House of Commons

Defence Committee

The Security of 5G: Government Response to the Committee's Second Report of Session 2019–21

Fourth Special Report of Session 2019–21

Ordered by the House of Commons
to be printed 15 December 2020

HC 1091
Published on 16 December 2020
by authority of the House of Commons

The Defence Committee

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

Current membership

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

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

Sarah Atherton MP (*Conservative, Wrexham*)

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

Richard Drax MP (*Conservative, South Dorset*)

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

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

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

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

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

Derek Twigg MP (*Labour, Halton*)

Powers

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

Publications

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

Committee staff

Matthew Congreve (Second Clerk), Mark Etherton (Clerk), Dr Greg Hannah (Committee Specialist), Sascha Sajjad (Committee Operations Officer), Ian Thomson (Committee Specialist), Dr Lauren Twort (Committee Specialist), Sarah Williams (Committee Operations Manager) and George Woodhams (Committee Specialist).

Contacts

All correspondence should be addressed to the Clerk of the Defence Committee, House of Commons, London SW1A 0AA. The telephone number for general enquiries is 020 7219 6168 / 3113; the Committee's email address is defcom@parliament.uk. Media inquiries should be addressed to Joe Williams on 020 7219 8878 | 075 4651 7626 or Toni McAndrew-Noon on 075 6243 5286.

You can follow the Committee on Twitter using @CommonsDefence.

Fourth Special Report

On 8 October 2020, the Defence Committee published its Second Report of session 2019–21, The Security of 5G (HC 201). The Government's response was received on 8 December 2020, and is appended to this report.

Appendix: Government Response

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

The Government agrees that 5G represents a new challenge for managing and mitigating security risks when compared to previous generations of mobile technology/networks. That is why the government undertook the Telecoms Supply Chain Review.

While previous mobile generations connected people to people, 5G has the potential to connect a vast network of people, objects and communication systems, including in critical sectors. The technical characteristics of 5G means that networks will run at much faster data speeds and will be based on software running on commodity hardware, rather than proprietary hardware. This creates opportunities as these new technologies are expected to transform how we work, live and travel—providing opportunities for new and wide-ranging applications, business models, and increased productivity. But as well as creating opportunities, it also creates risks.

The Telecoms Supply Chain Review Report[1] (published July 2019) identified three security challenges:

- First, as the Committee notes, the technical characteristics, such as increase in device connectivity, means 5G networks will have a greater surface area for potential attacks;
- Second, the speed, scale and processing power of 5G will enable a wide range of new services bringing a new dimension to the security risks, in particular as UK critical national infrastructure is likely to have a greater dependence on 5G infrastructure; and
- Third, new technologies could face an increasingly hostile environment, with certain state actors providing the intent and capability to carry out espionage, sabotage and destructive or disruptive cyber attacks—including through access to the telecoms supply chain. These actors may seek to exploit weaknesses in telecoms service equipment, and/or in how operators build and run their networks, in order to compromise security.

This risk assessment was supplemented in January 2020 by the publication of the summary of the National Cyber Security Centre's (NCSC) security analysis for the UK

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

telecoms sector.[2] The Government has complete confidence in the independent technical assessment of the UK's security experts, and the UK Government has published more of its security assessments in relation to 5G and telecoms networks than any other country.

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

The Government's primary aims for 5G are for the UK to become a global leader in the technology by reducing barriers to 5G deployment and realising the full benefits of 5G as quickly as possible. Security is paramount and networks must be secure for their economic benefits to be enjoyed.

The Government's programme of 5G testbeds and trials has sought to leverage UK cyber security expertise to ensure that the UK maximises the benefits of secure 5G networks and maintains our digital connectivity ambitions to support economic recovery and growth.

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

The Government agrees that the UK vendor market is not diverse enough, as highlighted in the Telecoms Supply Chain Review. The Review outlines the need for further diversification in the supply market for access network equipment, in order to reduce the risk of national dependency on a small number of suppliers. While the advice to remove Huawei equipment from the 5G supply chain is the right one, it will result in greater reliance on Nokia and Ericsson equipment. The Government does not believe that this is a satisfactory position in terms of the resilience of supply for an important part of our Critical National Infrastructure.

