Public Bill Committee

TELECOMMUNICATIONS (SECURITY) BILL

First Sitting
Thursday 14 January 2021
(Morning)

CONTENTS
Programme motion agreed to.
Written evidence (Reporting to the House) motion agreed to.
Motion to sit in private agreed to.
Examination of witnesses.
Adjourned till this day at Two o’clock.
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
The Committee consisted of the following Members:

**Chairs:** † Mr Philip Hollobone, Steve McCabe

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

Sarah Thatcher, Huw Yardley, Committee Clerks

† attended the Committee

Witnesses

Patrick Binchy, Technical Services Director, Three
Derek McManus, Chief Operating Officer, O2
Andrea Donà, UK Head of Networks, Vodafone
Howard Watson, Chief Technology Officer, BT Group
Alex Towers, Group Policy and Public Affairs Director, BT Group
Public Bill Committee

Thursday 14 January 2021

(Morning)

[Mr Philip Hollobone in the Chair]

Telecommunications (Security) Bill

11.30 am

The Chair: Before we begin, I have a few preliminary announcements. Please switch electronic devices to silent. Tea and coffee are not allowed during sittings of this Committee. I would also like to remind Members of the need to observe the rules on physical distancing, both in this room and when entering and leaving via the marked entrance and exit doors. It is important that Members find their seats and leave the room promptly in order to avoid delays for other Members and staff.

Today we will first consider the programme motion on the amendment paper. We will then consider a motion to enable the reporting of written evidence for publication, and then a motion to allow us to deliberate in private about our questions, before the oral evidence session. In view of the time available, I hope, but cannot insist, that we take those matters without debate. I call the Minister to move the programme motion standing in his name, which was discussed on Tuesday by the Programming Sub-Committee for this Bill.

Motion made, and Question proposed,

That—

(1) the Committee shall (in addition to its first meeting at 11.30 am on Thursday 14 January) meet—

(a) at 2.00 pm on Thursday 14 January;
(b) at 9.25 am and 2.00 pm on Tuesday 19 January;
(c) at 11.30 am and 2.00 pm on Thursday 21 January;
(d) at 9.25 am and 2.00 pm on Tuesday 26 January; and
(e) at 11.30 am and 2.00 pm on Thursday 28 January;

(2) the Committee shall hear oral evidence in accordance with the following table:

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Witness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Thursday 14 January</td>
<td>Until no later than 11.25 am</td>
<td>Three; O2; Vodafone</td>
</tr>
<tr>
<td>Thursday 14 January</td>
<td>Until no later than 2.45 pm</td>
<td>British Telecommunications</td>
</tr>
<tr>
<td>Thursday 14 January</td>
<td>Until no later than 3.30 pm</td>
<td>Mavenir; NEC Europe Ltd</td>
</tr>
<tr>
<td>Thursday 14 January</td>
<td>Until no later than 4.15 pm</td>
<td>Small Cell Forum; Digital Policy Alliance</td>
</tr>
<tr>
<td>Thursday 14 January</td>
<td>Until no later than 4.45 pm</td>
<td>British Standards Institution; Royal United Services Institute</td>
</tr>
<tr>
<td>Tuesday 19 January</td>
<td>Until no later than 10.10 am</td>
<td>Webb Search; Oxford Information Labs</td>
</tr>
<tr>
<td>Tuesday 19 January</td>
<td>Until no later than 10.45 am</td>
<td>Dr Alexi Drew, the Centre for Science and Security Studies, King's College London</td>
</tr>
</tbody>
</table>

(3) the proceedings shall (so far as not previously concluded) be brought to a conclusion at 5.00 pm on Thursday 28 January.—(Matt Warman.)

Mr Kevan Jones (North Durham) (Lab): I have no problem with the programme motion, because it is sensible, but I want to put it on record that it is frankly nonsense for us to come in today and sit in a room to take evidence from virtual witnesses, as we will do next week as well. There is no reason why evidence sittings, particularly, could not happen remotely. I have attended two meetings this week, including a meeting on Tuesday of the Defence Committee, which took evidence from witnesses virtually.

I understand that things are being done in this way at the insistence of the Leader of the House. I think he is hiding behind the usual channels having sorted it out. I want to put it on the record that that is not true and that objections have been raised by the official Opposition, certainly about evidence sittings being done in this way. If we are to travel long distances, as many of those present have, to get here today and next week, that flies in the face of the advice of not only the Government but Public Health England about moving between areas.

I do not know whether, at this late stage, we could at least consider whether next week’s evidence could be taken virtually, because it is a bit ironic that we are sitting in a room here—I accept your rulings about social distancing and so on, Mr Hollobone—and that the evidence that we shall listen to from the witnesses today and next week will be given virtually.

The Chair: Mr Jones, I note your remarks and know that many others will share your view. As the Chair of the Committee I can operate only under the rules that I have been given by the House.

Question put and agreed to.

Resolved.

That, subject to the discretion of the Chair, any written evidence received by the Committee shall be reported to the House for publication.—(Matt Warman.)

The Chair: Copies of written evidence that the Committee receives will be circulated to Members by email and made available here in the Committee Room.

Resolved.

That, at this and any subsequent meeting at which oral evidence is to be heard, the Committee shall sit in private until the witnesses are admitted.—(Matt Warman.)
The Chair: We will now go into private sitting.

11.34 am
The Committee deliberated in private.

Examination of Witnesses
Patrick Binchy, Derek McManus and Andrea Donà gave evidence.

11.35 am
The Chair: All our witnesses today will be giving evidence by video link. Before calling the first panel of witnesses, I should first like to remind all hon. Members that questions should be limited to matters within the scope of the Bill and that we must stick to the timings in the programme order that the Committee has just agreed. For this first panel, we have until 12.30 pm. Secondly, may I ask whether any hon. Members on the Committee wish to declare now any relevant interests in connection with this Bill?

I now call the first panel of witnesses: Patrick Binchy, technical services director at Three, Derek McManus, chief operating officer at O2 and Andrea Donà, UK head of networks at Vodafone. Would the witnesses please be kind enough to introduce themselves for the record?

Patrick Binchy: Good morning. I am Patrick Binchy, and I work for Three, as you said, as the technical services director. I do not know what happened previously, but we lost some degree of ability to hear what you were saying. I think it was Chi Onwurah who was talking, but we could not hear what she was saying, and then it went completely silent for about two minutes.

The Chair: Patrick, I think that was because we were in private session, deciding how we were going to conduct our affairs. You were not cut off out of any rudeness; it was simply that we were going through some procedural matters. May I ask Derek McManus to introduce himself, please?

Derek McManus: Good morning. My name is Derek McManus; I am the chief operating officer of O2 in the UK, and part of my responsibility is therefore network.

The Chair: Thank you. Andrea Donà?

Andrea Donà: Good morning, everyone. I am Andrea Donà; I head up networks for Vodafone UK. I would like to thank you all for inviting us today; I appreciate the opportunity to give evidence to the Committee.

The Chair: Thank you. Andrea Donà?

Q1 The Chair: May I ask our witnesses whether they would like to make a short opening statement? It is not compulsory. Then we will go on to questions.

Patrick Binchy: Other than thanking you for under your chairship, Mr Hollobone, I want to start by thanking, as well as the witnesses, the members of the Committee, the officials and the staff of the House, who in coming into Parliament during a pandemic are also taking risks, which we very much regret.

I should have mentioned, as an interest, that I spent 20 years working in the telecoms industry within four network operators and vendors, as well as Ofcom, the regulator. I also may know personally some of the witnesses.

The Chair: Thank you. We have three superb witnesses from Three, O2 and Vodafone. I am now in the hands of Members.

Q2 Chi Onwurah (Newcastle upon Tyne Central) (Lab): It is a pleasure to serve under your chairship, Mr Hollobone. I want to start by thanking, as well as the witnesses, the members of the Committee, the officials and the staff of the House, who in coming into Parliament during a pandemic are also taking risks, which we very much regret.

I should have mentioned, as an interest, that I spent 20 years working in the telecoms industry within four network operators and vendors, as well as Ofcom, the regulator. I also may know personally some of the witnesses.

The Chair: Thank you. We have three superb witnesses from Three, O2 and Vodafone. I am now in the hands of Members.

Q2 Chi Onwurah (Newcastle upon Tyne Central) (Lab): It is a pleasure to serve under your chairship, Mr Hollobone. I want to start by thanking, as well as the witnesses, the members of the Committee, the officials and the staff of the House, who in coming into Parliament during a pandemic are also taking risks, which we very much regret.

