

PARLIAMENTARY DEBATES

HOUSE OF COMMONS
OFFICIAL REPORT
GENERAL COMMITTEES

Public Bill Committee

TELECOMMUNICATIONS (SECURITY) BILL

Second Sitting

Thursday 14 January 2021

(Afternoon)

CONTENTS

Examination of witnesses.
Adjourned till Tuesday 19 January at twenty-five minutes past
Nine o'clock.
Written evidence reported to the House.

No proofs can be supplied. Corrections that Members suggest for the final version of the report should be clearly marked in a copy of the report—not telephoned—and must be received in the Editor’s Room, House of Commons,

not later than

Monday 18 January 2021

© Parliamentary Copyright House of Commons 2021

This publication may be reproduced under the terms of the Open Parliament licence, which is published at www.parliament.uk/site-information/copyright/.

The Committee consisted of the following Members:

Chairs: MR PHILIP HOLLOBONE, † STEVE McCABE

† Britcliffe, Sara (<i>Hyndburn</i>) (Con)	† Richardson, Angela (<i>Guildford</i>) (Con)
† Cates, Miriam (<i>Penistone and Stocksbridge</i>) (Con)	† Russell, Dean (<i>Watford</i>) (Con)
† Caulfield, Maria (<i>Lewes</i>) (Con)	† Sunderland, James (<i>Bracknell</i>) (Con)
Clark, Feryal (<i>Enfield North</i>) (Lab)	Thomson, Richard (<i>Gordon</i>) (SNP)
Crawley, Angela (<i>Lanark and Hamilton East</i>) (SNP)	† Warman, Matt (<i>Parliamentary Under-Secretary of State for Digital, Culture, Media and Sport</i>)
† Johnston, David (<i>Wantage</i>) (Con)	West, Catherine (<i>Hornsey and Wood Green</i>) (Lab)
† Jones, Mr Kevan (<i>North Durham</i>) (Lab)	† Wild, James (<i>North West Norfolk</i>) (Con)
† Lamont, John (<i>Berwickshire, Roxburgh and Selkirk</i>) (Con)	Sarah Thatcher, Huw Yardley, <i>Committee Clerks</i>
† Matheson, Christian (<i>City of Chester</i>) (Lab)	
† Onwurah, Chi (<i>Newcastle upon Tyne Central</i>) (Lab)	† attended the Committee

Witnesses

Hamish MacLeod, Director, Mobile UK

Matthew Evans, Director, Market Programmes, TechUK

Stefano Cantarelli, Global Chief Marketing Officer, Mavenir

John Baker, Head of RAN Business Development, Mavenir

Pardeep Kohli, CEO, Mavenir

Chris Jackson, President and CEO, NEC Europe Ltd.

Julius Robson, Chief Strategy Officer, Small Cell Forum

Dr Louise Bennett, Director, Digital Policy Alliance

Dr Scott Steedman CBE, Director of Standards, British Standards Institute

Charles Parton, Royal United Services Institute

Public Bill Committee

Thursday 14 January 2021

(Afternoon)

[STEVE McCABE *in the Chair*]

Telecommunications (Security) Bill

Examination of Witnesses

Hamish MacLeod and Matthew Evans gave evidence.

2.1 pm

The Chair: Order. We will now hear from Hamish MacLeod, the director of Mobile UK, and Matthew Evans, the director of market programmes at techUK. We have until 2.45 pm for this session, and I will try to alternate as best I can. May I ask the witnesses in turn to introduce themselves for the record?

Hamish MacLeod: I am Hamish MacLeod, and I am the director of Mobile UK, which is the trade body for the UK's four mobile network operators.

Matthew Evans: My name is Matthew Evans, and I am director of markets at techUK, the trade association for the wider technology sector, which has several telecom-related members.

The Chair: Who would like to have the first question?

Q26 James Sunderland (Bracknell) (Con): Gentlemen, good afternoon to you and thank you for coming in. A very quick and easy question: how do the challenges of maintaining security in a mobile network differ perhaps from those of a fixed network?

Matthew Evans: I am happy to take that question. From the principle point of view, the principles of cyber-security are the same regardless of the network: having security built in by design, but also having a zero-trust principle and good assurance that your defences are looking inwards as well as outwards. On a principle basis, they are very similar.

Hamish MacLeod: I have nothing to add to what Matt said.

The Chair: Thank you. Who is next?

Q27 Dean Russell (Watford) (Con): I would be interested to know whether you agree that strengthening the UK's telecom security through this Bill is important as we continue to roll out the gigabit connectivity.

Matthew Evans: I am happy to take that as well. We completely agree with the overall objective of the Bill, which we think provides clarity to the sector and helps us to further enhance the security and resilience of the UK's telecommunication networks. Obviously, as more and more services and applications are used over our fixed and mobile networks, ensuring their security and resilience is incredibly important. That is why we are pleased to welcome the Bill and the associated diversification strategy alongside it, which is obviously separate to the Bill but intrinsic to matters of resilience as we seek to broaden the supply chain.

Hamish MacLeod: I should perhaps reiterate what my colleague said this morning—that the mobile sector very much welcomes the Bill. Security has always been a top priority for mobile operators. We have always worked closely with the National Cyber Security Centre, but this is a great opportunity to formalise the arrangements and to make them more structured and transparent.

The Chair: Chi Onwurah, did I detect that you were going to ask questions on behalf of Catherine West?

Q28 Chi Onwurah (Newcastle upon Tyne Central) (Lab): Thank you, Mr McCabe. I was going to ask on behalf of my colleague, Catherine West, who cannot be here because we have chosen to sit physically rather than remotely. *[Interruption.]* It has been decided that we will sit physically. Her question is about international comparisons. Are you aware of what is happening with other countries' security frameworks in addressing Huawei and high-risk vendors? Are you aware of any international comparisons?

Matthew Evans: From techUK's point of view, obviously our members—you heard from some of them this morning, and you have more this afternoon—operate across a number of different territories. We seem to be the furthest, or the most advanced, in bringing into place quite a holistic security regime. That is in the first half of the Bill. Obviously, the conversation about high-risk vendors is prevalent in other areas, but I would say that in terms of bringing in a regime that covers the entire telecoms sector, this seems to be a world-leading initiative.

Hamish MacLeod: Chi, I am certainly aware of what other countries are doing as regards high-risk vendors. The operators absolutely accept the Government's policy and the 2027 timeline. The important thing now is to stick to that timeline, because it allows not only for an orderly removal of the HRV equipment, but for alternatives to develop and emerge as viable competitors to the remaining companies.

Q29 Chi Onwurah: So, what are other countries doing that you are aware of?

Hamish MacLeod: The States, New Zealand and Australia have all excluded Huawei, among others. We could supply you with a full list if that is needed.

Q30 Miriam Cates (Penistone and Stocksbridge) (Con): The Government's diversification strategy goes alongside the Bill. Obviously, the principle driver of the diversification is security reasons, but it will also open up the networks to smaller operators—I imagine, Matthew, many of your members are much smaller companies. Do you think that it will have a positive effect on the sector, in that sense, and are there any other barriers to entry for the smaller tech companies that you can identify and that could be addressed in the Bill?

Matthew Evans: Thank you for that question. As I said at the start, we welcome the Government's diversification strategy. It looks to tackle four issues, really, which are supporting incumbent suppliers to the UK market; attracting other global-scale suppliers; accelerating open interfaces and interoperability; and then the fourth area, which we could probably do with more detail on, which is really building on that domestic capability. I know that the taskforce that helped Government to frame the strategy is working on that aspect of it. As I say, I think we could do with some more detail.

However, we welcome the funding that has come alongside that strategy, and I think that we have a real opportunity in the UK in some of the areas where we have traditional strengths, in the software side in particular, to build some world-leading capability. As for the Bill itself, I do not think that it necessarily presents a barrier to that domestic capability; it is more in how we develop the strategy that sits alongside the Bill.

Hamish MacLeod: Just to add to what Matt said, yes, we very much welcome the diversification strategy. It is an absolutely necessary step to mitigate the risks of having to rely on two incumbents. It gives the UK an opportunity to have a leadership role in the development of exciting new technologies, such as open RAN, and, as Matt said, to grow the supplier base in the UK in the mobile sector.

Q31 Mr Kevan Jones (North Durham) (Lab): I think we have heard from the witnesses here now and from other operators that the 2027 deadline is important, in terms of not changing. We hear a lot about diversification, but let us be honest: we are going to have to have two vendors up until 2027 and possibly for a long time after. That is because, regarding the investment decisions taken by mobile phone operators, they are clearly not going to put kit in and then suddenly take it out post-2027. So, being realistic about the diversification strategy, which I support in terms of its ambitions, in practical terms—in terms of influencing what is in our telecoms—it is going to be a long way off yet, is it not?

Hamish MacLeod: Yes. As I just said, the 2027 deadline is very important, because that will give time for realistic competitive alternatives to develop. The open RAN is being deployed in the UK in sort of rural areas and in the less high-performance environments, and that will change over time. The investments that this diversification strategy talks about in research and development will help to develop open RAN, and also in the test bed programmes. All these things will help to build the capability of alternative vendors.

Matthew Evans: Just to add to Hamish's answer, there is a reason that we have a relatively constricted number of scale providers for telecoms, and it is the level of R&D required—that is the risk associated with each generation of technology if it is not taken up on a global scale by operators. To be realistic, we are likely to be focused around two incumbent vendors in the short term.

I think that what the diversification strategy sets out, though, and in fairness it is a strategy and not a complete plan, is a path to open up the UK market to those scale providers who at the moment do not participate in it. That is through trying to reduce the commercial and regulatory barriers that we face, such as on spectrum defragmentation and on providing a single RAN solution—at the moment in the UK, there are obviously 2G, 3G, 4G and 5G. But it also then opens up the possibility of greater use of technologies such as open RAN, which really breaks away from that proprietary architecture, whereby we have both the hardware and the software from the same provider.

That will be a challenge in the short term, but in the medium to long term there are actions that can be taken both to attract the scale providers not in the UK market and to make the UK market attractive to people who work in the open RAN area as well. So I think a dual-track approach helps to bring diversification to the UK market.

Q32 Mr Jones: I do not disagree with you in terms of the ambition to invest in open RAN technology, but, realistically, we will have to rip out Huawei hardware and replace it with Nokia or Ericsson equipment. Operators ripping that out just to test something on open RAN is not going to happen, is it? So we are stuck with these two suppliers for a long time yet. There will have to be a business case for open RAN because, if we look back at the history of where we are at with the limited market that we have in hardware—we will not go back to the ancient history of Margaret Thatcher's silly decision to privatise BT—and if we look at the profitability in terms of hardware, it is not there because we as consumers always want cheaper telecommunications and the companies want to get their costs down. Unless there is a very strong business case for open RAN in terms of deploying that technology, it is not going to happen, is it?

The Chair: Mr Evans, let us go to you first.

Matthew Evans: Is it going to be easy? No is the short answer. Is it possible to increase that diversification? Yes. We would like to see more commercial incentives for operators, who will have to change and adapt. This will be a change for operators as they diversify their vendor base. Part of the strategy has to be around the scales and the commercial incentives for operators to do so. We have certainly seen, as we heard from the witnesses this morning, UK operators really pushing the boundaries in terms of what open RAN trials can deliver. As I said, I suspect it will not be a short-term solution, but it is promising to see the trials that are already under way in the UK.