A more diverse supply chain is absolutely essential to reducing national dependency on any individual supplier as well as driving more competition and innovation in the telecoms supply market. This is why the UK Government has published a multifaceted 5G Supply Chain Diversification Strategy to address this need. This strategy balances rapid measures to maintain the resilience of our networks in the short-term, with bold and ambitious interventions to open up and grow the market in the medium to longer term.

The strategy also focuses on building UK capability across the supply chain. We want to make the most of the UK's vibrant and innovative telecoms sector and to work with industry to test, develop and deploy new and emerging technical solutions.

The 5G Supply Chain Diversification Strategy was published on 30 November.

4. **This inquiry was launched in the context of a lively debate on the security of the UK's 5G network in Parliament and across the country from late 2019 and through**

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

2020 with a focus on the presence in our network of high-risk vendors, particularly Huawei. A significant Government announcement took place in January with restrictions placed on high-risk vendors followed by stricter rules announced in July, with Huawei to be removed from the UK's 5G network by 2027. The UK Government has had to balance technical considerations with wider geopolitical considerations when formulating its 5G policy. (Paragraph 52)

As the Committee notes, the Government has followed an approach that takes into account our specific national circumstances and the full range of risks. The Government made its advice on high risk vendors after considering all the technical, economic and geopolitical information and analysis necessary—from the NCSC, industry and our international partners. This was evidence-based advice based on comprehensive security assessments and noting the realities of the telecoms market. This ensures that we can have confidence in our ability to mitigate the risks to 5G and full fibre networks.

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

Hostile actors must understand that irresponsible behaviour in cyberspace will carry cost. The UK and our allies will continue to expose those that aim to do us and our institutions harm. No longer can they act with impunity in the shadows.

The UK has been at the forefront of demonstrating that there are consequences including through co-ordinating use of existing tools and working to put in place new tools such as EU and UK cyber sanctions regimes. We have set out clearly how international law applies in cyber space.

Malicious cyber activity knows no international boundaries, so neither should our response. We coordinate our response with a wide range of international partners. We share our analysis of the threat and our experience in responding in order to increase the capabilities and commitment of countries around the world to respond.

Malicious actors in cyberspace are active and able to execute successful operations on countries around the world, including the UK, affecting critical national infrastructure, democratic institutions, businesses and the media. These actors are exploiting the Covid-19 pandemic by targeting individuals and organisations with a range of scams, ransomware and malware demonstrating an increased risk appetite, be it for economic, strategic, regional or financial gain.

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

The Government is committed to promoting stability in cyberspace based on the application of existing international law, voluntary norms of responsible state behaviour and confidence building measures supported by coordinated and targeted capacity-building programmes.

The UK works with the European Union, North Atlantic Treaty Organisation, the Organisation for Security and Cooperation in Europe, the United Nations, and bilaterally to protect the future of a free open, peaceful and secure cyberspace. We aim to enhance partners' capabilities, understanding of and willingness to use deterrence tools to increase international pressure on threat actors and counter hostile state activity in cyberspace. We regularly provide information about threats to help our partners to counter them, share information on our approach to deterrence and coordinate with partners on how to respond to state-directed malicious cyber activity.

The UK will not tolerate malicious cyber activity and will react robustly and proportionately to the threat. We are vigilant to these threats, wherever they come from, and we are ready to defend against them. The UK government has exposed those responsible for a range of the most destructive and disruptive attacks, identifying actors in North Korea, China, Russia and Iran.

Deterrence is about convincing actual and potential adversaries that any benefits they may seek to gain by attacking the UK will be outweighed by the consequences. We consider the employment of offensive cyber as part of our broader approach to deny benefits and impose costs on those who conduct malicious activity against the UK, including malicious cyber activity. Our cyber operations are designed and delivered by the recently announced National Cyber Force, a Defence and intelligence partnership. However, we are conscious that deterrence is but one strategy to deal with malign cyber activity and that other strategies may, in some circumstances, be more effective. We reserve the right to react asymmetrically, at a time and place of our choosing, in line with our values and the law.

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

The UK has unique insight into Huawei's presence in our networks and the Government has been quick to respond to the changing risk environment for network security.