I should have mentioned, as an interest, that I spent 20 years working in the telecoms industry within four network operators and vendors, as well as Ofcom, the regulator. I also may know personally some of the witnesses.

The Chair: It sounds like you might be dangerously over-qualified to take part in this Committee.

Chi Onwurah: You make a very good point, Mr Hollobone. I am going to try to keep my engineering and technical interest as much to the back as possible.

I am the shadow Minister for digital, and I am leading for Labour on this Bill. I will focus on the costs of removing Huawei and the diversification strategy, and Opposition colleagues will be focusing on different areas. I thank you for your presence and expertise. I want to ask two somewhat related questions.

First, some have given estimates of the costs of removing Huawei from your networks, and I want to verify whether those are the most up-to-date estimates. I also want to know whether they include opportunity costs, and the time and resources from your boards and others in your organisations. Are they the full costs, if you like, of the removal of Huawei? How can we minimise the economic impact, in your view? Are there other significant costs associated with the Bill and the implementation of a new security framework?

Secondly, your mobile network procurement is currently made through what I will call full-service providers, such as Huawei, Ericsson and Nokia. They basically
Patrick Binchy: There was quite a lot in those questions. I guess the first thing is that the costs are obviously commercially sensitive, and we cannot disclose them in a public environment, but we would be very happy to respond to any of the Members or the Committee in private to give the detail behind that. At a more generic level, there will, of course, be cost to the industry and to Three. We had selected Huawei to build our 5G network, and we have now selected a second vendor, Ericsson. We have to go through the process of mobilising Ericsson and removing the Huawei equipment, which has a cost to it and will have an impact.

In terms of the diversification of the market, there are really only two players in the UK market now. As you rightly point out, there are service as well as equipment capabilities within those suppliers. As we look for diversification, we need to diversify across all those aspects of the market. We are working with the Government, NCSC and DCMS in terms of how to approach that and how to build that. We will continue to support that as we go forward.

Derek McManus: We have similar commercial sensitivities on cost. You may or may not be aware that we are not indebted to Huawei. For our network, the cost of removing from the radio network is relatively small compared to some of our competitors. So, I will focus more on your second question, if that is okay.

You are absolutely right that we tend to buy end-to-end service in the current mobile environment. ORAN today is set up with a quite separate and different supply chain, with different companies specialising in software, different companies specialising in hardware and specialists doing the integration. It is likely to change the nature and relationship that we will have with suppliers. ORAN is relatively immature in its development. As it is technically and commercially ready for scale deployment, that may well change. But we see today that the leaders in ORAN tend to be smaller companies specialising in the hardware or, more specifically, the software.

Andrea Donà: Very much like my colleagues, I am more than happy to write to the Committee in the future, once we have completed our procurement process, with the details on the cost for replacing our high-risk vendor. More specifically, when it comes to the diversification strategy and the role that open RAN has, we at Vodafone believe that the UK should seek to be a leader in open RAN. We are, indeed, leading the way, and have committed to swapping out 2,600 of our base stations to an open RAN technology.

In order to fulfil that ambition, the current timescales for removing the high-risk vendor equipment must remain unchanged. We need the stability and the time, as Derek rightly points out, to allow industry and Government to develop a diverse supply chain and allow the technology to mature, both in its functionality and its capability, as well as the possibility of scaling industrially. The legacy vendors have had a lot of time in the market to develop their competence. We need to support any new entrants in the open RAN space with appropriate investment incentives and a policy framework that attracts and supports new entrants in the open RAN space.
very welcome for us. Our continual engagement will enable us to ensure that the new regulations can be enforced in practice effectively to achieve the scope of the Bill.

The Chair: Thank you. We will come to Miriam Cates next. Then, after Miriam, the order will be Kevan Jones, David Johnston, Christian Matheson, Dean Russell and James Wild.

Q4 Miriam Cates (Penistone and Stocksbridge) (Con): May I, too, pass on my thanks to the witnesses for appearing before us today? You have all referred to the significant financial costs to your organisations of removing the equipment from the high-risk vendors, but obviously, given the potential security implications, some are calling for the 2027 deadline to be brought forward. What would be the financial and logistical impacts of bringing forward the deadline on your organisations and your ability to operate? Would that be just too impossible—too difficult?

Patrick Binchy: In line with the previous answer, I cannot go through the specific commercials—they are commercially and competitively sensitive. But I would be happy to take such questions offline if you want to follow up on that.

Regarding the 2027 deadline, I think there is a balance here between UK connectivity and UK security. First and foremost, I would say that we have a security regime in place today. We use the Huawei cyber-security evaluation centre to check all of the technology that comes through Huawei and goes into UK networks, and we work closely with the security authorities to make sure that we are protecting the UK public today. We also have full visibility of any traffic that is transiting our network, either incoming or outgoing, so we are confident that we have the security in place today that is necessary.

In terms of achieving the 2027 timeline, that is a challenge. It is not going to be easy, because we need to balance that national connectivity against security and do it in a way that ensures that we continue to provide good-quality connectivity to the public.

There are a number of timelines within the legislation. We do not think the timeline for 2021 in terms of using equipment is a major issue. The 2023 35% cap and the 2027 are challenging, but we have plans in place. We have put our second vendor in place. They are already rolling our 5G network out in Manchester, Glasgow and Reading, and we are confident that we can meet those timelines and supply good-quality connectivity to the UK public.

Derek McManus: I think everybody, particularly in this environment, understands the immediate value of connectivity in the situation that we as UK society face. In terms of the opportunity for that connectivity to be part of economic growth as we evolve 5G and help build the economy, those are two of the competing challenges that we have to balance, while also removing HRVs and delivering diversification.

Yes, it is a matter of balancing costs in terms of investment, but we also have to recognise the customer disruption caused by removal of equipment. It is important that we maintain those other two key criteria—that important connectivity and that support to economic growth. By working together and taking the right balance, the Bill’s timescales are appropriate. I cannot, obviously, talk about the plans of individual businesses to meet the deadlines, but as an industry, I think it is appropriate.

Andrea Donà: At Vodafone, we believe that the Government’s decision to set a timeframe of 2027 truly reflects the complexity of what we have been asked to do. It is important that the deadline of 2027 does not change further. We need certainty and a fixed time plan so that we can plan for the future. Any further changes will disrupt our investment plans and will also cause undesired further disruption, as we attempt to accelerate a swap out that is, in itself, very complex, and will deliver inevitable disruption to our customers—the businesses and the public services. We are actively working with all the involved parties—the Government, Ofcom, NCSC and DCMS—to ensure that we minimise disruption. It is a complicated and difficult effort from a technology perspective, but also from the perspective of the practical implementation on the ground.

If the Government truly share our ambition to be a leader in digital infrastructure, we need to ensure that we give the high-risk vendor enough time to carry out the plans, under a very well-defined timescale and, as I said earlier, in parallel, allow the diversification agenda to grow, as well as the stability, to allow new entrants to come in and be a viable alternative to the incumbent high-risk vendor that we are swapping out.

The Chair: We will come on to Kevan Jones. Now I am getting the hang of this now, I do not think it is fair to always ask Patrick to be the first out of the blocks to answer the questions, so I will try to rotate so that everyone has a chance of going first.

Q5 Mr Jones: What is very clear from the first report from the National Cyber Security Centre is that existing Huawei equipment is a manageable risk. The only things that changed the Government’s stance were US sanctions on semiconductors for future equipment and, added to that, a layer of—I think—lobbying on behalf of certain anti-China parts of the Conservative party to remove the equipment from day one. Personally, I think there is no justification to do that. However, as you said, that leaves you with just two vendors for hardware, and any new entrant would have to meet the conditions in the Bill. What do you think the Government mean by a diversification strategy, and what are the timescales for that?

Having met many of you at a previous Committee and taken evidence from you, it is clear that there is little profit to be made on the hardware side because we all want cheaper phone calls, and you obviously react to customer demand to try to get costs down. What are the realistic prospects of any UK-based company or other vendor coming into the hardware side? On open RAN, I accept that it is for the future, but what timescales are we talking about for that having an impact on how our telecoms networks are organised?

Derek McManus: On timescales for ORAN, I think we are very early in the evolution of that technology. There are trials in the UK, as there are in various markets across the world. In our view, it will be at least a couple of years before you have a viable technical and commercial product, focused initially on rural. To have diversification in a meaningful way, you have to have
scale, and scale will take a number of years beyond that—I would say five to eight years to get a real, viable-scale vendor to challenge the two incumbents.