Hamish MacLeod: I would also like to highlight the Government's commitment to taking a greater part in the process of international standard setting and driving scale across the global market. Although we expect the operators to do the technical heavy lifting, the Government can leverage our international relationships, and the actual resource makes the whole standardisation process move along more quickly.

Q33 Mr Jones: I do not disagree on that, but let us be honest. Telecommunications is a competitive market. If we want to move to open RAN or make real generational change, the Government will have to intervene quite heavily in the market to change minds. Operators will not do it unless they see a competitive advantage. That is possibly why we have had the situation with the hardware side of it, with China buying into the market by undercutting other people and providing state subsidies, for example. Without support for R&D and actual market intervention, that radical change will not happen quickly.

Matthew Evans: I think the £250 million is clearly initially focused on the R&D ecosystem. That is a big commercial barrier when you look at the testing environment and the time it often takes for operators, understandably, to feel confident in deploying equipment into their networks, because they are ultimately responsible for the integrity of them. If we can supercharge the testing environment in the UK, we should be able to shorten the time to market, but open RAN in particular is going to require a boost in funding to accelerate the maturity of that technology.

The other part of the diversification strategy is the scale vendors that may be operating in other parts of the world but are not present in the UK today. That is

why it is also important to tackle some of the regulatory or commercial barriers that exist and prevent them from entering the market today.

Hamish MacLeod: I do not think I really have anything to add to what Matt just said.

Q34 David Johnston (Wantage) (Con): I think we all support diversification in principle, but what does success look like for the two of you? How many companies would it be? We have only two vendors that we can choose from at the moment, so how many do you think is acceptable? Is there an analogous comparison for you, whether in tech or elsewhere, of the much broader choice that we should be aiming for, and how long do you think it will take to get there?

Hamish MacLeod: One of the things about open RAN and more open architecture generally is that you generate competition in the hardware and in the software—it is not one package—so I think it is realistic to expect more competition, particularly in the software side of things.

The Chair: Do you have anything to add, Mr Evans?

Matthew Evans: Not too much. It is hard to put a number on it, but success would be where we clearly have a greater number of vendors than today, and that is a mix of open and proprietary technology. As Hamish says, the reason it is hard to put a number on it is that in that open stack, you could have competition within the stack, rather than between vendors that sell the consolidated package.

Q35 David Johnston: So you do not want to put a number on it, but is there another sector that you would draw a comparison with that does not have this problem and is, in principle, the sort of thing we should be aiming for here?

Hamish MacLeod: The analogy that has sometimes been used with me is looking back 40 years to the computer market. We all used to buy IBM computers and you got the computer and all the software integrated, and then the two separated out. There was interoperability and you create a lot more competition and innovation. That is a potential analogy—a rough analogy, I would say.

The Chair: Anything to add, Mr Evans?

Matthew Evans: No, that is a good analogy.

Q36 Christian Matheson (City of Chester) (Lab): I want to follow up the point that Mr Jones and Mr Johnston made. The Government are requiring the industry to make these changes for all the reasons that we understand. We are hoping for diversification across the sector to provide innovation. What would the industry be looking for from the Government to assist that and drive it forward? Mr Jones talked about the role of the Government in assisting that. How could they best assist that?

Matthew Evans: The strategy sets out the outline of what the industry would like to see. There are commercial and regulatory barriers that need to be removed or analysed. That includes things like how the lifespan of 2G, 3G and 4G in the UK is going to exist, and setting out a road map. That will allow people to develop

technologies in 5G and future generation without having to invest in what are still very good technologies—those that have already been deployed.

What we would like to see in the strategy—this is where the funding is really important—is the R&D and testing ecosystem. We would like to see something like the Future Networks Initiative, which is a proposal for a series of test centres around the UK specialising in different areas of telecoms, particularly open RAN. As I said before, that should help accelerate the adoption of new products and services when utilised in conjunction with the National Telecoms Lab. That is key. As Hamish has said, standards are also really important. Again, we need closer collaboration between the Government and industry, because the technical side is naturally going to be driven by industry.

The Chair: Mr MacLeod, do you have anything to add?

Hamish MacLeod: Very little to add. Personally, I can say that the recent 5G testbed programme that the Government have been initiating to generate interest, applications and scale is a good model. We expect to see that being replicated; indeed, the two might work hand in hand going forward.

The Chair: Thank you. I am going to switch to the Minister and shadow Minister. If there is time left, I will come back to other Members, but I want to be sure that we do this fairly. I call Chi Onwurah.

Q37 Chi Onwurah: Thank you, Mr McCabe, and I thank our witnesses for joining us. I started out in telecoms in 1987, as a hardware engineer. Since then, as you have indicated, our hardware sector in telecoms has disappeared. Hamish, you have talked about the equivalence with the computer sector, which has experienced a similar demise over the past 40 years. I am interested in whether it is possible to have a secure telecoms supply chain without having secure hardware. What are your views on that? The draft vendor designation talks a lot about the geopolitical influence of China rather than about the technical requirements, and that would be as true for hardware as it is for software. Do you think it is possible to have secure supply chains without having sovereign or friendly hardware capability?

I am also really interested in what you said, Mr Evans, with regard to research and development. I absolutely agree with you that we clearly need investment in research and development if we are to lead in hardware and in open RAN and software. You said that the £250 million was focused on R&D, but it is actually focused on testing. It does not really do much for research at all, as far as I can see. You also referred to the diversification strategy as a strategy and not a plan, so do we need investment in research and development? Is the £250 million, which I think—I am looking at the Minister now—is over five years, a significant amount of investment in research and development for the mobile sector and tech sector generally?

Finally, the Bill gives the Secretary the State a huge amount of powers to set out requirements to remove vendors and for Ofcom to inspect what operators are doing. Do you think that might have an impact on international foreign investment in the UK telecoms

sector, and are you confident that the right sort of technical, security and democratic scrutiny is in place? That is three things: hardware, research and development, and scrutiny.

The Chair: Shall we start with you, Mr MacLeod?

Hamish MacLeod: I think the question that was directed at me was whether it is possible to have a secure supply chain. I will not try to gainsay Chi's knowledge on this, but my understanding is that that is the role that the proposed National Telecoms Lab will perform, to validate that security aspect.

Matthew Evans: I agree with Hamish on that first point, to answer Chi's questions on R&D. We do not yet know how the £250 million is going to be spent. We believe that we will need to accelerate the maturity of technologies such as open RAN, to make them deployable and commercially viable. Yes, we do need to see more, but as I said, that has to be alongside testing, because accelerating the maturity of it does not really matter if the operators do not get that confidence in either the hardware or the software.

In terms of the Secretary of State's powers, we are broadly comfortable. We would like to see some thresholds on what amounts to a security compromise, particularly in terms of Ofcom's powers of oversight. From our point of view, and this is also relevant to the foreign direct investment question, if it is evidence-based, as transparent as possible—we know that we will not see all that evidence, particularly that element in the security services—and the actions are proportionate, that is also important. We believe that that builds into the best practice that we see in other areas of national security.

In terms of the technical expertise, we know that NCSC is going to work closely with Ofcom, in terms of providing that oversight. We are comfortable with the experience that we have had over the past couple of years, as the telecoms supply chain has gone through, in terms of the expertise and the overall regime that this Bill seeks to put in place.

Q38 Chi Onwurah: To clarify that point, you are happy with the existing level of scrutiny and involvement of the security services in the development of the framework and the review of the telecoms supply chain, and so on, and you would like to see that continued. When it comes to investment, could you say a little bit about the £250 million over five years, which is, say, £50 million a year? Is that a significant amount of research and development investment in the tech sector in this country?

Matthew Evans: I think it sends quite a strong signal to the market of the Government's intent. If we published the strategy without the funding, it would not have sent the same signal. We have seen NEC, for instance, commit to opening an open RAN test centre in the UK. I think that is a signal of how the market is starting to react. This needs to work with the grain of industry, so it is important that industry is able to participate in this funding. I think it sent a strong signal.

The Chair: Do you have anything you want to add, Mr MacLeod?

Hamish MacLeod: No.

The Chair: I will switch to the Minister at this point.

Q39 Matt Warman (Boston and Skegness) (Con): Thank you, Mr McCabe, and thank you both for your engagement and for welcoming what we are doing. I am interested to know what you feel will be the best way to work with the sectors that you represent, particularly in taking forward the diversification strategy. It is an increasingly diverse sector. The Government want to get the best they possibly can out of that £250 million initial tranche of diversification money. What are your thoughts on how we have worked with the sector thus far and what more should be going on in the future?

Hamish MacLeod: My meeting following this hearing is with the operators addressing that very point. This is something that we want to work extremely closely with the Government on. We are meeting officials next week to continue the conversation on doing things such as setting out the road map for what needs to be done R&D-wise to develop open RAN, what needs to be done from the point of view of the test programme, and what needs to be done on the standardisation road map. We will be taking a very close interest, both as individual operators and jointly.

Matthew Evans: To add to that, I echo that we have had excellent engagement with the Minister's officials. It is about keeping the momentum up while working with the grain of industry and making sure that we are getting the incentives on the supply side, in the R&D and in the testing, and also in the demand side. That is all about making sure that we have the right commercial incentives for operators, but also that we have the right skills and, if necessary, reinforcing the operators on some of those points as well.

The Chair: Chi?

Q40 Chi Onwurah: I did not think I would get a chance to ask further questions.

I respect your reluctance, if you like, to voice criticisms at this stage, but can I just get a further idea on the level of R&D spend in the sector? We heard from British Telecom this morning that it spends £500 million a year. I imagine it is not the only company to spend. Do you have a view of the level of R&D spend? You talk about the £250 million being a signal. Am I right in thinking that a lot more investment needs to be attracted into the UK telecoms sector in order to really move the dial? That is what we are talking about, is it not—really moving the dial on UK telecoms capability?

Hamish MacLeod: Absolutely. The £250 million was very much described as an initial £250 million, because you are right that moving the dial will take significant investment. With R&D, there is pure R&D—what you do in labs—but there is also the testbed activity, which is a very important aspect, and trials at scale and all those things. Working with the operators, bringing in international partners and leveraging what is going on elsewhere in the world will all be important.

Matthew Evans: The important word there is “leveraging”. Telecom spend on R&D, both traditional and in open RAN, runs into billions and billions of pounds each year, but we can use that £250 million to leverage greater investment. It has to be with the grain of what the industry is delivering, so we can attract more of that investment. If we can be world leaders in the adoption of open RAN, that is key, and we will attract that investment. That is why I think the supply has to match up with the demand side fully.

The Chair: Does anyone else have any other questions? No. In that case, I thank both our witnesses for their evidence. We are extremely grateful to you. We will end this session and move on to the next panel.

Examination of Witnesses

Stefano Cantarelli, John Baker, Pardeep Kohli and Chris Jackson gave evidence.

2.39 pm

The Chair: We are now going to hear from Stefano Cantarelli, global chief marketing officer, John Baker, head of RAN business development, and Pardeep Kohli, chief executive officer, of Mavenir. Joining them is Chris Jackson, president and chief executive officer of NEC Europe Ltd. We will use the same format as last time, although if you want to direct your question to a specific witness, that might be helpful. We have until 3.30 pm for this session. I ask the witnesses to introduce themselves.

Stefano Cantarelli: Good afternoon everybody. My name is Stefano Cantarelli. I am the chief marketing officer for Mavenir. I have spent the last 30 years of my life in telecommunications, of which 20 years have been in the UK, in both fixed and mobile networks.