Because of the work of the Huawei Cyber Security Evaluation Centre (HCSEC) and the Oversight Board we know more about Huawei, and the risks it poses, than any other country in the world. This information—coupled with the technical security and economic analysis conducted during the Telecoms Supply Chain Review—has provided a clear evidence base for the Government's overall position on mitigating risks from high risk vendors.

The Government will continue to work closely with vendors such as Nokia and Ericsson as we look to diversify our telecoms supply chain, both of which remain of high importance to the UK market.

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

The HCSEC is integral to the UK's Huawei security mitigation strategy and it provides the UK a unique insight into the workings of Huawei equipment and software. The government requires that HCSEC continues to be maintained at an appropriate level while there is any Huawei equipment in the UK telecoms networks. Huawei has committed to this in writing.

The Government is intending to introduce a new security framework through the Telecommunications (Security) Bill. This will consist of strengthened legal security duties in primary legislation and specific security requirements in secondary legislation, for all public telecoms providers to follow. Detailed technical guidance will be set out in codes of practice demonstrating how certain providers should meet their legal obligations. This new framework will place the emphasis on providers to ensure steps are taken to implement a higher baseline of security in the UK telecoms sector. These security requirements will raise the security standards across the sector and will apply to all providers and, by extension, all vendors who supply those providers.

Not all vendors have the same security concerns that are attributed to Huawei; however, high security standards are essential for the secure and resilient functioning of telecommunication networks. Mitigation strategies for each high-risk vendor will be dependent on the specific risks relating to the vendor's circumstances and the context in which they operate in the UK. An HCSEC-like model may not be appropriate for other high-risk vendors.

The Telecoms Supply Chain Review recommended the creation of a national facility to help manage the security, functionality and interoperability of telecoms equipment used in the UK. We expect this to be a secure research facility, allowing teams from academia, subject-matter experts, critical industries and government to research, test and learn about security on the UK's telecoms networks. Further detail is set out in the 5G Supply Chain Diversification Strategy. Creation of this facility, coupled with the requirements on providers to ensure vendor security as part of the new telecoms security framework, should raise the standard of security across the sector.

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

The Government appreciates the recognition of the excellent job that Government Communications HQ (GCHQ) and the NCSC do to manage risk in the UK telecoms network. We have always been clear-eyed about the risk posed by Huawei. Since Huawei first came to the UK in 2003, their presence has been carefully risk-managed and subject to detailed formal oversight through the HCSEC since 2010, and the HCSEC Oversight Board, which has reported annually since 2014.

Through the HCSEC and wider Huawei mitigation strategy and our close cooperation with telecommunication providers, coupled with the technical expertise within NCSC and GCHQ, we know more about Huawei, and the risks it poses, than any other country in the world.

Approaches to Huawei in other countries have been vastly different to the UK. Some governments, particularly in Europe, use transparency centres as a form of oversight. These centres allow host Governments limited access to Huawei source code and equipment. However, they do not provide the same level of scrutiny and access to Huawei equipment and code that HCSEC is afforded.

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

The Government agrees that the UK market will benefit from a greater number of vendors. We have developed the 5G Supply Chain Diversification Strategy, published on 30 November, to diversify the supply chain. We are talking to a range of suppliers about the barriers they face to entering the UK market and how we can accelerate the realisation of our long-term vision for the telecoms access market.

We recognise that there is a need to work at pace to make early progress on diversification. As a first step towards delivering our long-term vision, the Government announced in the National Infrastructure Strategy that it has committed an initial investment of £250 million, to kick off work to deliver our key priorities. Further details are set out in the 5G Supply Chain Diversification Strategy, published on 30 November.

We are also exploring ways to incentivise research and development in the UK telecoms sector, such as alternative 5G deployment models, and accelerating the development of 'interoperable' equipment—kit which can be used by multiple vendors—and making it standard across the sector.

The UK is not alone in facing this problem. We are also working with like-minded international partners to develop new and sustainable supply chain capacity and deliver against our shared goals.

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

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

The Government welcomes the Committee's conclusions and recognition of the Government's response to the changed context. The Government's position as set out in January related to high risk vendors generally; however, the US sanctions in May applied only to Huawei. Following analysis of the implications of the US sanctions by the UK's technical experts in the NCSC,[3] it was clear that the risk in relation to Huawei's presence in future UK networks had changed. As such it was necessary and correct to update the Government's position in relation to Huawei.