On your previous question about the likelihood of there being UK players in that market, the UK used to have a very healthy telecoms supply industry, which sadly over time has faded away. I think it is more likely that the UK could play in the software part of the future of radio, and particularly ORAN, than in the hardware part. I cannot see today a viable UK hardware provider. Actually, there are not that many UK telecoms suppliers around. But software is a bigger opportunity. Part of the diversification work that is going on with the industry and Government is looking at ways to encourage the inclusion of UK business in that emerging opportunity.

Q6 Mr Jones: So, for the conceivable future, we will be reliant on those two vendors: Nokia and Ericsson.

Derek McManus: Yes, and if you look at the scale of mobile growth, the fact that there are only two remaining viable competitors is an indication of how difficult it is to have competition in today's marketplace. That is technical and, to meet the economic challenges, that requires scale, too. There are other providers in the marketplace, but only two provide the 2G, 3G, 4G and 5G capability that the current UK markets require.

Andrea Donà: To answer the specific question on timescales, Vodafone UK is pioneering the development of open RAN. We were the first operator to achieve a commercial open RAN solution, in August last year, having delivered the first commercial open RAN unit on the ground radiating and carrying traffic at the Royal Welsh showground. We recently developed and announced plans to deploy open RAN across 2,600 sites. It is a promising innovation, but it is not yet mature enough to match the traditional vendors in terms of functionality and efficiency on an industrial scale.

However, if the UK wants to lead in this field and take advantage of the existing advantage that it has when it comes to design, it should continue putting its weight behind this promising technology and allow partnerships to be formed, where the incumbent vendors are asked to play a role in the architecture of this new technology. That will allow other parts of the technology chain—as Derek said, software, the baseband or the antennas—to attract and welcome new entrants through appropriate policy frameworks and the diversification strategy.

With new entrants, as we open this technology, we fuel innovation. If the UK keeps ahead of that, it will be able to be at the forefront of exciting new innovation. We welcome the steps that were outlined by Government to try to press this technology ahead. You could do that through trials or through incentives for the MNOs to use their technology. We can work together to create local research and development centres to fuel this new technology.

Q7 Mr Jones: In the near term, it is not going to replace the hardware that we need at the moment, the two vendors are providing. Are you talking specifically about open RAN, or are you talking about diversification or any strategy to develop a UK hardware supplier?

Andrea Donà: There is an opportunity for British companies to play an active role in the open RAN ecosystem. As we open up the interfaces of the technology, it creates a golden opportunity for British companies, with British support and know-how, to come and contribute to the development of this new technology.

Patrick Binchy: My views are broadly aligned with the previous answers. The reality of the situation that we find ourselves in is that there are only two practical vendors for the next couple of years. As both my colleagues have said, beyond that there is opportunity for ORAN.

I am not sure if it came across in the previous answers, but I would stress strongly that the first thing we need is the R&D. We need to understand how we can move this technology forward. As Derek said, trials are primarily operating in rural capacity, but to be a true competitor to the incumbents we have to be able to use it in deep urban areas, under significant loads, which needs a lot of development.

The Government can support trials and help build the ecosystem around them, but the first thing that we need is to get the research and development that will feed the trials. In terms of the Government's development of opportunities in ORAN, it is key that they look at working with international partners. This has to be scaleable; otherwise, it is never going to be commercially viable. The UK market will not be big enough to drive that scale and commerciality.

Q8 David Johnston (Wantage) (Con): It was widely reported that between 2009 and 2011, Vodafone found back-door vulnerabilities in equipment in Italy, and that you were assured by Huawei that they were being removed. You subsequently found that, in fact, they had not been removed. Do you have any concerns about back-door vulnerabilities in the equipment between now and 2027, and can you give us a sense of your management of that risk and what you do to try to make sure that there are not any?

Andrea Donà: Specifically on the incident you are referring to, which was in April 2019, it was a Telnet protocol, which is used by many vendors in the industry to perform diagnostic functions. It is important to note that it would have not been accessible from the internet. Detailed analysis showed that it was simply a failure to remove a function that is used, as I said, for performing diagnostics after it had been developed.

On the broader question of security and our concerns, we have always maintained the very highest level of security policies, security processes and security procurement mechanisms and frameworks. We use a layered approach to our security needs, whereby we secure by design. All our systems and process put in place guarantee the highest security standards, end to end. The UK networks and standards are the highest in the world. We constantly work hand in glove with the NCSC, an ad hoc centre where any new Huawei equipment or software goes through rigorous checks, audits and assurances, in line and in close collaboration with NCSC.

Patrick Binchy: I do not have much to add to that. We are similarly aligned in terms of our processes, from procurement to deployment. We have security checks throughout, and separate functions to make sure that
we are adhering to those. We work very closely with the NSCS and HCSEC in terms of the technologies that are in the network. Going forward, we will continue to do so. We will be reviewing the software and hardware versions that we have in place and ensuring that those are fully checked and validated. As I said earlier, we also have a full, independent view of the traffic traversing our network, so if something untoward were to start happening, we would immediately have a view of it, and would be able to shut it down independently.

Derek McManus: As I said earlier, we do not have sufficient numbers in the UK. We have fewer than 10 Huawei base stations, so although we perform all the necessary checks, we are not exposed on the scale of others in the market.

The Chair: I propose drawing this part of our deliberations to a close at 12.30 pm. We have five Members seeking to ask questions. If our panelists keep each of their answers to one minute, we will get everybody in—and we will get all the answers as well. I call Christian Matheson.

Q9 Christian Matheson (City of Chester) (Lab): Thank you, Mr Hollobone. In that case, I might take liberties and squeeze two questions into one.

Gentlemen, can I assume that you have done an audit—an asset register, if you like—and that you know where all the at-risk equipment is in your networks, so that once the Government push through an order, you know exactly where to go to address the requirements of that order? How interconnected are your networks?

Are you as confident as Mr McManus, who says that the integrity is fairly good? Do you all rely on each other to maintain an overall integrity? What if one is insecure?

Patrick Binchy: Of course, the networks are interconnected. As I said, we have full visibility and control of what transverses between the networks, so we can maintain full control over that. I do not think there are any significant risks in this space, because of all the security checks that we do on the equipment that comes into the network. We maintain a regular relationship with NSCS in terms of any future threats or concerns that it has. We all have our asset registers, and an understanding of what we have in our networks. We maintain and update those on an ongoing basis as the technology changes and evolves.

Q10 Christian Matheson: So you know where all the dodgy stuff would be, if you were asked to find it.

Patrick Binchy: We know where all the equipment is for our main supplier, yes.

Derek McManus: On the question on the asset register, absolutely. As for whether networks are interconnected, Patrick gave a good answer. The O2 and Vodafone networks are somewhat different, in that we work together on a network share; the O2 team manages and maintains a network in a certain geography, and the Vodafone team manages and maintains a physical network in another geography. In that sense, the O2 and Vodafone networks are very interconnected.

Andrea Doná: It is vital that the secondary legislation that accompanies the Bill clarifies assets in the telecoms network architecture that will be in scope of the security requirement, so that we can work knowing what we have audited, and knowing that the auditors always shared with NCSC. We need a clear understanding between Ofcom and us; as providers before the legislation is enforced, so that we understand exactly the boundaries and the scope, and we all work together, having done the audits, to close any vulnerabilities that we might have. That is a clear aspect of our working together: ensuring that the assets in the telecoms network infrastructure that are in scope are very well defined.

Q11 Dean Russell (Watford) (Con): Can you describe in layman’s terms the types of security threats that your organisations face, and how the security framework would address those?

Derek McManus: There are a number of different security threats. I will talk about network from a physical point of view, though there are obviously also scams and threats through direct human contact. It is mostly penetration of the physical network either from attack or from virus software. Attack is where foreign agencies or bodies look for vulnerabilities or holes in your defences. The role of the telecoms operator is to ensure that all its physical equipment and software are of the highest support and variation that defends from attack. We see quite a high volume of attack, either DDoS or penetration, on a regular basis. As I said, we do cyber-security by design. It is built into the fundamental processes of expanding and adding to our network, to protect us from those very things.

Andrea Doná: To add to what Derek says, it is also important that Government play a role in securing the additional security needs across the whole ecosystem of the supply chain, including the vendors. With the ever-changing nature of the threats we are exposed to, as Derek explained in layman’s terms, we have to change the protocols and the rules by which we and our vendors implement our defence mechanisms.