John Baker: Good afternoon. I head up business development for Mavenir. I was instrumental in setting up the UK industry back in the '80s for manufacturing and R&D for Nokia, and with Vodafone and Orbitel. I have long experience in the industry and I have been leading the open RAN initiatives from the US globally. I am a member of the open RAN policy coalition board.

Pardeep Kohli: I am Pardeep Kohli, President and Chief Executive Officer of Mavenir. I have been with the company since 2005. The company is over 20 years old and employs about 4,500 people. We have a good presence in the UK. We have been providing software for telecoms applications to UK operators for over 20 years. All operators use our software today for making phone calls, sending messages and voicemail. We started working on open RAN five years ago and now we have deployment in the UK, which has been provided in the test sites. We are building networks in other parts of the world as well, based on open RAN.

Chris Jackson: Good afternoon. I am Chris Jackson, CEO of NEC Europe. I have worked for NEC for 12 years. I took on the role of CEO for Europe on 1 April last year. In terms of my opening statement, I fully support the principles of the Bill. It has been well constructed. The additional powers that the Government and Ofcom now have are much more wide-ranging, and we absolutely support that. We very much promote the vendor diversification strategy, and we are supportive of the aims and objectives behind it.

The Chair: Who wants to go first? It looks like it is Mr Johnston. Can I just ask you to say which of the witnesses you are directing your question to?

David Johnston: Yes, although I was going to ask them who they think is best to answer it.

The Chair: There is always one.

Q41 David Johnston: We asked the previous witnesses this question. When it comes to stringency on these issues, do any of you feel able to give us a sense of the international comparison between the regime that this Bill creates and regimes around the world?

John Baker: Perhaps I could take that one. This is falling in line with what is going on globally. We see initiatives coming from Spain, the EU and the US. The US is further ahead in terms of passing law on trusted suppliers, and it is now setting timelines and budgets for taking suppliers out of the network. That rip-and-replace programme is now under way. The money for that was approved in December, and operators are looking at open RAN as solutions for that. That is very similar to the activities that you are planning through this Bill in the UK.

Chris Jackson: What we have seen in Japan is strong support for this direction, but I think the UK Government have taken the lead in terms of putting forward an aggressive stance on this to ensure that the security of the country is protected. The UK is doing everything that we would expect it to, and we fully support that.

Stefano Cantarelli: Some of the things said about the diversification of the supply chain are particularly important in terms of the ability to create competition and, as such, innovation. The interoperability of interfaces is fundamental in order to boost data and to be able to create more competition. We strongly believe that competition is based in innovation, and innovation these days can create a very powerful cycle of technology. It is not like how it was in the old days when it took maybe a year, two years or three years to get things into deployment; today, in less than a year a trial can become a commercial deployment.

Pardeep Kohli: I agree with the other gentlemen. In a number of countries, operators have made the decision that, going forward, they will only buy open RAN-based solutions. Governments are supporting that in many parts of the world.

Q42 Mr Jones: This question is to whoever wants to pick it up. The debate in the UK on Huawei has been around hardware, and clearly open RAN is the future. Can you give an indication of two things? First, what are the timescales for its development and deployment? Secondly, because we have got operators currently taking out Huawei kit and putting in Ericsson or Nokia kit, how do you incentivise those companies to take the open RAN approach in terms of developing a market for that product? Where are we at internationally on open RAN compared with other countries?

Pardeep Kohli: Let me start. You are right that until now it was all about hardware, because people were building proprietary hardware to supply radio products. When you do hardware-based solutions, the scale matters, because you need logistics, manufacturing capability and factories, and obviously Huawei, Ericsson and Nokia had a strong base and the logistics set up.

When you do open RAN, it is more software leaning on general-purpose hardware. Companies like us do not need manufacturing plants any more because we are only providing software, and we have the advantage that our software can run on a private cloud that an operator can build on, for example, standard Dell servers—there are plenty of them, and people can build those—or we can run it on a public cloud on Amazon or Google.

If you look at the scale that Google, Amazon and Azure have, Huawei is nowhere close to their scale. In that sense, the whole matter of Huawei's scale does not matter at all the moment you move a hardware problem to a software problem.

The same thing happens with logistics and people. For us, hardware-based solutions need people to carry the hardware around, bolt it and everything. For software, with the click of a button you can distribute it to 2,000 sites; you do not need people and logistics to drive hardware around. This is how with what we are doing—for example, we are working with Dish to build a nationwide network, and we will have 50,000 sites deployed in less than two years—not that many people are required to do all this, because the problem has moved from hardware to software.

We would like the Government and other people to understand that there is no way any company can beat Huawei with the presence it has in China alone if they take on the problem as a hardware problem. It must be converted into a software problem—that is the only way it can be solved.

On your question about how we convince operators, it is always on the point about proof. We are a 20-year-old company working with operators all over the world. We handle 60% of the world's operators' messaging. If you look at SMS, for example, we carry that traffic for all the operators in the UK, and voice calling. We already do more critical services: radio is important, of course, because of the connectivity, but operators are relying on us for the day-to-day services. Now we are working with them to prove that our software is as good or better than what they can get on from the incumbents. Of course, we are expecting them to participate in the journey and work with us so that we can prove to them that we are good. We have done that in all other layers of the software, so we feel that if somebody engages with us, within six to nine months we will prove to them that we are good and it works.

That is working; in terms of the whole idea that the technology does not exist, we have crossed that hurdle. Now it is more about, "Okay, does it work for this use case or that use case?", or, "In my network, I may have some proprietary stuff I have done with existing vendors, and I want you to do that as well." So it may take six to nine months, or even 12 months, to get there, but I think we are beyond the point where we need to prove that it works. We know it works.

Q43 Mr Jones: Which country in the world is at the forefront of open RAN deployment?

Pardeep Kohli: If you look at investments, because of Dish, the US is making the most investments; the Government have now surpassed \$1.9 billion on rip-and-replace to replace Huawei equipment, so that will create an ecosystem. In Japan, with Rakuten, they are building a whole nationwide network based on open RAN. We have seen Deutsche Telekom, for example, announce in Germany that it is building an ORAN town, so it will have a whole city that will have only ORAN components in a due timeframe. We have systems applied now in Sri Lanka, in India and in Malaysia. A lot of countries are looking at the economics: obviously, volume makes the numbers different, and with higher volume you will improve the economics further, but if you include the

opex cost as well to go along with the capex cost, there is no way to compare what you can get with this technology compared with the legacy one.

The Chair: I am just conscious of time; do any of the other witnesses have anything they want to add to what we have heard from Mr Kohli?

John Baker: I would just like to add that Vodafone has been very much in the lead with the development of open RAN solutions. We have been engaging with Vodafone for three and a half years in test labs and specifying the technology, and so on. The UK has been very much part of bringing this technology forward, as well as BT with the Telecom Infra Project labs.

Chris Jackson: Coming back to your question, I would not like to speculate as to how long it would take for open RAN to become standardised and commonplace within the UK. The Government are setting up a national telecoms lab and SONIC. There are a number of companies like ourselves, NEC, who have just set up our 5G global centre of excellence here in the UK, and the operators have all set up laboratories. If we can start to encourage and bring all those parties together, that is the key to accelerating the technology.

Incentives definitely play a part in this; to comment on Japan for a moment, I know the Japanese Government have incentivised companies to embrace open RAN, and that might well explain why companies such as Rakuten and NTT DOCOMO have been very successful in launching the technology. That proves it can be done and shows that where there is a willingness, there is a way, but if we can drive all those different parties coming together, that is how we will get traction.

Stefano Cantarelli: I just want to say quickly that we are part of some of the initiatives Chris has mentioned, such as SONIC with DCMS and so on, and we think they are particularly useful to give visibility on the status of open RAN. My last comment is about the hardware; I heard a few comments this morning, and I want to underline that hardware is still quite a profitable business. If we look at what happened to IT servers in the IT industry, there are companies that are much more than profitable in those spaces. Commoditisation of a hardware does not mean that there is no profitable business behind it.

The Chair: Thank you. I am going to Mr Sunderland. I will come back to you if you want to come back later.

Q44 James Sunderland: I note from the briefing notes that I have here just how much global experience Mavenir has, and that perhaps sets you gentlemen apart from the previous witnesses. Could I therefore ask you this, please? Is there anything, in your experience in this field—particularly, perhaps, in America and the far east—that may require to be better reflected in the legislation?

The Chair: Is this question for all the witnesses?

James Sunderland: Yes, please.

The Chair: Who do you want to go first?

James Sunderland: Mr Baker is the obvious candidate.

John Baker: I think the legislation, as you have it written, is good and supportive. The underlying thread of this is all about open interfaces. Having open interfaces fully specified makes the ability for testing of elements in the network simpler and easier, because you open up the testing community, the vendors, to produce interoperable equipment, so you can compare equipment side by side. This has been the basis of the whole open RAN discussion. Open RAN is about open and interoperable interfaces. If you follow that philosophy through into this Bill, you should be able to test each of the elements and the network end to end, from a security perspective, so we are fully supportive of the activities that you have in place.

The Chair: Anyone else?

Stefano Cantarelli: I will just add that of course, when we say “open interfaces” and “open and interoperable”, “open” means standardised and well known, not open in the sense of open sources or whatever else people can think of. As far as the Bill is concerned, I believe that it is quite appropriate for the specific actions and conditions that will be triggered. I would just suggest that you make sure that it is followed up by secondary legislation to make sure that in some cases there are very tangible and specific examples that will be able to make it a bit more specific and will give directions within the framework that the Bill itself provides.

The Chair: What about Mr Jackson or Mr Kohli? Do you have anything to add to that?

Pardeep Kohli: I was about to read something to you about the example offered by the Government of Japan. I am just reading the wording of the document. It says:

“The Government of Japan cites the need for equipment to be interoperable, based on open architecture, and utilize international standards to be certified. MNOs and private network owners are eligible for tax benefits, which include the following... Tax deductions of 15% or special depreciation of 30%... Fixed property tax exemption of 50% for 3 years”.

That is how the Government of Japan have passed the law.

Chris Jackson: I have nothing further to add to what Pardeep has just said. He has succinctly put basically what we need to do.

The Chair: Do we have any Catherine West questions in this round?

Chi Onwurah: Catherine is always interested to understand what international comparisons there are, but I think that that has already been addressed, so thank you; she will be grateful to you.

The Chair: In that case, let us go to Miriam Cates, please.

Q45 Miriam Cates: This is a question for Chris from NEC. I think that you have partially answered it already, so do not feel that you have to repeat what has already been said. It appears to me that, if the open RAN trial is successful and the open RAN technology is adopted, it has the potential to significantly disrupt the telecoms market in a way similar to how APIs have disrupted the software market. First, how do you think that it will change the shape of the industry over the medium to long term? And secondly, what experience and capabilities does NEC have that give you the confidence that you will be able to run this trial and it will be successful?

Chris Jackson: First of all, the answer is yes in terms of, “Do I think it is a game changer?” Absolutely. You only have to look at what happened in the IT industry to see what open standards have done for that, so I absolutely think it is the right thing to do and we very much support it.

In terms of NEC’s capability, if you look at the work that we have done with Rakuten and NTT DOCOMO in Japan, we have shown that we have proven experience and open RAN capabilities. We also have a long history of R&D capability, and we have the capability on the ground now, with the launch of the global open RAN centre of excellence, to take that development further forward in the UK. Those are the main reasons I think the NEC is well placed to take advantage.