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

The Government agrees with the Committee that Huawei should continue to be distanced from sensitive networks. High risk vendors are not—and never will be—in our most sensitive networks. The decision was made in January 2020 that high risk vendors, including Huawei, should be excluded from the core parts of the network that are critical to security and excluded from sensitive sites.

The Telecommunications (Security) Bill that is currently in Parliament will provide the government with new national security powers to impose controls on the use of high-risk vendors.

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

The UK's most sensitive information and capabilities are protected independently of any public networks and their security does not rely on any public network. Our advice on high risk vendors in January and on Huawei in July do not affect our ability to share sensitive intelligence data over highly secure networks both within the UK and with our partners. This has been categorically confirmed by GCHQ.

In addition, the January decision on high risk vendors provided for the banning of high-risk vendor equipment, including Huawei base stations and fibre access, from being deployed near particularly sensitive sites.

14. **The Government has had to balance its own technical considerations with pressures from allies such as the United States. The UK's closest allies, including the United States and Australia, originally embarked on a policy at odds to that of the**

3 https://www.ncsc.gov.uk/report/summary-of-ncsc-analysis-of-us-may-2020-sanction

UK. This had the potential to damage the UK's close intelligence, security and defence relationship with them, although reassurances have been given by Ministers that this was not the case. (Paragraph 91)

The Five Eyes relationship is robust. The nature of the partnership is such that whilst we share the most important, fundamental principles, there are areas where, from time to time, our approaches differ. These differences encourage a diversity within the partnership that reinforces our understanding and approach. We continue to cooperate with our allies and partners on a broad range of security issues.

The security and resilience of the UK's telecoms network is of paramount importance. When necessary, the Government has taken decisive action suited to the UK's unique circumstances, based on expert analysis by our technical advisors and consistent with our security needs.

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

The UK has a special and enduring relationship with the US on security, as well as a vast range of wider issues. That relationship goes beyond any single issue and is deeply rooted in our shared history, interests and values. We have been in close touch with the US on telecoms security throughout the last year and continue to work closely with them to increase global telecoms security standards and promote diversification in the global telecoms industry.

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

Each approach will depend on national circumstances, and the particular risks as they are manifested in each country. It is important that we work closely with allies in this critical area and share experiences and approaches, with the aim of raising global cyber security standards and diversifying the supply chain. The Government is doing that and will continue to engage closely with allies.

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

The UK has always been open to a range of vendors in our telecommunications network. We welcome Chinese investment, but will take the necessary measures to protect our national security—as we have done for our 5G infrastructure.

Since Huawei first came to the UK in 2003, the risk associated with their presence has been carefully managed. Huawei's presence in the UK has been subject to detailed formal oversight through the HCSEC since 2010, and the HCSEC Oversight Board, which has reported annually since 2014.

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

All investment involving critical infrastructure is subject to thorough scrutiny and needs to satisfy our robust legal, regulatory and national security requirements. The new regime introduced under the National Security Investment Bill will be an important addition to existing tools and align more closely with those administered by our Five Eyes allies.

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

The UK and China have a constructive and positive relationship and are clear and direct where we disagree. We welcome Chinese investment, but will take the necessary measures to protect our national security – as we have done for our 5G infrastructure.

In keeping with our principles, the UK is a fair and open market for Chinese investment that adheres to our values just as we will continue to pursue access to China's market. As an open economy, we welcome foreign trade and investment, including from China, where it supports UK growth and jobs. But we will not accept investments which compromise our national security.

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

The UK wants a mature, positive relationship with China, based on mutual respect and trust. There is considerable scope for constructive engagement and cooperation. But as we strive for that positive relationship, we will not sacrifice either our values or our security.

All investment involving critical infrastructure, including nuclear, is subject to thorough scrutiny and needs to satisfy our robust legal, regulatory and national security requirements. The new regime introduced under the National Security Investment Bill will be an important addition to existing tools.

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

The Government agrees that it is vital that we work with our allies on matters relating to network security. That is why we will continue to work closely together to tackle common security challenges, sharing our approaches and experiences with security partners to allow effective risk-mitigation and raise cyber security standards together.