It is important that the Government do not leave providers such as us alone to reinforce these additional minimum security standards; they should play an active role in ensuring that vendors adapt their technology road map, so that things are done in a much more future-ready, cyber-security-compliant manner, because we face an ever-changing picture and ever-changing scenarios.

Patrick Binchy: In terms of the threats and penetration, as Derek said, the key things are that they get into the networks, either to bring the networks down and create chaos for the UK economy, or to extract information from the networks. All our security, as both my colleagues have said, is built into design, right from the very start of the procurement process. How do we protect against, and build networks that are able to detect, avoid and block, any of those risks and threats? We do that through our knowledge, the knowledge of NCSC and the authorities, and the knowledge of the wider industry on what is going on beyond the UK and in the international regime. We are constantly reviewing and updating our capability to protect against any of those threats.

The Chair: Gentlemen, we are right up against the clock. We have seven minutes left. Your answers are superb, but they need to be pithy, because we have three sets of questions coming and we need to get the answers in, and I am afraid that 12:30 pm is a hard cut-off; I am not allowed to extend beyond that.
Q12 James Wild (North West Norfolk) (Con): Hopefully my question has a simple yes-or-no answer. The Bill enables the Secretary of State to issue directions to telecoms not to use a designated vendor’s equipment. Does that provide the legal certainty that you need—a direction based on national security—to deal with any contractual issues you might have with those suppliers?

Patrick Binchy: I do not think it is quite as simple as yes or no; there are some challenges in how those rules and laws are articulated, and whether that allows us to move away from our commercial obligations. Of course we work with NCSC, and so far, what is in place is fully aligned with the direction taken by the Government and the Bill, so in this case, we believe it is sufficient.

Derek McManus: I refer you to Patrick’s answer. I have nothing specific to add. It depends on the circumstances. We continue to collaborate, and to speak with the authorities to ensure that we align with current and future needs, from a security point of view.

Andrea Donà: We will abide by the requirements.

The Chair: Superb—textbook answers.

Q13 Chi Onwurah: I ask these questions on behalf of Catherine West. Vodafone runs networks across Europe, and so does Three, whose owner is headquartered in Hong Kong, and O2, which is owned by Telefónica. Does the Bill duplicate or reflect legislation that you have seen elsewhere in your operations? What international comparisons are you aware of? Also, we have talked about standards being a key part of international collaboration. How many people, or what presence, do you have on international standards bodies?

Derek McManus: Basically, we have not seen anything directly like the UK legislation, although various forms of it can be seen internationally. The second question was on standards. We operate in 23 countries, and as you can imagine, their standards are key to us. We hold a lot of expertise, from a Telefónica group point of view, that the UK team is able to rely on and work with to ensure that we are at the very edge of developing the right standard.

Andrea Donà: As the Government plan to take a lead in enhancing the minimum security requirements, and in diversifying their telecoms strategy, we as a global company are happy to support the standard setting, and to advise on the practical implementation of the additional security requirements.

Patrick Binchy: I refer to Derek’s answer. We have a very similar position with regard to the UK legislation: we have not seen quite the same in the other countries. On standards, we play an active role, and we have a number of UK staff who act actively in standards setting.

Q14 The Parliamentary Under-Secretary of State for Digital, Culture, Media and Sport (Matt Warman): Thank you to all of you for your engagement today and with the Government up to this point. Given the time, I have one simple question. The Bill is setting up a new telecoms security framework to enhance network security. How confident are you that you will be able to comply with that in full, and what else would you like to see the Government do to enable you to do that?

Andrea Donà: We need the clarification that I mentioned of what is, and what is not, in scope, so that we have absolute clarity from the word go. We all work together to understand the profile of that implementation. It cannot be a big bang—everything complying from day one. We obviously need to do a detailed risk assessment of the areas that we need to work on immediately on the Bill’s coming into force, and of what can afford to be done at a secondary stage, based on the risk assessment and the risk management analysis of the various assets in our network.

Derek McManus: As I said in my opening remarks, collaboration to date on getting the Bill to this stage has been positive. We should continue that. My request is for flexibility to help us execute effectively, while balancing the other demands on the industry.

The Chair: You have 30 seconds, I am afraid, Patrick Binchy.

Patrick Binchy: Again, very similarly, we have to balance good connectivity with security. We are confident that our plans will meet the needs, but we will continue to work with Government and security on how we achieve and deliver that. It will be challenging, but we are confident that we can do it.

The Chair: Order. I am afraid that brings us to the end of the time allotted for the Committee to ask questions. On behalf of the Committee, I thank all our witnesses very much indeed for their evidence this morning.

Examination of Witnesses

Howard Watson and Alex Towers gave evidence.

12.30 pm

Q15 The Chair: We now move on to our second panel, which consists of Howard Watson, chief technology officer, and Alex Towers, group policy and public affairs director, both from BT Group. We have until 1 o’clock for this session. Would our two witnesses please kindly introduce themselves for the record and make a brief opening statement?

Howard Watson: Good afternoon, Mr Chairman. My name is Howard Watson, and I am BT Group’s chief technology officer.

We at BT support the principles of the Bill. We echo what the other operators have said—I have just listened in to the previous session—about the importance of having realistic timeframes, and we are pleased that the Government have listened on that. We have some outstanding questions, but they are pretty much about the detail of the implementation of the Bill. There is also need for some further reassurance about the proportionality across the rich landscape of operators that we have in the UK in how that regulation will be applied.

Alex Towers: Hello, my name is Alex Towers and I am director of policy and public affairs at BT Group. I have not really got anything to add to Howard’s opening statement. I think that covers it.

The Chair: Lovely. I am now in the hands of Members. I am very happy to give preference to Members who did not ask a question in the previous session. First out of the blocks is Sara Britcliffe.

Q16 Sara Britcliffe (Hyndburn) (Con): Thank you, Chair. It is just a quick one. What are the most pressing threats facing public telecoms networks, and how does this Bill address them?
Howard Watson: I note that some of this was answered by my colleagues earlier. Threats to the network include physical access. We all saw earlier this year a lot of attacks on our physical infrastructure, which were highly regrettable. I mean by that the setting alight of some of our infrastructure. We also faced logical threats, such as malware implants, DDoS attacks and what are called advanced persistent threats, which is an actor embedding themselves into parts of the environment, staying hidden for a while and potentially collecting credentials—think of the SolarWinds hack that is in the news at the moment. We take all those threats extremely seriously at BT. For as long as we have operated, we have worked very closely with all aspects of Government, and in particular with the National Cyber Security Centre. We take a sort of defence in depth approach. We have a red team who are ethically hacking us, and we are part of the TBEST scheme.

We think that the UK has a good track record here, but we also welcome the strengthening of that in the Bill. We think that some of the specific items about protecting even more against potential insider threat, looking hard at the vendors we use in the supply chain and having specific rigour about that, and the reporting mechanisms and requirements in the Bill, specifically around telecoms security requirements, will enhance that for all operators in the UK.

Alex Towers: I do not have much to add to that, except to say that, as Howard says, lots of the attention in the debate in the run-up to this Bill has been focused on a small number of very specific, clearly high-risk vendors. It is right that we take steps to protect ourselves around them, but just as important in the Bill will be the telecoms security requirements that stretch well beyond those specific vendors into all manner of aspects in which operators run their networks. Putting those two things together will be important.

The Chair: Thank you. The running order is Dean Russell, Miriam Cates, Kevan Jones, Christian Matheson and Chi Onwurah.

Q17 Dean Russell: Thank you, Chair. I would like to understand more how the diversification strategy that accompanies this Bill will benefit you as an organisation and the public.

Alex Towers: I think we see long term that diversification of vendors would be good for the operators in the marketplace if we can get to that point. It is important to say, I suppose, as the other operators were doing earlier on, that we are not at that point right now, so we are having to manage a situation where with the market as it stands we have a small number of very large-scale, important vendors and suppliers and we are having to remove one of them, clearly, from the 5G marketplace. That creates a degree of complexity and engineering difficulty that we need to just work our way through; so there is a lot of work to do just to manage within the current market framework to replace Huawei and to bring Nokia and Ericsson to the point we want. While we are doing that, if we can at the same time create the prospects of, in the longer term, a more open marketplace with a wider range of vendors—with other-scale vendors that do not quite work at the minute in the UK market, and Howard could probably explain exactly why that is, as well as with the potential for open RAN and other types of technology and software-based models to be developed—that is good for the whole industry and could be good for UK jobs and potential UK companies and therefore also for the citizen.