A final point that I would make is that, one of the things that we are going to see, which we would want to see, is a lot of smaller companies coming into this marketplace. That is very healthy, and they would certainly play an important part in driving innovation. There is also definitely a need for large companies with strong balance sheets, and NEC certainly ticks that box.

Q46 The Chair: Do any of the rest of you have anything to add to that?

John Baker: Yes, I will jump in. Mavenir is heavily invested in the UK as well. We have addressed the 2G, 3G, 4G solution with the recent acquisition of ip.access in Cambridge. We are building up a significant open RAN solution centre in the UK and we have made several press announcements about that.

In terms of hardware versus software, we have demonstrated that with some of the networks that we have deployed, such as T-Mobile in the US, which has 150 million subscribers essentially running on disaggregated software and hardware platforms. That demonstrates that you can build secure, reliable mobile networks with a software architecture. That is the way of the future. Obviously, that now has to fit into the cycles of deployment and rip and replace that the various carriers have.

The Chair: Who is next? If there are no pressing answers, I will go to the shadow Minister.

Q47 Chi Onwurah: Thank you for joining us today. Having read your bios, I am impressed by the breadth, geographic as well as technical and operational, of your experience. To make this concrete for me and others, let us say we had a new mobile network operator in the UK tomorrow. Could you—I will ask someone to answer on behalf of Mavenir and someone on behalf of NEC—provide a 2G, 3G, 4G, 5G network tomorrow, or in 12 months? As a software network, what physical boxes or hardware would it be running on? As part of that, what UK or other providers would be in your supply chain?

Pardeep Kohli: Maybe I can take that. To answer your question, if there is a greenfield operator in the UK that is similar to Dish, which we are working with in the US, we can definitely provide that. Dish, for example, is doing only 5G, but we obviously look at requirements all over the world and we appreciate that, in certain parts of the world, there is still a lot of 2G and 3G presence, and, of course, 4G will be there for a long time. We have a solution that can handle 2G, 3G, 4G, 5G, and if you

are talking about a 12-month window, we can definitely provide a complete greenfield solution for those four technologies.

Regarding the hardware aspect, everything other than the real radio that goes on the tower and does the transmitting and receiving is largely general computing open silicon—

Chi Onwurah: Sorry—say that again. I could not hear that. What is the rest of it?

Pardeep Kohli: It is general-purpose open compute; it is already available hardware.

Chi Onwurah: It is computing—it is processors.

Pardeep Kohli: That is correct. You get processors for CPU or general-purpose computing, or even if there are some accelerators, which we use for some specific algorithms, even though they are openly available from companies like Xilinx and Nvidia. They make those chips and we can use them to do some of the functions; but they are openly available, and you can buy that today. That is what carriers are doing. They are building the new networks.

Regarding the hardware that goes on the tower, that depends on the frequency band you allocate, so if there is an operator coming in that is on a frequency band that the existing operators do not have, whoever the vendor is would have to build those radios anyway, and it takes about nine to 12 months to build those.

Q48 Chi Onwurah: Who builds the radios?

Pardeep Kohli: Today, because it has always been proprietary solutions, that is where the challenge comes for companies like us, because it is demand and supply. Until open RAN came in, you really could not build this channel on radio, because there was no demand for it. So today the radios get built only by companies like Huawei, Ericsson, Nokia—I know NEC is building a few of them; but now, with open RAN, there are new players coming up. NEC, for example, is building radios outside of the Japan market. Fujitsu has now started building radios. We are actually building some radios ourselves for the frequency bands that are not available from our partners, so if NEC has a radio we use the NEC radio, but if it does not have a radio and Fujitsu does not have a radio and if you want to get into that market, we start building some of those radios ourselves. So we actually have, now, opened a centre in the UK, to build some of those radios, and we are working with Facebook and together we are building some of the radios for a frequency band not currently open.

Q49 Chi Onwurah: So you couldn't provide a network tomorrow, but you could provide a network in how long—a 2, 3, 4 or 5G network?

Pardeep Kohli: So if the frequency band radios are available today, which are right, then we can actually build it in 12 months—the complete network; but if the bands are not available and we have to build those radios then, maybe, by the end of next year.

Q50 Chi Onwurah: And NEC?

Chris Jackson: Just to add to what Pardeep has been saying, I think open RAN is not about, necessarily, any one company providing an all-encompassing solution. So at the moment, for NEC, we would provide 4G and

5G radios, but in terms of 2G and 3G we will work with our partners to provide that solution, so we would leverage third parties in order to provide that all-encompassing solution. I think that is the way that open RAN will work moving forward. As I say, you will not see any one company dominating one particular area. It is about bringing best of breed together. In terms of the actual hardware platform, in terms of 4G and 5G, NEC will provide that radio, but as I mentioned for 2G and 3G we would look to other vendors to provide.

Q51 Chi Onwurah: And who are those other vendors? Are they UK, Europe or US-based?

Chris Jackson: The majority would be US-based now, but again, we are not restricted to that. As a systems integrator, which is what you will basically need, moving forward, we would work with whichever vendors were the best of breed for that particular scenario.

Q52 Chi Onwurah: You seem to be saying, then, that you are in a position to compete with Nokia and Ericsson as of today. Is that what you are saying?

Chris Jackson: We would not compete with Nokia and Ericsson in terms of standard RAN, but the whole idea is that we would look to bring open RAN technology. That is the direction that NEC is supporting. If you ask me whether we could step in today and provide that capability, we believe yes, we could.

Q53 Matt Warman: Again, I thank both NEC and Mavenir for the productive conversations that we have had already about getting involved in UK networks. Obviously, one of the things that was in the diversification strategy is the project with NEC—the NeutrORAN project that we have talked about a little bit today already; and I hope we could do, if possible, something similar in the future with Mavenir. What is striking about the NEC project—it is genuinely significant for UK networks—is that it is a £1.6 million initial jolt of funding. First, Chris—but I am very interested in Mavenir's perspective as well—will you say a little about how Government can best target the funding? One of the things that we learnt in our previous discussions with you was that this is not solely about the scale of the funding but about the targeting, the way in which we do it and how we get the best value for taxpayers. Chris, will you say a little about that, then we can hear from Mavenir about what the equivalent sort of things might be?

Chris Jackson: First of all, thank you very much indeed, Minister, for support in that particular trial. We believe that this is very important, because it has given us the opportunity to showcase 4G and 5G open RAN capability with multi vendors, and we are doing it in supporting the share of your network, which we know is an important KPI for the UK Government, in terms of increasing that capability across the UK. They want to ensure that the investment is targeted at areas within the UK—where the UK will receive the most benefit—and, more importantly, or as importantly, an opportunity for a trial that brings multiple companies together. So, although NEC is leading this particular trial, we are working with a number of other companies to bring this overall solution together. That is exactly what open RAN is trying to embrace, and that is the way forward. We would be delighted to work with Mavenir; we are already involved with Mavenir as well. That is not a hurdle or obstacle for us.

Stefano Cantarelli: There are several angles. The first one is the neutral hosting. I would like to draw attention to the fact that we have already done work with British Telecom, two years back, on neutral hosting, so that has now been talked about for a long time. Also, you might have noticed in the market that companies—the one that comes to mind is Vilicom—have been doing this type of thing, where they deploy Mavenir infrastructure to provide neutral hosting capabilities. So, we are fully supportive and believe that this kind of funding is particularly important.

We understand that that there is some interesting funding. We are in discussion with DCMS. We are discussing some projects that we believe will boost a lot of the innovation in this space. For example, we are trying to get funding for our R&D activities for open source software that could boost the availability of radio units. We say that the radio unit is hardware, but in reality there is of course a bit of software on top. This type of software, which is mainly interfaced towards the rest of the software and the control of the operation and maintenance activities, is not differentiated for each radio unit; it is just standard. By having an open source like that, you can fundamentally get the radio vendors to focus on their IPR for analogue development and being able to produce a radio unit with different frequencies, as Pardeep said before, which we believe could boost the market. That type of funding is particularly useful, because it is aimed at boosting the market and giving availability in the open RAN of these radio units.

I would also like to add that most of the frequencies that are used today in the UK are available in our view for open RAN, so I do not see that as a problem. But that type of investment is particularly important—in R&D—so the trial that you have funded in the first round of the 5G Create programmes is particularly useful to get learning and experience. As I said, in the SONIC, we are particularly active, although that is not a 5G Create programme but a different one. We believe that in the second round, you can focus on funding some R&D specifically to boost the ecosystem of the open RAN.

Q54 Matt Warman: Finally, would you agree that there are plenty of opportunities for us to use those trials and test beds to boost British companies, particularly in software, around open RAN? That is probably where British firms are likely to focus, at least in the first instance, rather than hardware.

Stefano Cantarelli: First, remember that, as John mentioned, we acquired ip.access, which is a British company that has been in hardware for some time, so there is still space for hardware as well. Software is definitely where the majority of the innovations are. That is particularly clear—Chris mentioned this—in the IT space, where they moved from generic servers. I want to reinstate that, with servers generically available everywhere. The whole thing has really flipped on to different software. That will definitely boost the ability of a lot of companies to bring innovation.

As we always repeat, competition means innovation, and innovation is the only way. Many years ago, I was part of Vodafone. I built the 3G network for Vodafone in the UK, and at that time I had only one supplier in my network—I will not say who. I introduced another one, and it was only then that the other suppliers started to be active. Some legacy suppliers—I would say most

of them—start to sit down and lie back if they are the only one in the network, because there is no motivation. From my experience from all these 30 years, that component is so important.

Matt Warman: Thank you.

Q55 Chi Onwurah: I wholeheartedly agree with that last comment about the importance of competition, particularly in the supply chain. That is my experience as well, in terms of building out networks. I am just struggling to understand why Vodafone, Three and O2 said earlier that there were only two full-service suppliers in the UK, when Mavenir is saying to me that you could supply a 2G, 3G, 4G or 5G network within a year. I am struggling to understand how that works. Is it a question of the network operators not being prepared to commission you? Is it an issue of price, complexity or management? Why are you not considered a full supplier by the existing network operators in the UK?

Stefano Cantarelli: Let me just address that initially before anyone else. We are a supplier in other places in the network, so they consider us a reliable supplier. We supply voice services, messaging services and everything else. You mentioned the initial deployment of open RAN by Vodafone this morning. That relates to us, because we are the supplier that it has deployed and is continuing to deploy. We are actually deploying sites for it.

I think that you have to look at two aspects when you are on an operator's side. I am speaking from experience. It is not just about the technology; it is also about your processes and how you are able to move forward and change your mindset. I think that operators have a lot of complexity. We sympathise with them, of course—it is not an easy environment—but there are a couple of mindsets that they need to over-pass, if you let me use that word.

First, the world is changing. It is not hardware and software together; it is software and hardware disaggregated, and that of course requires some different capabilities. It is the same as when we passed from circuit voice to packet voice. Some people here may not get the example completely, but it is just a different point of view. That does not mean that it is more complex or whatever; it is just a different point of view, and you need to change. We know that change is not an easy thing. That is the first aspect that we need to take into consideration.

The second aspect is that, despite the technology that is available, you still need to consider the in-life service that you need to swap over. You have to consider that you did some planning or design based on certain principles that were available before, and you need to rethink how you are going to do that. For example, most of the 5G deployed today just uses additional frequencies on the existing sites that they have deployed with 4G, 3G and 2G. This is not what I consider full 5G, with all the characteristics of low latencies and so on. You need to start to think about the densification of sites. The Government can help a lot—with policies, by helping to define new capabilities, and by allowing the operators to change their architecture by enabling them to get more sites, and get permits more easily to build new sites.