Collaboration and engagement with international partners will also be essential to achieving the UK's ambitions on diversification to support industrial capacity. The UK represents a relatively small share of the overall telecoms supply market, and so to drive change on issues such as standards, which exist within well-established international organisations, we will need to work with like-minded partners to forge a consensus on these issues.

The market failure that has restricted diversity and choice in the telecoms supply chain is an international problem and needs international cooperation to address, so we want to work with like-minded countries to achieve these goals. The UK is committed to acting internationally as a burden-sharing, problem-solving nation and, to do that, we work with others bilaterally and in a range of formal and informal multilateral fora. Different groupings are best suited to different issues and each therefore has its particular value. Those groups have always evolved and will continue to do so.

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

The UK is currently a member of a number of different small groups, both informal and formal, which serve a variety of purposes. Those groups have always evolved and will continue to do so.

We believe that liberal democracies and open, market economies are, by virtue of those characteristics and their shared values, best-placed to achieve a common agenda, domestically and internationally. The Government will consider how that can best be advanced through current or new groupings.

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

Standards are a crucial part of the Government's work to diversify the supply chain. Identifying and shaping priority telecoms standards in a more democratised and transparent way is crucial to ensure that standards setting bodies consider the vast range of stakeholder needs, and support diversification, innovation and open interfaces. This will include assessing how we can best support UK industry to embed them in standards work to deliver in these areas. The related standards setting bodies are industry-led and global in nature, so this will require working closely with industry to promote this.

It will also be important to work with our international partners to promote further the principle of interoperability and help to achieve our ambitions in creating a more diverse telecoms equipment market. We will be starting this work as soon as possible. This will be crucial for effecting lasting change and the Government is assessing how we can best position the UK for leadership to support our needs.

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

The Government recognises that there may be pressures to remove Huawei from 5G networks before 2027; however, we have provided this advice after taking into account our specific national circumstances and how the risks from these sanctions are manifested in the UK. To go further and faster beyond a 2027 target would add considerable further costs and delays to rollout of the 5G network. As the Committee notes, working to a shorter timetable for removal would mean a greater risk of actual disruption to mobile telecoms networks.

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

We duly note the recommendation to articulate a long-term plan, which aligns with the PM's ambition for the UK to be a 'Great Science Power'. On 1 July, the Government published its ambitious Research and Development Roadmap to ensure the UK is the best place in the world for scientists, researchers and entrepreneurs to live and work, while helping to power up the UK's economic and social recovery and level up the UK. The Roadmap builds on the ambitious commitment set out at Budget to increase public spending in research and development to £22 billion by 2024/25, putting the UK on track to reach 2.4% of GDP being spent on research and development across the UK economy by 2027.

We are now working with universities, businesses, the third sector and across government to develop a more detailed plan for delivering on the Roadmap's ambitions. This will complement a refreshed Industrial Strategy, which will put the UK at the forefront of emerging technological opportunities and will boost productivity across the country, while supporting our long-term recovery and transition to net zero.

As part of our work on the Roadmap, we continue to very actively consider how best to protect the research and development assets we regard as central to the UKs interests and will report on this in due course. Concurrently, we are continuing to develop principles and refine the necessary governance to guide future strategic decision making on critical and emerging technology.

The Government is committed to the long-term security and enduring resilience of the UK's telecoms network. We have published the 5G Supply Chain Diversification Strategy for the telecoms industry to deliver on this commitment. It is vital that we address the market failure that has led to a lack of competition in the telecoms supply chain.

This is not just an issue that the UK is facing. Diversification is a global issue and we need to work collaboratively with like-minded partners to deliver solutions that open up the market to alternative telecoms infrastructure providers and to develop new and sustainable supply chain capacity on a global scale.

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

The Telecommunications (Security) Bill makes clear that providers are responsible for the security of their own networks and services. As such, we expect the cost of ensuring adequate security to be met by individual providers. We remain committed to working with industry to ensure a proportionate approach to implementing the details of the strengthened security framework that will determine the scale of impacts.

The Minister for Digital Infrastructure has already announced that the Department for Digital, Culture, Media & Sports (DCMS) will be consulting on whether further changes to the domestic Electronic Communications Code are needed to address access to land issues and make it cheaper and easier for networks to be deployed, maintained and upgraded.