Howard Watson: I certainly welcome the Government’s supply chain diversification initiative here. It is concerning that we are moving from, essentially, three suppliers in the mobile supply chain down to only two. Our network going forward will use both of those. So widening that choice over time, for all the operators in the UK, is I think a critical opportunity. Please bear in mind that most operators quite like to have a primary source and a second source. It is unlikely that we will all start deploying equipment from four or five different vendors, because the operational challenge of the person in the van maintaining that tends to limit you to a choice of two; but being able to choose two from six is a lot better than choosing two from two, of course.

We welcome the three initiatives, which I will summarise. The first is whether we can encourage Samsung, NEC and other large vendors who build mobile networks elsewhere to enter the UK market. The second is open RAN and it really just creates through more open standards the ability to have more players in that end-to-end solution. The third area really is to have a thriving research agenda for the UK. We really welcome the £250 million allocated in the recent spend review. We already have a thriving research capability in the UK and I think continuing to focus that on antenna design, optoelectronics and semiconductors will have a role to play in diversification going forward.

Q18 Miriam Cates: You have said in your written evidence that you fully support the objectives of the Bill, to improve security in the networks, but 20 years ago we could not possibly have anticipated the kind of threats that we face today, so it is safe to assume that we cannot perceive the kind of threats that we will face in the future. Do you think that the Bill is wide-ranging and flexible enough for the Government to be able to respond to future threats and, if not, what could be done to make it more future-proof?

Howard Watson: I actually think the structure of the Bill accommodates that quite well. It allows secondary legislation and guidelines to be upgraded. We note the critical role of the National Cyber Security Centre in working with Government in doing that. I think, actually, you have taken care of that well with the way the Bill is structured.

Alex Towers: Yes, I would completely agree with that. I suppose our concern, slightly, at the minute, is to see some of that detail that is going to sit underneath the Bill in terms of a code of practice, in particular, and secondary legislation, because that is where it will become clear exactly what the implications are for operators. The sooner we can see some of that detail and get into the teeth of that, that would be great; but the way the Bill is structured, to allow that sort of detail to be updated on a regular basis as the world changes around us, seems totally sensible.

Q19 Mr Jones: The debate to date has mainly been around hardware, but you raised the issue—the bigger threat, certainly that I see, is from hacking and the vulnerability there. In terms of diversification, to be honest, we will have two vendors for the next considerable time, so when we talk about the diversification strategy and getting new vendors into the market, what timescales are we looking at? Are we actually putting all our eggs
into the open RAN basket? I agree that there is the possibility of advancing that sector in the UK. Realistically, we will have those two, one of which, we know, is financially vulnerable. What difference would having just one vendor make to you?

Howard Watson: Let me work through that. First, from our perspective, given that we do have quite a large amount of BT in our mobile network, which is with the high-risk vendor, we have a large swap-out programme already under way. Effectively, we already use Nokia to extend their reach, but also to introduce Ericsson. That essentially means that I will be replacing a significant amount of my network over the next seven years.

It is quite difficult for me to start introducing new opportunities and new options into that, certainly in the early part of that. For my network, I see the opportunities in the latter part of this decade, not the early part. That does not mean that there will not be opportunities to try open RAN in some of the rural areas or to conduct some trials with the other vendors that we have talked about. It is very much an industry approach that we are taking here. Some of my colleagues may be able to move a bit earlier. It is important that we collaborate and work as a UK set of operators with the Government to make sure that we have the right rich set of solutions.

We would not want to come down to just one vendor. That would certainly be a worry for many reasons, so we need to continue to ensure that, in the short term, we absolutely have the choice of two.

Alex Towers: Given the timeframes that Howard has described, it is a five to seven-year cycle of replacement for the vendor. That is why it makes sense, we think, to go big now on large-scale trials of things like open RAN. The important investment in R&D and the £250 million is a good step towards that, but we will probably need some more, because we need to be ready for the next cycle if it is going to be a workable solution in future.

Q20 Chi Onwurah: Thanks very much for joining us. We have heard that open RAN will not be mature for another eight years. Do you agree with that assessment? In that case, as you have outlined, we have two vendors and potential financial concerns about one. Can you say categorically whether it is possible to have network security with only one full-scale vendor to choose from and whether it is possible to have that with two?

Secondly, we heard from Sir Richard Dearlove, the previous head of MI5, that when Huawei was first used as a vendor or equipment supplier by BT, it was not considered worth informing Ministers of that fact, despite what he considered to be evident security concerns. Can you say what in the Bill changes that so that the Government of the day will be better aware of ongoing and future security concerns?

Thirdly, on behalf of Catherine West, on international collaboration, what presence do you have on standards bodies? Can you say what your budget is for research and development so that we can see how that compares with the £250 million on offer?

Alex Towers: I will defer to Howard on the questions about standards and technical details. On your point about the relationship with Government, I do not think that any of us were around in 2005, but I know that there is some sort of contested story about exactly who was told what about the introduction of Huawei. You would—[Inaudible.] We have moved a long way on that. We have a very close working relationship with the NCSC and with other parts of Government, and we would be very confident that we are constantly in contact with them about exactly the mix of suppliers that we are using. The introduction through the Bill of TSRs will take that even further, so we would be very confident that we have got a good enough structure there to ensure that any concerns that any part of Government had would be captured and dealt with, and Ofcom is also now in a position to regulate.

The question about relying on just the one supplier is less a concern about security and more one about the commercial resilience of that position. Howard can probably say a little bit more about the standards and the technical questions around that.

Q21 Chi Onwurah: Do you not think resilience is part of security? Is a network secure if it is not resilient?

Alex Towers: I think they overlap and that is one of our questions about the drafting of the Bill. There is clearly a relationship between those two things, and the concern about the timeframes for the removal of Huawei, for example, has been partly about ensuring that we have operational resilience during what is going to be a very complicated engineering programme to take out all its kit without losing resilience, in the sense of outages and blackouts for customers. Some of the Bill’s provisions talk about outages, but there is a difference between outages for operational maintenance and updating of kit and outages because of a security issue or attack. It is going to be quite important to pull those threads apart a little bit.

Howard Watson: On the vendor point, to summarise the approach that we are taking, we stopped purchase at the end of December, we will stop deployment in September of this year, we get down to 35% by two years hence from the end of next week, and then we have it removed from the mobile network by December 2027. I think that timeframe works well for us with introducing effectively a third supplier into our mobile network in terms of that 2027 point. It certainly helps mitigate any future steps in terms of a two-to-one.

I would not bank on it taking a full eight years to have an open RAN opportunity. As we heard from Andrea, colleagues at Vodafone have already started deployment. The real challenge there is about being able to use open RAN in dense urban areas where the technology works at its hardest, shall we say.

On your final question about research, we are in the top five investors in R&D in the UK—we invest in excess of £500 million a year across both research and development. In fact, the only companies that research more than us in the UK are the pharmaceuticals. I have 280 researchers based in the BT labs at Adastral Park near Ipswich and they, plus a standards organisation—we also draw in from engineers across my organisation—remain really actively involved in the standards bodies. I welcome what colleagues from the other operators say and think it is really important that we maintain that as a UK presence and as a European presence to ensure that we are not lost in the middle of any risk of
Q23 Chi Onwurah: I was interested in what you said about the weakest link for networks. I agree wholeheartedly with that. What are your thoughts on fixed networks? While the Government are consulting on fixed networks, apparently they are not minded to require the removal of high-risk vendors from existing fixed networks. You have Huawei in your fibre-to-the-cabinet network. Do you agree with that? Do you think that there is a reduced risk in the existing fixed network? Do you intend to remove high-risk vendors—that is, Huawei—from existing full-fibre build? Do you think that presents a security risk?

Howard Watson: We do believe that fixed networks, whether full-fibre or fibre-to-the-cabinet, have a different risk profile—a lower risk profile—from mobile networks. Please remember that it is only in the access part of the network, so the fibre—the device in the exchange that connects to that. In the core of the fixed network, we have no presence of high-risk vendors. So we do believe that is manageable. We worked really closely with DCMS and NCSC to arrive at the 35% threshold that was published a year ago, and we think maintaining that in the fixed network is proportionate and sufficient to ensure security there. Combined with the oversight that, again, we continue to support from the HCSEC and NCSC to ensure that we are inspecting everything that goes into the network.

