Diversification Taskforce; **Scott Bailey**, Deputy Director of the Diversification Unit, Department for Digital, Culture, Media and Sport — Q388–409

Tareq Amin, Chief Technology Officer, Rakuten Mobile; **Dr Tobias Feakin**, Ambassador for Cyber Affairs and Critical Technology, Australian Government — Q410–427

Dr Ian Levy, Technical Director, National Cyber Security Centre; **Dr Yih-Choung Teh**, Group Director for Strategy and Research, Ofcom — Q428–480

Published written evidence

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

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

1 Anonymous 1 (UKT0009)

2 Anonymous 2 (UKT0017)

3 BT Group (UKT0030, UKT0019)

4 British Standards Institution (BSI) (UKT0021)

5 Burrington, T (UKT0016)

6 CSA Catapult (UKT0032)

7 Davies, Mrs Anne (UKT0003)

8 Department for Digital, Culture, Media and Sport (UKT0034)

9 Digital Catapult (UKT0037)

10 Fitzgerald, Dr A J (UKT0015)

11 Holden, (UKT0012)

12 Huawei Technologies (UKT0005)

13 Institution of Engineering and Technology (IET) (UKT0036)

14 Internet Service Providers' Association (ISPA) (UKT0023)

15 Juniper Networks (UKT0033)

16 Kaltakis, Dr Dimitris (UKT0004)

17 Mavenir (UKT0038)

18 National Physical Laboratory (UKT0007)

19 OneWeb (UKT0014)

20 Openreach (UKT0022)

21 Oracle Corporation UK (UKT0035)

22 Parallel Wireless; and Isotek Microwave (UKT0013)

23 Potter, Mr R B (UKT0010)

24 Rushmere Technology Limited (UKT0025)

25 Samsung Electronics UK (UKT0029)

26 Samsung Electronics UK (UKT0008)

27 ScotlandIS (UKT0006)

28 Seeds, Alwyn (Professor of Optoelectronics, University College London) (UKT0024)

29 Spirent plc (UKT0001)

30 Telecom Infra Project (UKT0028, UKT0027, UKT0018)

31 UK Photonics Leadership Group (UKT0026)

32 Vodafone UK (UKT0031, UKT0002)

33 techUK (UKT0020)

List of Reports from the Committee during the current Parliament

All publications from the Committee are available on the publications page of the Committee's website.

Session 2019–21

Number	Title	Reference
1st	The UK response to covid-19: use of scientific advice	HC 136
1st Special	Balance and effectiveness of research and innovation spending: Government and UK Research and Innovation Responses to the Committee's Twenty-First Report of Session 2017–19	HC 236
2nd Special	Commercial and recreational drone use in the UK: Government Response the Committee's Twenty-Second Report of 2017–19	HC 270