This initiative was already in place before the recent announcements regarding high risk vendors and consultation will take place in due course. DCMS and the Cabinet Office are progressing initiatives to ensure that public sector landlords (including government departments and local authorities) work collaboratively with the digital sector to provide access to public sector land, buildings and other assets.

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

The Government agrees that the UK market for vendors is far from satisfactory, and we recognise that there is a need to work at pace to make early progress on diversification. The Government announced in the National Infrastructure Strategy that it has committed an initial investment of £250 million, to kick off work to deliver our key priorities.

However, we recognise that it is long term market failure that has brought us to the position where the market has consolidated to a small pool of scale suppliers. We have developed a targeted 5G Supply Chain Diversification Strategy, published on 30 November, to diversify the supply chain and strengthen the UK market. We are talking to a range of suppliers about the barriers they face in entering the market and how we can accelerate the realisation of our long-term vision for the telecoms access market.

We are also exploring ways to incentivise research and development in the UK telecoms sector, such as alternative 5G deployment models, and accelerating the development of 'interoperable' equipment—kit which can be used by multiple vendors—and making it standard across the sector. This in turn would bolster the position of vendors to enter the market and strengthen our position on 5G.

The Government is committing to diversifying the UK telecoms supply chain and has appointed the Telecoms Diversification Taskforce to support it in this work. The Taskforce, which is composed of leading figures from industry and academia, is already providing independent and expert advice to the Government—turbocharging our diversification strategy.

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

The Government is having regular discussions with companies across the industry, both mobile operators, and suppliers such as NEC, Samsung and others, to find solutions that work for them.

We recently announced our intention to provide NEC with £1.6 million grant funding towards an innovative NeutrORAN testbed as a part of the 5G Testbeds and Trials programme. This grant funding is a clear showcase of the UK's commitment to, and momentum in, Open RAN development, that will position the UK as a leader in adopting Open RAN technology.

Additionally, 17 UK small and medium-sized enterprises (SMEs) are involved in 5G Create projects, including those that will help to drive forward the government's work to open up the UK's telecoms supply chains. Three of the six projects—5G Edge-XR, 5G Smart Junctions and Liverpool 5G Create—involve British SMEs trialling the use of open access 5G infrastructure and network solutions. BT's 5G Edge-XR project will be tested in a platform that includes Samsung kit, marking the first time the South Korean telecoms vendor is participating in a UK-based 5GTT project.

Further details on how we plan to promote the development of industrial capacity in the UK can be found in our 5G Supply Chain Diversification Strategy, published on 30 November.

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

The Government agrees that OpenRAN is an important part of the future diversification of telecoms networks alongside other technologies that support open and interoperable networks. Our diversification strategy is based around three key strands; i) supporting incumbent suppliers, ii) attracting new suppliers and iii) accelerating the development of open-interface technologies, to grow the market and promote competition and choice. Solutions such as OpenRAN will be key to creating a diverse, open and sustainable supply chain, and present an opportunity for the UK to build its capability as a global leader in technological development and in production.

Our investment into NEC's NeurtORAN trial is a clear commitment to accelerating open interface solutions.

Vodafone UK recently announced its commitment to deploying Open RAN technology across 2,600 of their sites between 2022 and 2027. That expertise will be leveraged as the Government develops measures to accelerate the development and deployment of Open RAN.

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

The Government's most important duty is national security. The Government fully supports the statement that commercial decisions cannot be placed above security, that

is one of the reasons that the Telecommunications (Security) Bill has been introduced to parliament. The Bill was introduced to the House of Commons on 24 November 2020. It will ensure that we have the powers we need to drive up security standards and control the presence of high-risk vendors.

The new security framework will be one of the strongest regimes for telecoms security in the world. At the heart of the security framework will be strengthened security duties which will raise the height of the security bar and set out tough new standards for public telecoms providers to meet in the design and operation of their networks.

The legislation will also establish stronger national security powers for the government in relation to telecoms security, to allow it to impose new, stringent controls on the presence of high-risk vendors in the UK telecoms networks.

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

The Telecommunications (Security) Bill was introduced to the House of Commons on 24 November 2020.