I will also say that it is essential that we do take that approach because, as you know, we have large ambitions to increase full-fibre coverage in the UK. Ofcom reported in December that that was now at 18%. We at BT have now built for 3.5 million homes. We have a plan, which we have talked about—this is with the right conditions—to get to 20 million. We do need that 35% to be part of that plan because, again, introducing alternative vendors is challenging.

Q24 Chi Onwurah: Can you say why the risk profile is different for fixed as opposed to mobile?

Howard Watson: Fundamentally, you are dealing with a customer that is a fixed end point, so you are not having to provide handover between different sites as you do in mobile. Essentially, we are taking an electrical signal, modulating it into optical and converting it back to electrical at the other end, in very standard ethernet-based protocols. It is therefore really easy to see if there is a problem, so if something was infiltrating the network, we would spot it very quickly. Also, it is a very segmented network. The FTTC network has a granularity of over 85,000 cabinets in the UK, and the FTTP network has splitters for every 32 homes. Any issues are very easy to spot and so it is much easier to keep secure.

Q25 Chi Onwurah: Finally, with regard to having only two vendors for the mobile network for a number of years, can I ask two questions? I think that there has been a little discussion about resilience versus security, but if you are dependent on two vendors, one goes down and you are dependent on the other, would you say that that network was still secure? And is an increase in prices for equipment likely to accompany the reduction in the number of vendors available?

The Chair: I am afraid you have only about a minute to respond. Which of you gentlemen would like to answer?

Howard Watson: I will take that. You are right. We want two vendors to be consistently in the market, so that we can continue to deploy. If one of them were to...
fail—well, we insist on commercial and physical measures being in place such that we could step in and run the equipment that was already in the network, so it would not be switched off in the short term or anything like that; there would be no immediate threat to the existing network. It is the ability to build forward that is important.

As I think Alex mentioned earlier, the primary reason, which relates to the second part of your question, is that we want competition on pricing. As we have looked to have the two remaining vendors compete with each other for replacement of our Huawei estate, that has actually worked quite well as we have put in place contracts for that replacement.

The Chair: Gentlemen, I am afraid we have reached the limit of our own bandwidth this morning. That brings us to the end of the time allotted for the Committee to ask questions. I thank both gentlemen for their evidence. The Committee will next meet in this room at 2 o’clock this afternoon to take further evidence. Members will be delighted to know that they will have a far more accomplished and competent Chairman present.

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

1 pm

Adjourned till this day at Two o’clock.
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.

PBC (Bill 216) 2019 - 2021
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 *(Hyndburn)* (Con)
† Cates, Miriam *(Penistone and Stocksbridge)* (Con)
† Caulfield, Maria *(Lewes)* (Con)
Clark, Feryal *(Enfield North)* (Lab)
Crawley, Angela *(Lanark and Hamilton East)* (SNP)
† Johnston, David *(Wantage)* (Con)
† Jones, Mr Kevan *(North Durham)* (Lab)
† Lamont, John *(Berwickshire, Roxburgh and Selkirk)* (Con)
† Matheson, Christian *(City of Chester)* (Lab)
† Onwurah, Chi *(Newcastle upon Tyne Central)* (Lab)
† Richardson, Angela *(Guildford)* (Con)
† Russell, Dean *(Watford)* (Con)
† Sunderland, James *(Bracknell)* (Con)
Thomson, Richard *(Gordon)* (SNP)
† Warman, Matt *(Parliamentary Under-Secretary of State for Digital, Culture, Media and Sport)*
West, Catherine *(Hornsey and Wood Green)* (Lab)
† Wild, James *(North West Norfolk)* (Con)

Sarah Thatcher, Huw Yardley, *Committee Clerks*

† 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 closed 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. [Interjection.] 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 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 it be? 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 specialists 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 tested 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 lever 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 Cantarella: 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 actually makes the ability of different operators 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 comparisions 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 openness 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: 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 went in our previous discussions with you is 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 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 fund really 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 generally 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 5G 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...
probable 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: 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 spy put back, 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 do we realises 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 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, whereas smaller players 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.

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 if 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 to do things to hold a place that smaller players require assistance from the Government to enter the whole 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. That is important, 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 a good point. I recognise that the legislation needs to be put into that aspect of network security. Are you suggesting that more thought needs to be put into that aspect of network security? 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. A very good point.

Q68 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 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 those 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—you 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 the 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, guidance and guidance and 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 ‘RUSH’ 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)
Public Bill Committee

TELECOMMUNICATIONS (SECURITY) BILL

Third Sitting
Tuesday 19 January 2021
(Morning)

CONTENTS

Examination of witnesses.
Adjourned till this day at Two o’clock.
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

Saturday 23 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 (Hyndburn) (Con)
† Cates, Miriam (Penistone and Stocksbridge) (Con)
† Caulfield, Maria (Lewes) (Con)
Clark, Feryal (Enfield North) (Lab)
Crawley, Angela (Lanark and Hamilton East) (SNP)
† Johnston, David (Wantage) (Con)
† Jones, Mr Kevan (North Durham) (Lab)
† Lamont, John (Berwickshire, Roxburgh and Selkirk) (Con)
† Matheson, Christian (City of Chester) (Lab)
† Onwurah, Chi (Newcastle upon Tyne Central) (Lab)
† Richardson, Angela (Guildford) (Con)
† Russell, Dean (Watford) (Con)
† Sunderland, James (Bracknell) (Con)
Thomson, Richard (Gordon) (SNP)
† Warman, Matt (Parliamentary Under-Secretary of State for Digital, Culture, Media and Sport)
† West, Catherine (Hornsey and Wood Green) (Lab)
† Wild, James (North West Norfolk) (Con)
Sarah Thatcher, Huw Yardley, Yohanna Sallberg, Committee Clerks

† attended the Committee

**Witnesses**

Professor William Webb, CEO, Webb Search

Emily Taylor, Chief Executive, Oxford Information Labs

Dr Alexi Drew, Research Associate at the Centre for Science and Security Studies, Kings College, London

Simon Saunders, Director of Emerging Technology, Ofcom

Linsey Fussell, Group Director for Networks and Communications
Public Bill Committee

Tuesday 19 January 2021
(Morning)

[Mr Philip Hollobone in the Chair]

Telecommunications (Security) Bill

9.25 am
The Committee deliberated in private.

Examination of Witnesses
Professor William Webb and Emily Taylor gave evidence.

9.26 am

The Chair: We now resume the public sitting. Welcome to our third session of oral evidence on the Bill. All our witnesses today will be giving evidence by video link.

Before calling the first panel of witnesses, I remind all Members that questions should be limited to matters within the scope of the Bill, and that we must stick to the timings in the programme motion that the Committee has agreed. For the first panel, we have until 10 minutes past 10 o’clock.

I now call the first panel of witnesses: Professor William Webb, CEO of Webb Search, and Emily Taylor, chief executive of Oxford Information Labs. Would you please be kind enough to introduce yourselves for the record and make a brief opening statement? We will start—ladies first—with Emily Taylor.

Emily Taylor: Thank you, Mr Hollobone. Good morning. My name is Emily Taylor. I am a lawyer by training. I have worked in the internet environment for more than 20 years. I am CEO of Oxford Information Labs, a cyber-intelligence consultancy. We are actively involved in standards organisations such as the International Telecommunication Union. I have authored papers on 5G and geopolitics, and on China’s efforts to standardise many standards organisations, including the Internet Engineering Task Force, the International Telecommunication Union, which sits within the UN, and bodies such as 3GPP—the 3rd Generation Partnership Project—and the globe. Most relevant to this Committee is perhaps that I spent seven years at Ofcom, helping it with radio spectrum and technology strategy. I spent 18 months at the Department for Digital, Culture, Media and Sport, helping it with its 5G programme. I have also co-founded a start-up in the telecoms space, so I understand that area.

Potentially, I can help the Committee on the security side by looking at whether we can be sure that we are being proportionate in our response to security issues. I can certainly help on the diversification side by talking a little about the strategies of operators, the potential role of open radio access networks and other such diversification strategies, and perhaps some of the better ways to deliver diversification in the future.

The Chair: Thank you very much indeed. I am now in Members’ hands. Who would like to be first out of the blocks? Kevan Jones.