These sites will not be like sites today; on these sites, there will be lot of carriers, a lot of technologies, and a lot of frequencies. As Pardeep said, a site today is

probably just a radio unit that connects, through an internet connection—not necessarily just fibre—to a software data centre. These things are more important, and they are the reason why, although operators are in the middle of that transformation, it is taking a bit of time.

Q56 Chi Onwurah: That is very helpful. I think you said that a site would connect not with fibre, but with something else.

Stefano Cantarelli: Not only with fibre. The open RAN interface is such that you are not forced to use fibre only. You can also use internet connectivity. The internet is what you use when you are in a building.

Q57 Chi Onwurah: That is really helpful. What you are saying is that although you could deliver a full-service 2G, 3G, 4G or 5G network tomorrow, that is not what our mobile operators want. They want an incremental improvement from what they have to what they need to provide services. The cost is a real issue. The transition from 4G to 5G/open RAN is part of the challenge, and we need to understand better how the Government can support that. You talked about making it easier to roll out new open RAN sites. I am interested to know whether there are other ways in which the Government could support that.

Stefano Cantarelli: I add that this transformation in the core infrastructure has already almost happened. Already, most of the core infrastructure of the MNOs is running on general-purpose hardware, such as Dell servers and so on, with software on top of it. The RAN is really the last one to be transformed, for the reason that I gave, and also because, as I said, the market has been dominated by some suppliers who have been providing hardware and software, because they work with better interfaces between the radio access component.

Chi Onwurah: Thank you. That is very helpful. That makes me think that there are security issues arising from, for example, having our cloud infrastructure dominated by one vendor, such as Amazon Web Services. Those are perhaps future security issues that we need to look at. I now understand much better what you need to support your transition, so thank you very much for that.

Q58 The Chair: Do any of the witnesses have any final points that they want to make?

Pardeep Kohli: I would just add that I understand the operators' point of view as well. They are familiar with these vendors; they have been using them and they understand their processes. The vendors know each other. Obviously, we have to gain their trust. We spend over \$300 million on research and development every year on open RAN, so we are fully committed, and we will seek any help that you can provide on engaging with operators in the UK market.

Chris Jackson: Can I come in on the NEC side of things? Frankly speaking, we are re-entering this market, and one of the reasons why is because we believe that open RAN, and particularly the Bill, now provides the framework and conditions to enable us to compete. It is probably similar for the operators; it is a change for them to actively work with companies such as NEC, as opposed to the companies they have previously been working with, but we are starting that process. We are

actively engaged with the operators, and more support from the Government, through the Bill, is the way to move this forward.

John Baker: One last comment. Open RAN is all-inclusive, so this is not excluding the incumbents of the network. As soon as Nokia and Ericsson add open RAN interfaces to their products, we will be very happy to work with those guys. That will speed up the ability to deliver open RAN solutions in the marketplace.

The Chair: If there are no further questions, it remains for me to thank all our witnesses. We are extremely grateful to you.

3.26 pm

Sitting suspended.

Examination of Witnesses

Julius Robson and Dr Louise Bennett gave evidence.

3.30 pm

The Chair: We will now hear from Julius Robson, who is the chief strategy officer of the Small Cell Forum, and Dr Louise Bennett, who is the director of the Digital Policy Alliance, and we have until 4.15 pm for this session. May I ask the witnesses to introduce themselves for the record? Julius, could we start with you?

Julius Robson: I am Julius Robson, the chief strategy officer for the Small Cell Forum. We are a global organisation of component, equipment and service providers, all working to make mobile infrastructure more accessible to public and private sector organisations of all sizes. We see diversity as being really essential if we are to deliver on the promise of 5G connecting cities and communities, and to provide smart industry and the internet of things.

We welcome the publication at the same time of the Bill and the 5G diversification strategy; it is really important to consider both together, so that we can arrive at the best of both worlds. Two angles have not really been represented to the Committee so far, but are important to diversification. To fuel open RAN, we need chipsets for base stations. We also need to think about diversification at service provider level, so that in addition to mobile operators there are other service providers, particularly neutral hosts and private networks, which can help with this diversification agenda. Those are the topics of which I would like the Committee to be aware.

The Chair: Thank you. Dr Bennett?

Dr Bennett: I am Louise Bennett, and I have worked in computers all my career, with a focus on security and risk management. I am attending as a director of the Digital Policy Alliance. The DPA is an independent, not-for-profit membership organisation that alerts parliamentarians and policy makers to the potential impacts, implications and unintended consequences of policies associated with online and digital technologies. I am very grateful to have been asked to give evidence.

DPA is broadly supportive of the intentions of the Bill, because it baselines the security measures required by law in the UK telecoms network, and anything that encourages security to be top of mind for vendors in multiple supply chains is a very good idea.

There are four areas that are absolutely key to telecoms security and on which I hope to answer questions in this sitting. The first is the security of network architecture. The Bill really focuses on this, but in our opinion it does not cover everything adequately. The second is the security of data—both data about the network and data going across the network. The latter is covered to quite a large extent, but the former, which I would characterise as begin about the network asset database, is not adequately covered, and if it is not properly covered, I do not think that you will succeed in your intentions.

The third area is the processes for maintaining, over time, the security needed time—that is not adequately covered, either—and appropriate scrutiny of how that is done. The fourth area is operational costs and other impacts of compliance, which I do not think have been fully considered.

The Chair: Thank you very much. Okay, who wants to go first?

Dr Bennett: I am happy to go first.

The Chair: I think it is possibly better if I get one of the Members to put a question to you first. David.

Q59 David Johnston: That was a helpful teaser of what you think about this legislation. Could you expand on exactly why you have that view on what you see as the inadequacies?

The Chair: I think that is primarily to Dr Bennett.

Dr Bennett: It is because I care very much about you succeeding with this. I think everyone in the telecoms industry wants your intentions to be met, but we have to remember that when it comes to something as complex as security in the UK telecoms network, even if everyone follows best practice, it is a question of not if there will be a security breach, but when, and how quickly you can mitigate it. The reason is that our communications network has grown like Topsy. It has multiple digital infrastructures sitting on a lot of legacy systems, including analogue systems and copper. It is a very complex system of systems, with multiple, ill-defined interfaces and literally billions of end points, many of which have no security at all; the internet of things is an example.

The question is how you can minimise the likelihood of breaches. To do that in this very complex situation, you need a balance between light-touch regulation, which Ofcom seems to prefer, particularly with tier 3 suppliers, and the absolute need for security. Looking at our absolute need for security and the recent SolarWinds compromise, the inclusion of SolarWinds Orion products in networks was considered by everyone to be perfectly sensible. It was a trusted supplier. However, the latest things that I have seen say that thousands of networks have been compromised by that. As it seems to have been a spying attack, only about 10 networks are known to have been breached, but it will take months for all of those networks to be secured, and there are other potential breaches. The NCSC recently put out a note about that to all end users.

That is typical of the kind of things we will face. If we want an infrastructure that can cope with that, we need to do a lot of things. There needs to be a very honest

and open dialogue between all the telecoms suppliers, their supply chains, their subcontractors, the Government, Ofcom and other agencies.

Q60 The Chair: I will interrupt you there for a second, but I will come back to you. Mr Robson, do you have anything you want to add?

Julius Robson: Security is about resilience, and it is not a question of whether something will go wrong; it is a question of when. When we realise that one of our vendors is high-risk, will it take seven years to fix that problem? That is not a healthy place for our industry to be in. We want a rich diversity of suppliers working together, so that when we identify a suspect component or part in our network, there is something sitting there, warmed up and already integrated, ready to be swapped over. That is where we want to get to.

Dr Louise Bennett pointed out that there are many parts to this network; it has lots of legacy pieces. It is not a bad thing that our network is comprised of many diverse parts—that makes it less vulnerable to a single point of failure. Someone pointed out earlier that there is the idea of the weakest link—something is only as good as its weakest link—but actually, a diverse system with many different types of vendors involved is harder to take down. Maybe you can take down part of that network, but the whole thing will not fail if just one part is compromised. I think diversity is the answer to resilience in this case, and we should be looking to head in that direction.

Q61 David Johnston: Just to be clear, is your critique of this legislation that you feel that something is missing from it? Or, given that you think breaches are a case of “when” rather than “if”, which I am happy to accept, is your critique that no one piece of legislation could totally protect us from this, and that it is about what the whole sector is doing to keep us secure?

Dr Bennett: It is partly to do with what the whole sector is doing, but I think some things have not had enough emphasis in the Bill. One of them is what I have called the asset database. Those of us who were involved with the millennium bug know that we spent a hell of a lot of time trying to understand what the asset database for all our networks was, in order to find the components that were likely to cause a problem. I assume that the tier 1 suppliers and our main network suppliers have a comprehensive asset database, but you actually need a well-secured asset database that goes down to the component level. Over time, as you maintain it and move some components out and other components in, you need to be clear about what has happened to them.

At a subcontractor level, that can often be extremely difficult to do. You can find someone who thinks, “Oh, it’s okay; I’ve replaced that with something, and the spec looks similar.” The spec may look similar, but when someone says, “Actually, it is version so and so of such and such a component from such and such a supplier that you now need to take out,” you will find that you do not know in your asset database that you have some of those components in it. I could not see anything in the Bill that talks about the asset databases of the companies that supply the networks we are using, and I think that omission needs to be dealt with.

That leads to another point, which is about the processes for maintaining security over time. You may now be taking out all the Huawei kit and putting other

things in its place, but that is happening all the time—that maintenance is going on all the time. There is no mention in the Bill of a technical advisory board focused on the provisions of the Bill, and that would be a very helpful addition. The board would perhaps be able to point out that there were new types of components coming in that ought to be looked at or considered and that ought to be recorded in people's asset databases, and people should make sure that happens.

Leading on from that, I also think that the processes are not as transparent as they ought to be for Parliament. It would be helpful if there was a commissioner, such as the Information Commissioner or the Investigatory Powers Commissioner. That would be helpful in keeping an eye on what is going on here, and in order to be able to help policy makers and the Secretary of State to make the right changes.

The Chair: I am just going to interrupt you there, because I am conscious of time and a couple of Members are indicating that they want to come in. I call Christian Matheson.

Q62 Christian Matheson: Thank you, Mr McCabe. I want to follow on directly from the answer that was given to Mr Johnston. This morning, I asked some of the larger mobile firms whether they had done a proper audit, they had an asset register and, when the orders came through from the Government, they knew exactly what to take out and where it was. Those were the largest mobile firms. They all expressed confidence that they did. Dr Bennett, are you suggesting that at that top level we should be querying that confidence a little bit? Perhaps you are suggesting that that confidence should not be taken as read, as we flow down through the rest of the sector from the top level.

Dr Bennett: I would hope that those at the top level are clear about it, but I would be surprised if there were not occasions when they had used subcontractors to do maintenance and the imperative had been to sort out the fault ASAP. Knowing precisely what components had gone in could be wrong, and that might come up in an audit. I think it becomes more important as you flow down the levels.