Q82 Mr Kevan Jones (North Durham) (Lab): Thank you very much for agreeing to come before us this morning, Emily, will you expand on standards issues and how important that will be to how the telecoms sector develops in the future? Who are the leading players in setting standards? You clearly made reference to China trying to get a set of regulations to suit itself. Where are we on what has been described in many documents as the D10—trying to get the democratic nations to influence that agenda? How do you see the way forward?

Emily Taylor: Thank you very much for those questions. The first aspect is why standards are important. Standards development can be very long, drawn-out and not the most interesting thing to participate in, but they are vital both for our security going forward and as part of the diversification strategy. Dominance or over-reliance on a small number of players is bad for innovation, security and procurement. It is great to see the importance of standards coming through in the diversification strategy that has been published. Although standards can take many years to be created, they also hang around for many years, so if we miss the boat with a particular standard when it is critical to a new industry or technology, that can have a lasting effect on our domestic and international industries.

Many scholars, such as Laura DeNardis, have pointed out that technology is not neutral, and this really applies in standards. By accident or design, standards embed the attitudes, values and world view of the engineers who create them. That has not really been a problem for western countries to date, because the US and European participants have tended to dominate, but going forward we need to find a new way of coping and co-existing with a technological superpower that does not share our values and that has invested heavily, with a strategic approach to standards, for several years.

You asked who the leading players are in standards, and in particular you alluded to the role of China. It is quite telling to reflect on the number of leadership positions across the standards organisations environment currently held by Chinese nationals. Of course there are many standards organisations, including the Internet Engineering Task Force, the International Telecommunication Union, which sits within the UN, and bodies such as 3GPP—the 3rd Generation Partnership Project—and
the European Telecommunication Standards Institute. The Chinese players we see, not just from the Government but industry, include Huawei, Futurewei, ZTE, China Mobile, China Academy of Telecommunications Technology, and Tencent. All of them are active in standards.

The ITU is headed by a Chinese national, and of 11 working groups within the ITU’s Telecommunication Standardisation Sector, or ITU-T, China has a chair or vice-chair in 10, and a total of 25 positions at chair or vice-chair; 135 so-called “questions”, which are sort of agenda items across those working groups; and 87 rapporteurs. I could go on, but I think the point is made.

On where we are with a D10, as you know, the Defence Committee has quite majored on the idea of a D10—indeed, the idea has been going around for several years. The key element as I understand it is a recognition that this country needs to act with others to have a chance of having the coverage and investment that China has had, and that there are like-minded countries that we can partner with across standards, and also to reinvest in domestic or shared capability for manufacturing. Manufacturing has been leaving western countries for more than 30 years and we are now seeing the effect of that. It is all very well to worry about the rise of China, but if at the same time you are asking China to make absolutely everything, it is inevitable that there will be some technology transfer.

Of course, the D10 does not exist. The idea of a Five Eyes type of thing that would also morph into an economic and legal type of partnership also does not exist. Five Eyes is an intelligence-sharing network, not an economic bloc or a trading bloc. So there are challenges, but there are also opportunities for partnerships.

Q83 Mr Jones: It is quite clear from what you have said that China has been active in this sector. That is not unusual; China has done similar types of things in other international bodies. Have we in the west taken our eye off the ball in terms of representation on these bodies, and what will it take to step up to the plate and be involved in these standards settings?

Emily Taylor: It is a bit like waking up halfway through a chess game and realising that you are about three moves away from checkmate. I think we have taken the eye off the ball, although the UK has been strong on standards and has invested in them, but we cannot match China, where we see the fruits of a patient long-term strategy. It is all laid out in the “China Standards 2035” document, but some people in working groups say that they get more than 100 papers to deal with just before a meeting.

There is a sense that we are losing a grip. Part of that is that we did not realise how far standards embed our values until we started to see the alternatives. New IP is something that we have been writing about and studying over the last year. That is China’s efforts to standardise effectively an alternative architecture for the internet, which would not be compatible with what we have today. That is at quite an advanced state across numerous working groups within the ITU.

The Chair: Professor Webb, would you like to respond?

Professor Webb: I certainly agree with all that. I have written standards myself and even run a standards body, so I know how they work. The important point is that it is not possible for a Government just to say, “We are going to influence that standard.” Standards are influenced by the working papers written by the companies that attend the standards body. The UK Government themselves could not really have an influence, and nor could a university or any other organisation like that, not unless they spent inordinate amounts of money and hired a lot of people to write a lot of papers. There needs to be a concerted global or western European effort, or some kind of larger scale activity that can help the larger companies with the resources and expertise and the standards bodies to step up their efforts.

Q84 Sara Britcliffe: Can I just quickly follow up with both witnesses? Were you consulted on the Bill prior to this?

Professor Webb: No, I was not.

Emily Taylor: No.
Q86 Chi Onwurah  (Newcastle upon Tyne Central) (Lab): It is a pleasure to serve under your chairmanship again, Mr Hollobone, and thanks very much to the witness for briefing us this morning. I should declare that I am a shareholder in Openreach and worked at side-by-side desks at Ofcom for some years, so I am well aware of his expertise in this area.

I have a couple of questions, starting with you, William. We heard from Mavenir on Thursday that open RAN could provide 2G, 3G, 4G and 5G networks now, but the operators were not looking to purchase networks from it. What is your view on the accuracy of that statement and the maturity of open RAN? What challenges does that pose with regard to the diversification strategy set out by the diversification taskforce?

Professor Webb: Thank you, Chi. I am sure Mavenir is correct that it can sell equipment that can do 2G, 3G, 4G and 5G, but that is not sufficient for an existing operator. If an operator wants to put this equipment into its network, it needs work with its network diagnostic systems; it needs to handle all of the various features that it might deliver to customers, businesses or whatever, or that it might use for optimising its network or the various software systems that it has. It has built these up over 20 or 30 years, so adding in the equipment is a lot more than simply ticking the box and saying that it can transmit 2G or 3G. That takes quite some time, particularly with the more complex base stations that we find in city centres. The ones in rural areas are typically much simpler and less problematic if they go wrong. That is why we see people like Vodafone trialling open RAN in those places.

Although Mavenir has all the ticks in the boxes, it does not yet have work-through with the operators to deliver something that really works for all of its network. As we have heard from the operators, that is a long, slow process. The operators are rightly risk averse—they do not want to rush out a whole load of equipment and for their networks to fail after a few months, with all the problems that that would have for consumers. So it seems to me that we are still some time away—I think the operators have said five, six or maybe seven years—from any significant deployment of open RAN. That sounds very plausible to me as a strategy for evolving a network. Of course, by the time you get to that point, they will have deployed most of their 5G network already, so it feels as though open RAN will be too little too late to have a significant impact on diversifying the 5G networks that we have in this country and that we will have for the next few years.

Q87 Chi Onwurah: What would your recommendations be in terms of an effective diversification strategy? Where is the capability strong?

Professor Webb: If I wanted to diversify, I would instruct the telecoms operators to diversify. I would not try and pull the levers one step removed. I would say to the telecoms operators, either with a carrot or a stick, “You must diversify. If you have x number of vendors in your network, I will give you £x million as a carrot.” The stick might be some kind of licence condition that said, “In order to meet your licence, you have to have at least x number of vendors in your network.” That seems to me to be the way to pull through, and then the operators can decide whether they want ORAN, something like NEC or Samsung or someone like that. They can make that choice and that will pull through the decisions on their behalf, rather than the Government trying to decide on their behalf what the best technology for them to use might be.

Q88 Chi Onwurah: Emily, what other security threats are not fully addressed by the Bill? How can we ensure that our networks are resilient to future security threats? I am thinking of the consolidation in cloud services, for example. As we move to more software-based networks, more and more of the value is in the cloud services. Say, for example, Amazon Web Services was bought by a Chinese company. Would you consider that a threat to the security of our networks?

Emily Taylor: Thank you very much for those questions. As a general point about the cyber-security of critical national infrastructure, I feel a little like we have been fetishising 5G and a single company for the last two years, perhaps at the expense of a more holistic awareness of systemic cyber-security risks. Ciaran Martin spoke eloquently yesterday about the need for flexibility in what critical national infrastructure is. The last year has shown us that what is critical very much depends on what you are going through at the time. Healthcare systems probably would not have been top of the list two years ago, but now they are. The SolarWinds attack shows that the identity of the vendor is not always the key risk point. SolarWinds is a very trusted vendor from a like-minded, close ally country, and yet it turns out to be a critical single point of failure across key, very sensitive Government Departments, both in the US and the UK.