When there is this desire, quite rightly, to bring in new and additional suppliers, those suppliers will need help to ensure that their parts of the network are working well. Again, I would suggest that something that is not in the Bill but should be there is the type of sandpit that the City of London has done for FinTech companies, where new entrants can test their equipment against the type of networks that they will be interacting with. That would reduce the risks of security problems in that area and give everyone confidence that the lower tier suppliers are compatible and have the same level of security as the top level of suppliers.

Q63 Christian Matheson: Should there be some form of external audit of asset registers?

Dr Bennett: Yes.

Q64 Christian Matheson: And who should do that external auditing?

Dr Bennett: This is the type of thing that would be done by a commissioner. I think NCSC is well placed to be involved in that and things like sandpits. I am not sure whether Ofcom has all the resources it would need

to be able to do that. But we also must remember that audits and responses to audits are quite expensive things. If we want the infrastructure to be secure over time, as we all do, we have to agree that that is an expense that we will have. That will make the whole system more expensive to maintain, because it is an important job.

The Chair: Thank you. Mr Robson, do you want to add anything to that?

Julius Robson: I think it is very important. One of our angles on this security Bill is that we see diversity as important not just for building resilience, but for delivering on the promise of 5G, which is to take mobile—which currently is about voice and data for people—and deliver it into organisations, to have e-health, smart industry and connected communities. To do that, you need a diversity in service providers. It is fair to say that mobile operators have done a great job of the outdoor national network, but perhaps not so much delivering into enterprise.

We want to ensure that when we implement new policies, like the telecoms security Bill, we are not introducing large barriers to entry to those smaller players that will come in and diversify our network. This talk of making everyone auditable is a workload that will drive us back towards a monolithic industry, where you have a small number of service providers, and only the largest vendors are able to service that. We need to ensure that whatever policy we implement looks forward and is workable for this diverse ecosystem that we aim for in 2025 and beyond, not the monolithic one we have today.

Q65 James Sunderland: Dr Bennett and Mr Robson, thank you for coming in. I have listened intently to what you have said, and it is fascinating. May I offer an alternative view? First, the Bill itself creates new powers for the Secretary of State to make regulations. Section 105A is a duty to take proportionate measures, to identify and reduce risks. Section 105B is a power to make regulations imposing duties. Section 105C is a duty to take appropriate and proportionate measures in response to compromises. Section 105D provides for powers to respond to a compromise itself. The Bill is all about giving the Secretary of State powers to do things; it is not a panacea. So may I ask you to comment on two things? First, what you have referred to this afternoon is valid, but it will be covered in secondary legislation or in powers taken by the Secretary of State after the primary legislation has gone through. Secondly, the Bill should be seen for the framework that it is, and not as a panacea, which it is not.

The Chair: Who wants to go first? Dr Bennett, I think that was mostly directed at you.

Dr Bennett: I appreciate that it is a framework, but it is a framework that does not say that powers in certain areas are going to happen and how you might do it. I think the Secretary of State and the whole industry actually needs a lot of help to do this. The whole tenor of wanting to have things like the telecoms diversification taskforce and the 5G diversification strategy is absolutely right, but as you do that you are bringing in people to do these things who have less resources than the people currently in there. As Mr Robson said, they can afford the expense of the barriers to entry, whereas smaller players require assistance from the Government to enter this world without going out of business because of the impacts of the cost of compliance.

Q66 The Chair: Mr Robson, what is your take on Mr Sunderland's alternate view that this is a framework and it will be all right in the end?

Julius Robson: It is a good point. I recognise that the Bill essentially describes a process of setting codes of practice and does not actually say what those codes of practice are. One thing I noticed is that the language of the Bill speaks very much to the problem we have today that there are only one or two viable vendors of networks. The open RAN movement is about ensuring that your network is comprised of parts from many different vendors, with hardware from some people and software from others, and a mix of providers doing similar things. The Bill must ensure that it represents that world. So where it talks of "public electronic communications network" providers, do we assume that you have to be a network provider—an end-to-end network—to play in this game.

I did read that the code of practice will define three tiers of telecom providers, with the biggest and most important providers subject to the most intense scrutiny and oversight. That is not expressed in the Bill—it is in the notes—so I assume it will come out in the codes of practice, but at the moment we do not have visibility of what that will look like. From our point of view, it is important to encourage companies of all sizes to be able to play in this game, so proportionate legislation is important.

The Chair: Do you want to come back, Mr Sunderland?

James Sunderland: No. Thank you for the answers.

Q67 Chi Onwurah: I am the shadow Minister for the Bill. Let me start by welcoming you and thanking you very much for your expert input. I particularly welcome you, Dr Bennett, for your expertise and the fact that you are the only female witness we have today—it is clear to me, as someone who worked in engineering for 20 years, that the sector's gender balance has not improved. I hope that Parliament can do more to ensure more balance in witnesses in future.

I have questions for both of you, but let me start with Dr Bennett. I was impressed by your structured list of things that are missing from the Bill, because we are here to scrutinise the Bill and see how we can improve it. I think you talked about the breadth of the security challenge and how this Bill, as it stands, might not meet the full breadth of it. You had four areas, and I think you have run through two of them in more detail. Could I ask you to summarise again the areas that you think are missing? In particular, could you talk a little bit more about the need for improved scrutiny? Could you just summarise that and then go into more detail on the ones where you have not yet?

Dr Bennett: I said that the areas that needed to be covered were network architecture, which is the Bill's focus, the security of the asset databases that make up the network, how to ensure security of the data passing over the network, the maintenance of security over time, and the operational costs and other impacts of compliance. I have touched on all of them, but perhaps not very much on the operational costs and impacts of compliance.

The more diversified your network, and the more small vendors there are, the harder it will be for them to maintain the level of scrutiny, record-keeping and general

security that is required as their bits of the network develop and the interfaces they have with other bits of the network change over time. That is an area where the Government should consider giving help to people to cover those costs. I have said that audit is needed of the assets in the network. The costs of being audited and of dealing with audits are very high, and they are costs that small companies may not have the resources to meet.

If the Government suddenly say, "All components from supplier X must now be removed from the network because of x, y and z," it is incumbent on the Government to have some funding to help people to do that and to ensure that that really does happen, because it could be a step too far if you have a lot of very small suppliers that do not have the resources of skills, time or money to do it. You need to think about that and about how you can ensure that they are not squeezed out of the network—this diverse network that we want—by those costs.

Q68 Chi Onwurah: To follow up briefly on that, I think what you are saying is that there might be a contradiction between the desire to have a more diverse supply chain, with more smaller players, and increased regulatory and other costs in this. With regard to network architecture and data flows, you make a very good point: we have been concerned about high-risk vendors, designated vendors and so on, but that will not address the issue of securing data flows. Do you have any thoughts, and are you suggesting that more thought needs to be put into that aspect of network security?

Dr Bennett: I think most people would agree that the diversity of end points, of interfaces and of applications running over complex networks all pose security problem areas. The more of those you have, the more resilient your network might be on the one hand, because there are multiple parts, but on the other hand, the harder it is to maintain them adequately.

We see some of these problems today in the decision to move the copper out of the network. Applications that are very important to many users, notably alarm signals, are ones that often assume they have an underlying network of a particular type, and if it is not there those applications do not work and they do not work suddenly. These types of things are very complicated but are actually very important for the end users. It may be an alarm that says an elderly person has fallen in their home; it may be an alarm that says your bank has been attacked by a criminal gang. Who knows what it may be? But those types of things are the types of applications that run over these very complex networks, and unintended consequences can happen as you change the network architecture. If those tier 3 suppliers and the people providing key applications over the network are not involved in this conversation at the CNI level with the top-level suppliers, all sorts of unintended things can happen.

It is a question of how you make sure that you minimise the number of these unintended consequences and support people to realise what they need to do early on, so that they are not caught out by them.

Chi Onwurah: A very good point.

Q69 The Chair: I just want to check if Mr Robson has got anything he wants to add at this stage.

Julius Robson: We are discussing the use of the mobile network for new and innovative services, such as worker alarms or falling-over alarms. Actually, there are some smaller players working in specialised industries that understand those customer requirements probably better than mobile operators, and that are very used to dealing with them. In fact, many of the applications for mobile are those that already exist in proprietary and bespoke wireless systems today and that we would want to move on to mobile. Some of the newcomers probably understand these things better than others and the diversification policy is about bringing in that expertise—those industry specialists who understand these requirements.

I would also say that, yes, the network is complicated—radio wireless networks, with lots of endpoints—but intrinsically the wireless medium is insecure. Anyone can listen in to it; it is possible to modify the signal. It has been designed so that everything going over it is secure and protected, and those security paradigms are locked up in the core, so that there are parts of the network that you do not have to worry about, because the information has been secured at a higher level.

I think this was mentioned by Andrea from Vodafone this morning: it is really important for us to understand which parts of the network are in scope of the security rules and which bits we do not need to worry about. The air—anything in the airwaves—is intrinsically already easy to eavesdrop on or modify. So obviously that is out of scope. I think we do not have to get too worried about certain parts of the network.

The Chair: I am just going to go to the Minister; if there is time, I will come back. Minister.

Q70 Matt Warman: Thank you both for what has been a really interesting discussion. I wanted to ask, partly because you mentioned it specifically: when it comes to looking at other parts of the network, such as the internet of things, are you aware of the work that we have been doing—for instance, in October we published work specifically on regulating smart devices—and do you see that sort of work as being complementary to the kind of work that we are talking about here today in relation to the Bill? Perhaps once you have dealt with that, we can deal with the Bill itself.

Julius Robson: I think it is important. What we are looking at in the 5G era is the application of mobile technologies for specialist industries, and it is entirely relevant that those industries have their own requirements for security and other requirements that apply on top of what is necessary in the basic mobile network. I do not think we need to duplicate that effort. Where we are using mobile in certain scenarios, the scenario should define the requirements. The base level of mobile connectivity should be something suitable, and affordable, for the consumers and the masses.

Dr Bennett: I am aware of the work you have been doing on security for the internet of things. I think it is complementary and extremely important. Everything should have security by design in it. It is very important to cover these types of points.

Q71 Matt Warman: In saying that, it seems to me that it supports the point of view expressed earlier, that this piece of legislation should not be expected to do everything. It is part of a broader Government response. You laid out a lot about what you think a secure network looks like and what its characteristics might be.

They are not controversial in themselves. The point of debate seems simply to be whether those are for a regulator to define and be able to update on a regular basis, because we need to be able to respond, or whether they should be on the face of the Bill.

I would have expected you to say, if I can put words in your mouth, that you would like the agility of the regulator's ability to update those codes of practice, to be able to say to networks, "This is what secure looks like. If you are complying with these kinds of codes of practice, then we will be able to understand that you are meeting the requirement." You seem to actually be saying that you want greater rigidity. I am interested to understand whether you would like the codes of practice to have the flexibility offered by the writing from the regulator or whether you would like to see them on the face of the Bill.

Dr Bennett: I think we actually want both. There should be mention in the Bill of some of the ones that I think are key, so that people realise that there is going to be a code of practice on that they should follow. It is very important to be able to be agile and to get early information, from something like a technology reference panel, about things that are coming along, in order that you think about them before they get attached to the network. Trying to do it after you have attached something to the network is frankly a nightmare, so you need to be anticipating. It is not clear that there are mechanisms for that anticipation in the Bill.

Given the SolarWinds Orion hacking, which is a recent example of something that will take a long time to sort out and is precisely what you do not want to happen in the future, it would be sensible to get someone like NCSC to test whether the things in the Bill, and things that should be in the Bill, would have enabled the mitigation of that problem to happen faster than it has. The Bill ought to be doing something like what the Americans are doing in response to that now. The Government should consider a rapid response, co-ordinated unit to deal with similar incidents in the future, because they will happen. That is the kind of thing that ought to be in the Bill to say, "This is how we are going to be able to mitigate these problems when they happen, as quickly and sensibly as possible."

Q72 Matt Warman: I suppose, in a sense, you are already seeing some of that, are you not, with us already publishing the draft designations, the draft directions and some of the secondary legislation that would be enabled by this Bill? I think you are arguing for as much transparency as possible, of the sort that you have already seen from the extensive NCSC blogs on what the standards might look like. I do struggle to see how you would put that on to a statutory footing in the way that you have described without constraining some of the agility. Fundamentally, however, your argument seems to be in favour of transparency above all else.

Dr Bennett: Yes, and anticipating things as early as possible.

The Chair: Chi, we have time for another quick question. I think you had a point that you wanted to come back to.

Q73 Chi Onwurah: I did have a question. I also wanted to say that I think Dr Bennett's point is about transparency, but also about anticipation, responsiveness and a fast response regime. My question is to Mr Robson.

You are the Small Cell Forum and you have put a big emphasis on diversity in the supply chain. I think you said—I do not want to put words in your mouth—that security requires diversity in the supply chain. You represent potential small providers. Is there anything that the diversification strategy needs to do that it does not do to better support the entry of smaller players?

Julius Robson: Thank you for that question. I have mentioned chipsets, which are important, and lots of people have talked about software and open RAN. The specialist base station chipsets are an important component, and if we can make them available at scale, which is something that we work on with our FAPI—our functional application programming interface—I think that will really help to fuel the diversity of equipment providers. That is one aspect.

Another aspect—I am not sure how well it is coped with in the consideration of the supply chain—is diversification at service provider level. As I have mentioned, mobile operators are the main service providers for mobile services, but they partner with other providers, particularly ones that work in specialist environments. There is a particular type called neutral hosts that can offer multi-operator services. If you wanted to connect to a hospital, it would not be any good to have just one operator service and have only a quarter of the people served. You need all of them served, and that needs to be done affordably. We want to make sure that the partners of mobile operators, such as neutral hosts, are supported in legislation.

It is also about recognising, as has been mentioned, the challenges of getting the hardware out. You can scale software just by selling it to more people, but hardware needs more feet on the streets and more deployers. We have to look at how we go about enabling more people to deploy mobile infrastructure into communities and industry, so that more people are aware of how it works, which means making the system simpler. From a security perspective, we need to recognise that there are parts of the network that need to be kept secure, and there are parts of the network that are out of scope of that.

Q74 Chi Onwurah: I would be interested to hear more about what is out of scope, because my understanding was that the Bill covered all aspects of telecoms security.

Julius Robson: Just to make the point that you do not have to worry about every last resistor—components were mentioned—and every piece of equipment you have. As I pointed out, the radio airwaves themselves are also not secure. The whole system is designed to securely operate over an untrusted environment. In standards, we have the concepts of trusted and untrusted networks. Typically, you can operate your mobile network over the internet, which is considered untrusted. It is important that we recognise that paradigm.

I would say that all service providers are well accustomed to working with the level of security that the mobile operators and the regulatory regime demand, so we are happy with that. I just hope that we do not introduce new burdens with this legislation that stand in a way of diversification.

The Chair: Looking around the room, I think that is it. In that case, I thank Dr Bennett and Mr Robson for their evidence. We are extremely grateful to you. Thank you both very much indeed. That brings this session to a close.

Examination of Witnesses

Dr Scott Steedman and Charles Parton gave evidence.

4.14 pm

The Chair: We now move to the sixth and final panel of the day, which consists of Dr Scott Steedman CBE, who is the director of standards for the British Standards Institution, and Charles Parton from the Royal United Services Institute. We have until 4.45 pm for this session. Again, I ask the witnesses to introduce themselves for the record. May we start with Dr Steedman, please?

Dr Steedman: Good afternoon, everyone, and thank you for the opportunity to attend the Committee this afternoon. My name is Scott Steedman. I am director-general of standards at BSI, the British Standards Institution. In my role, I have primary responsibility for the activities of the National Standards Body, which provides the UK experts—industry, Government and consumer experts—to participate in the development and maintenance of standards at the national, regional and global level.

The Chair: Thank you. Mr Parton?

Charles Parton: Good afternoon. My name is Charlie Parton. I used to work as a diplomat, for 37 years, and the vast majority of that was working on China. Since I left diplomacy in 2017, I have continued to work on China. My “Mastermind” special subject, I suppose, is the Chinese Communist party and domestic politics, but of late, in the past couple of years, I have also been looking at strategy—UK relations with China—and, in that context, the question of Huawei and how we deal with technology and divergence.

The Chair: Thank you both, gentlemen. Let us start.

Q75 Dean Russell: Many years ago, I used to work in communications and did some work with Huawei as a client. I remember, 10 or 11 years ago, someone told me that about 80% of all electronic communications go through some form of Huawei technology across Europe. I do not know how true that was, or whether it was inflated, but I am interested to understand from your perspective, given the impact of the Bill, how you see what it proposes compared with what is being done in other countries, in particular looking at comparable countries such as our Five Eyes partners.

Charles Parton: I think you are absolutely right to focus on our Five Eyes allies, in particular America and Australia—Canada and New Zealand at the moment are a little bit undeclared—which have come out very forthrightly to say that we really should not be entertaining Huawei in our systems. We have now followed them—even if only by 2027—and I think that is very much the right decision for a number of reasons, which I could go into if you wish me to.

I am not a technologist, and look at it much more from the political angle. It seems to me, if I may say briefly on the technology and the 5G system that is going to last us for the best part of 25 years and on which, no doubt, 6G will be built, that the idea that we can stay ahead in technology and be absolutely certain for the next two or three decades that we are ahead of the game and can keep them out of manipulating our data or using it in some advantageous fashion, is one of very great trust in our own abilities—first, they are putting enormous resources into it.

There are other reasons why the decision to get rid of Huawei was correct, and one is what I call the “black vulture of policy”. We have seen the way in which China will bully and sit on those countries that go against its wishes, in whatever field—way outside telecom. If you are dependent on another country’s systems, whether for getting equipment on time, or upgrades—let alone the more devious aspects of possible interference—I think that you will be looking at that black vulture and thinking, “Is it safe to pursue a policy that is very much in my interests, on telecoms, if I am going to be hit hard in other areas?” We have seen that: Australia, at the moment, is under the cosh; the UK was under the cosh when the Dalai Lama visited in 2012; Norway has been under the cosh, and so on.

In that context, are we saying that Huawei rules the Chinese Communist party’s policies? Of course not, but they are very intimately linked. I think that if the Chinese Communist party says to Huawei, “Jump!”, the only response from Huawei is, “Yes, sir! In what direction and how high?” You might look at the national security laws and say that those of course oblige them to co-operate and all that, but I do not think that matters so much—if the Communist party says, “Do it!”, they have no choice. If you look at how close they are, as another illustration, look at what is happening in Canada with the two hostages and the chief financial officer, Meng Wanzhou. Again, I could go into more detail if you want.

Also, there is the financial support that Huawei has received over the years, in terms of cheap finance, loans to customers, tax rebates and so on. Why does it do that? Because the Communist party wants to dominate the technology of the future, and Huawei is its tool for doing that. So I think that to trust Huawei in the long term would be a very unwise decision.

Dr Steedman: Can I take us back to the Bill and talk in that context? We are in a period of very rapid technological development and evolution. Many countries, including the Five Eyes countries, have allowed the market to drive this forward and not perhaps paid attention to it. While this was a hardware-driven sort of infrastructure, that was possibly manageable, and we have managed it over the last few years fairly satisfactorily. But looking ahead to the 5G and, perhaps—who knows?—the 6G world, we have moved to a much more vulnerable position away from hardware and towards software.

I welcome this Bill because I think it is incumbent on countries that want to protect themselves with secure and resilient infrastructure, and because it puts in place a structure of regulation, guidance and standards, which I represent, that will enable a transformation in the industry of the United Kingdom. It will enable us to use technology and software from providers all over the world, but also from SMEs and start-ups in the UK that we can encourage, and create a really innovation-friendly future. But to do that we have to create a market framework that is structured under a quality piece of regulation that enables that to take place in a clear way—clear for the market, clear for the regulator Ofcom, and clear for the Department that manages it on behalf of the Government.

In this Bill we see clear statements about new duties, codes of practice and guidance—another form of standard—to be approved by a Secretary of State for the industry, and also indications about the use of industry standards to support and deliver a new policy. We can really play

to our strength in the UK, where we work in a very performance-based market structure, and we can enable a pro-innovation culture that will stimulate and deliver the diversification, security and resilience that we are looking for.

It is not unusual in the world that major commercial players, given free rein, try to influence things in the direction that suits them best. It is not unusual. We are talking about China specifically, but it is not unusual. The key to this is ensuring that in the standards landscape, which is used to support the delivery of regulatory bodies, the governance and processes of the development of those standards is managed and influenced with UK stakeholder interest at heart. In the big landscape of standards, which we might want to talk about further, there is a very wide range of organisations developing standards, from the fringes to the formal systems, and we can discuss and deploy that in a coherent and consistent way.

There is evidence from other Departments of how this works in a co-regulatory manner, supporting industry, Government, Departments and the regulator to deliver the outcomes that we as a nation desperately want.

Q76 Christian Matheson: First to Mr Parton, we talk about Huawei, but is it the case that it is not Huawei but the Chinese state or the Chinese Communist party trading as Huawei? All the focus is on Huawei at the moment, but are there any similar companies, or front companies, that the Bill might have to cover in future? Bearing in mind the view that the Bill can help with diversification among trusted partners in the UK, how did Huawei get into such a dominant position globally? What can we do, perhaps in legislative terms within the framework of this Bill, to avoid that in the future?

Charles Parton: Of course, Huawei got the headlines because of the urgent need for 5G, but you are absolutely right that it is not the only player in telecoms, and indeed telecoms is not the only subject. I think that we need to look much more seriously at the whole question of technological co-operation with China. This gets into the whole question of divergence, or decoupling if you are American.

We have to recognise that, whereas our aim in China relations is to maximise trade, investment, global goods and so on, there are increasingly limits because divergence is happening. The intention of the Chinese Communist party is to dominate. As Xi Jinping in fact said in his first speech to the Politburo, the intention is to dominate western capitalism. He said that the Chinese system will take the superior position. Clearly, technology and its advance is a very important way of doing that, so it is not just Huawei and 5G. Therefore, we have to look very carefully at the whole question—that, I suppose, is what lies behind the National Security and Investment Bill—of how we co-operate on technology with China.

I have called for this a number of times, as many others have. The Government will need to set up a body and give much clearer guidance on which subjects in this field of technology we can co-operate happily with China, as well as which organisations—many are connected with the military, and the distinction between civil and military technology is eroding—and which individuals, because there are a number of individuals who have taken back or collected technology to help the Chinese security apparatus develop it.

You are absolutely right that it is really important to look much more broadly than Huawei. The company that comes immediately to mind is Hikvision, because it has such a large amount of the CCTV market. Secretary of State Dominic Raab made an interesting point in his speech the other day about the reputational harm that could be done to some of our companies if they are co-operating with Chinese companies that are deeply involved in the surveillance state, of which of course Huawei and Hikvision are two. Huawei has three laboratories with the public security bureau in Xinjiang, and is devising for them technology that will enable them to pick out Uyghur faces in crowds. That is on that side.

I think your second question was, why has Huawei been successful?

Q77 Christian Matheson: How did they manage that dominant position, and what lessons are there to be learned from that, either in stopping other companies from getting that dominant position or in helping us to diversify?

Charles Parton: I think the Chinese state very strongly supported Huawei through its financing provisions and tax breaks, and indeed worldwide by giving cheap tied loans to countries and companies that would use its equipment. Of course, Huawei has been very successful because it is enabled thereby to provide very cheap goods, and it works extremely hard and quickly. I have to say also that there have been times when we have helped it. I am not a great supporter of the Huawei security cell that checks it. I think Huawei must be delighted with that, because some of the best brains in Britain are paid to pick out the holes in its shoddy system. It does not necessarily have to do the work and it can plough ahead with speed, in the knowledge that the Brits will very kindly point out where its systems are deficient and demand that it fills them. It is a great model, and we need to think a bit more carefully about that in future.

Dr Steedman: Technology companies that secure major positions in the market, wherever they come from, do so either because the market is not being monitored or regulated carefully enough, or because they win the contracts. You would need to ask market experts about why Huawei achieved the position that it did.

Perhaps I could focus on the diversification question and looking to the future. There are very effective ways and means to manage the market structures in our country, and they require a combination of regulation, guidance and standards. You can do that through procurement routes on both the technical side and the supply chain side, and you can do it through the contractual routes. Although we have a very successful and professional regulator in Ofcom—its role is to police the regulatory environment—we can also encourage, through the supply chain channels, the use of standards on specific technical requirements and on specific contractual requirements which encourage better business behaviour.

The Government in the UK use a small proportion of the British standards catalogue—perhaps 10% or 15% of the 37,000 standards that I am responsible for—in support of regulation. This is the area where co-operation can take place in a very effective way between UK experts, industry experts, consumer experts, regulators, academics and other countries of our choosing. Indeed, in the international domain, I have 1,200 committees. The UK chairs, hosts and manages 200 international

committees, and a lot of the action, in terms of co-operation outside individual companies and universities working in their laboratories, takes place in the international standards system. It is in this system that we can seek to increase UK participation, co-ordination and influence, in order to get the results that we want. We want to ensure that the standards used are open and interoperable, that their governance is managed in an independent and neutral way, and that British stakeholders have the opportunity to influence the content of those standards.

The key to international co-operation is managing and influencing the international standards through which technologies, software and business processes are all delivered around the world. That is the plug-and-play global economy—trade, innovation and so on. It is an enabler; it is not a level playing field. The Telecommunications (Security) Bill will provide the level playing field for parties in the UK, and standards provide the opportunity. I would encourage us to see beyond the Bill's provisions on rules, guides and guidance and to see the role of standards as a tool for us to help stimulate the diversification, security, resilience and quality that we are looking for in a future market environment in the UK. That is an area where the diversification taskforce under Lord Livingston, which I am privileged to be a member of, has been working very hard. We have some ideas emerging from that taskforce to support the 5G strategy, which I hope in the medium term will see British influence in international co-operation on standards really ramped out. We look forward to that.

The Chair: I think I might interrupt you there, because we have only until 4.45 pm. I would really like to bring in Mr Sunderland, the Minister and the shadow Minister, so we need very tight questions and very succinct answers.

Q78 James Sunderland: Gentlemen, I have been a massive fan of RUSI for many years, and clearly I am a recent convert to the British Standards Institute, so thank you for coming in. I have two quick questions, which should be quite straightforward.

The Chair: One quick question, I think. Seriously.

James Sunderland: The important question from me is: what will be the reaction to the Bill within the Five Eyes community?

Dr Steedman: I will lead on that. I think the Five Eyes community will welcome the Bill, and it may well begin to set a model for the way that the UK and like-minded nations can create a pro-innovation market framework which has sufficient regulatory powers, backed up by industry standards, to deliver the environment that we want and that will, particularly in the UK's case, stimulate new entrants, SMEs and innovation. That is a really critical part of future diversification, because we have no incumbent major players based out of the UK, so we need to stimulate our own industry as well.

Charles Parton: I do not have a great deal to add to that, other than, as a side note, that I do not think we should underestimate American bipartisan attitudes to the whole question of China and technology. I think we are going to have to take that into account in the broader context, because they are long-standing allies and sharers of the same values as us.

The Chair: Thank you. I see Dr Steedman nodding assent.

Q79 Chi Onwurah: Can I just say that I had been a fan of the British Standards Institute for decades and am a more recent convert to RUSI?

I start with a question to Mr Parton on behalf of Catherine West, which relates to the last point you made. As we know, the Government were moved to ban Huawei entirely from the network following US sanctions instigated by President Trump. What changes do you see the Biden Administration having on the US's outlook on China, if any? Can you also squeeze in a reference to Chinese influence on academic research and development in this country? Then I have another question for Dr Steedman, which I will ask afterwards, if I may.

Charles Parton: A very quick response to that. I am more an expert on China than America, but nothing in the last couple of years has suggested to me that the Democrats will take a very much different position from the Republicans on the question of technology. I think they see it as a very great threat, as the Chinese have said. I think nothing will change there.

On the question of academic influence, I really do not think we should underestimate that. I wrote a paper on it about two years ago and much of what I sketched out there exists. For that reason, if I may repeat the point I made earlier, a great deal of effort has to be made, particularly in the STEM subjects. We could talk about the arts subjects and the clampdown, or the influences, on the freedom of speech and the self-censorship there, but in the STEM subjects it is really very urgent that we give our universities good guidance on what subjects, what organisations and what people they can co-operate with in the China context. As some of the research has shown, in terms of what is going on in our universities, there are subjects that we perhaps should not be helping on. GAIT technology with Huawei is an example. What can GAIT technology be used for? Surveillance. Not always, but it is very important in surveillance when you cannot see someone's face because they are wearing a mask or it is bad weather. We have to be very much more on the ball in that area.

Chi Onwurah: As I said, I am a massive fan of standards development. I have worked in the area, with the ITU. I agree that it is essential to enable open RAN and diversification. The Government have said that standards are driven by vendors. We heard this morning from the network operators that their standards presence was driven by their headquarters—their owners. We do not have a UK vendor. When you say that we need to improve our presence in standards bodies, who is going to do that and how is it going to be funded?

Dr Steedman: Actually, we have excellent people in the UK who participate in international standards work. The challenge is that there is a huge breadth of organisations, fora, consortia and formal bodies that generate, develop and maintain the standards that are then used in the evolution of the equipment—hardware, software and so on. We need to pick those organisations that are doing the critical work, particularly perhaps the ones around security, and ensure that we have British voices in there. It is true that if you look at a consortia model, you will find that the consortia that develop standards are what we call pay to play: companies pay

to join a consortium, and together they sit and write a standard. But actually there are other organisations that have more governance and more formal mechanisms for national representation, national voice and consumer voice, as well as industry voices. This spectrum is the piece that is often not well understood.

Our ambition, on the diversification taskforce, is to look to co-ordinate UK voices, which are currently fragmented in these multiple organisations, and to see what we can do to target, to focus, on the areas of standards development that we know are going to support the ambition of security, resilience and diversification in the UK—and, frankly, to allow other areas of standards development to carry on as they will. People write standards to suit themselves. But where we need formal standards to support a market structure in the UK, we must be absolutely sure that those standards have had UK stakeholder voices in the process, and that is part of the formal process.

You mentioned the ITU-T. That is where the DCMS, of course, is representing the Government. And the BSI represents the UK in ISO/IEC JTC 1 and in and the European regional organisations, including ETSI. So there is a big opportunity for us to take those lessons that we have learned in influencing these great international organisations and extend that policy of influence through co-ordination of the UK voice in other spaces. The ORAN-ALLIANCE is one example of where we need to improve our co-ordination. Who is going to pay for it?

The Chair: I am going to interrupt you. I am sorry, but I want to let the Minister get a last question in. My apologies.

Q80 Matt Warman: Thank you, Mr McCabe, although Dr Steedman was articulating some of the answers to the question that I am going to ask. Dr Steedman, the diversification strategy, as you described, lays out the importance of our work in international bodies and in international co-operation. Could you lay out what you think the most influential bodies are and where the Government should be focusing there? And Mr Parton, could you talk about how you see this Bill fitting together with the National Security and Investment Bill, to try to tackle some of the issues that you described yourself a few moments ago?

Dr Steedman: Thank you, Minister. I might suggest that this is very much a matter of horses for courses. There is a range of organisations. I mentioned the ORAN-ALLIANCE; that is clearly one. We know, obviously, about 3GPP and the role of ETSI and 3GPP; that is another. And there may be roles for the formal bodies. We need to discuss the ITU-T, the UK participation in ITU-T and how we can strengthen that. With respect, this is an area that we need to work further on; and in the diversification taskforce, we are talking about the detail of that and how we might approach it from a United Kingdom perspective.

I am optimistic that the initiatives that have been taken today with the diversification taskforce, under Lord Livingston's leadership, are going to produce for you really quite powerful ideas and initiatives to be taken forward in the years ahead. This is possibly the first time that the UK has really co-ordinated its input in this way to try to achieve some industry transformation and behavioural change.

The other areas I have mentioned, Minister, that are really important are in the area of procurement. This is not just about the technical standards; it is also about the way standards are used in the supply chain to stimulate behaviours and to enable SMEs to participate, rather than our just being locked into large-scale providers. I am very keen that we should comment on and discuss that, and those standards are not in the technical environment; they tend to be more in the business environment, where the UK has a very strong position already in global business standards. So there is another tool in our tool shed, to be used when we come to looking at shaping the market. I am looking forward to discussing that further with you in the taskforce.

Q81 Matt Warman: Mr Parton, will you comment briefly on the co-ordination between the NS&I Bill and this Bill in a more wide-ranging response to the Chinese situation?

Charles Parton: I cannot possibly deal with this in one minute. Obviously, telecoms is a very crucial—an increasingly crucial—part of critical national infrastructure, so they are very closely linked. It goes back to what I was saying earlier. There is this question of where in the science and technology field and our research and development we allow ourselves to co-operate with

China, given that its attitude is one, I think, that is really quite risky. So, when the DCMS talks about the extremely fine idea of setting up a national telecoms laboratory, I do hope that, in setting it up—it talks about co-operating widely internationally—it takes that sort of thing into account, too. I think that there will have to be great restrictions there.

This might be another example. I am well out of my field here, but we have designated high-risk and non-high-risk vendors, but what happens if some of the Chinese—they do not have to be Chinese—higher-risk vendors try to sneak under the wire by purchasing or using proxies? Again, I think that needs to be considered.

The Chair: I am afraid that brings the time for this witness session to a close. I think that we could all have done with a bit longer with both of you gentlemen, but thank you very much for your evidence. We are extremely grateful to you. That brings the formal part of the proceedings to a close.

Ordered, That further consideration be now adjourned.
—(*Maria Caulfield.*)

4.45 pm

Adjourned till Tuesday 19 January at twenty-five minutes past Nine o'clock.

Written evidence reported to the House

TSB 01 techUK

TSB 02 BT Group

TSB 03 Junade Ali CEng

TSB 04 Three

TSB 05 ITSPA (Internet Telephony Services Providers' Association)

TSB 06 ISPA UK (Internet Services Providers' Association)