Thank you for talking about consolidation across cloud services. Chi. One of my reflections on open RAN is that, although, of course, I am excited at the idea of open, interoperable standards, which would prevent vendor blocking, most of my experience has been in the internet environment rather than the mobile environment, and we are replete with open, interoperable standards, but we have a major competition problem. That in itself is not going to be enough of a lever to secure diversification.

On the point about acquisitions, particularly where you have cutting-edge technologies coming through, this country is really good at R&D—we have wonderful universities full of very brainy people who are creating things—but there does not seem to be the follow-through to create world-beating companies that can compete across the world stage. Why is that? It is because they either get sold to the US or to China. Of course, the foreign investment security strategies are all part of this as well, but you make a key point. If Amazon Web Services was sold to a frenemy country, that would potentially introduce the same kind of, at least theoretical, security risks that we have been troubled by over Huawei and 5G.

It is also the case that consolidation of infrastructure providers, like the cloud providers, is a security risk, because they become too big to fail. There was a brief outage of Google just before Christmas, and people just cannot work. When Cloudflare or Dyn go down, they introduce massive outages, particularly at a point where we are all so reliant on technology to do our work. These are security risks, and that highlights the need for a flexible approach. You have to be looking across all sectors.
Chi Onwurah: I see that William wants to come in. I just want to say that we have also been told that there was a major difference between fixed and mobile architecture when it came to security issues. You were just saying that there may be differences, but there are security issues within fixed networks as well as within our mobile networks.

Emily Taylor: Generally, our standard of security across the board is not as high as it should be.

Professor Webb: I realise that Chi had also asked me how the UK can strengthen its ability to provide diversified supply chains, and I did not address that.

I want to pick up on something Emily said as well. I think she is absolutely right—the UK has a great number of really excellent engineers, both in universities and in leading consultancy-type organisations. Here in Cambridge there is a plethora of wonderful consultancies and start-up companies. In my experience, the biggest problem is actually finance. To try to raise the finance to get a start-up company off the ground, particularly one that sells to operators who have huge purchasing power and tend to squeeze all their vendors—quite naturally—is very difficult in the UK. It is much easier in the US. Addressing the ability to provide finance for those kinds of entities and, to Emily’s point, allowing them to exist for many years rather than to be bought as part of that financial process would help more than anything else, for the UK to grow its own major players in this space.

Q90 The Parliamentary Under-Secretary of State for Digital, Culture, Media and Sport (Matt Warman): Thank you for your comments so far. You will have seen in the diversification strategy that we completely agree with the points you have made around standards and the importance of international co-operation, so I will not go further into that. But it is interesting that a lot of what you have talked about is the diversification strategy rather than the Bill itself. In terms of where we have put increased duties on Ofcom, for instance, where do you feel that there should be more in legislation, rather than in the diversification strategy itself? It seems that tying our hands is not what you are asking us to do, but there is obviously a balance there, isn’t there?

Professor Webb: Yes, I think there is a balance. I do not have strong views on that. The legislation appears to be sufficient and flexible in this space. I think the issue is the way it is implemented, and particularly the downstream actions of the Government and of Ofcom might need a bit more care.

Emily Taylor: The legislation is creating a framework, and a lot of that will be filled out through statutory instrument and the codes of practice that are envisioned. I imagine the codes of practice will reflect the TSRs to a certain component in the network, or that they need to some financial incentive to have a more diversified supplier base. That would make some kind of sense, given that this would add costs to their management of the network.

In terms of security, I think it is a bit more difficult to see how that one might follow. I can imagine that there might be certain security issues where, for example, the decision might be made that a replacement is needed for a certain component in the network, or that they need to purchase some additional elements, and then you might imagine that it might help to have some sort of financial incentive to do that. But I think that would be on more of a case-by-case basis—I cannot see a clear, catch-all type of approach that would enable that.

Emily Taylor: I very much agree with what Professor Webb has said. Indeed, one of my reflections on the draft Bill is that it is very much at the stick end rather than the carrot end. Maybe we will start to see a bit more of the incentives coming through as the detail is filled out. But I think that thinking about incentives would very much reflect the close working relationship that there has historically been between the industry and Government. That is not the case in every country; it is actually a benefit in this case.

Security is expensive, and it is also long term. The telecoms supply chain review last year put it very accurately: the market does not reward investment in security—quite the opposite—so I would hope that there would be some recognition from Government about what is needed.

I do not think that the investment in the diversification strategy is nearly going to match the investment that is required by the mobile providers who—yes, they are very successful large companies—have not had the great
decade that, say, the Googles of the world have had in terms of their margins. So you are asking an already squeezed sector to make substantial investments, and I think that is the place where you could be looking at incentives.

**Q92 Christian Matheson** (City of Chester) (Lab): Ms Taylor almost answered this question, but I just want to press both witnesses on this. The Minister referred to Professor Webb’s comment on “carrot and stick”, and obviously we are very keen to see diversification of suppliers increase in domestic capability as far as possible.

There is one way of looking at this legislation, which is that it can provide a market-led opening for suppliers, in a market that is no longer, in the long term, going to be distorted by, for example, Huawei, with its state backing. Is there any evidence, therefore, that other suppliers—first tier and lower suppliers—are looking at this and thinking, “There is a chance here to get back into the game”? Ms Taylor, you talked about security being quite a difficult and expensive barrier to overcome, but are there any discussions in the wider sector about there being an opportunity to be had here, or about whether, actually, a stronger diversification strategy is necessary?

**Emily Taylor:** The initiative is welcome—the diversification strategy is welcome—but, as Professor Webb has described, there are many barriers to entry for new suppliers. To build out an entire country’s network requires substantial scale, and, very understandably, the operators are risk-averse. You cannot just turn up and build out a network; open RAN is exciting, but, as you have heard from witnesses—and this morning, from Professor Webb—it is not ready, yet, to build out an entire country.

Also, the market distortions can still happen despite a diversification strategy. You can well imagine that the companies that decide it is attractive to enter this market are not, perhaps, the cheeky start-ups that you would want to encourage; they would be already dominant in other sectors. Imagine if we were sitting here, in five or 10 years’ time, lamenting the fact that the equipment market is now dominated by Microsoft and Google. I am just making that up as a hypothetical example—I have no knowledge to back that up—but those are the companies that have the sufficient scale and skills, and as Chi Onwurah said in her question we are moving to a hybrid network, where skills in cloud computing and software are going to define the success of the player.

**Professor Webb:** If you want to encourage a new entrant—be that a company that has some skills in this space but is upping its game to develop a complete system, or a brand-new company—they have got to develop the equipment, and that involves developing a lot of software and hardware, and an awful lot of effort and investment. If you add yet more requirements on them—for example, security requirements—that makes their effort even harder; it makes it even harder for new entrants to compete with existing players, who have already made much of that investment, to have the scale and capability to add on that extra. Adding security is the right thing to do—I am not criticising that—but the implication is that it will make it harder to diversify the supply chain. What you want to do is make it as easy as possible for new entrants, with the minimum requirements on equipment, if you want to bring a larger number in.

**Q93 Christian Matheson:** It would level the playing field, would it not? Everybody is having to work to the same level of security standards, rather than others thinking they can jump in there and cut in.

**Professor Webb:** I am not sure it would quite work like that. I think the operators would always want to procure to a certain security standard, whatever the legislation or not, so everyone would have to get to that standard. Raising the standards bar would essentially require everyone to move up higher above that bar.

**Emily Taylor:** If I may, just to support Professor Webb’s point, the security standards do not level the playing field, although they are the right thing to do. In just the same way as we have seen some of the perverse consequences of, say, GDPR, the companies that have the scale and capacity to absorb the cost of compliance fare better than the smaller companies, who really do not have the scale and capability. The disincentive to enter the market, or perhaps the incentive to exit the market, as a result of these requirements, hits precisely the type of companies that you want to encourage, although it is welcome to see some recognition of that in the factsheets, with the tiering system. The third tier would probably let the smaller independent ISPs and providers off the hook. It is not quite correct to view it as the security requirements, levelling the playing field. They are definitely required, and the market is not delivering that, but it will require close monitoring. I think, to ensure that there is still a competitive market.

**Q94 Christian Matheson:** If I have got it completely wrong, feel free to say, by the way, that I have got it completely wrong, because you are the experts here, not me.

Finally, could you sum up the chat around the sector at the moment? I get the impression that you are suggesting there is still a way to go to bring confidence that we can diversify across the broad range of the sector, as a result of this proposed legislation, and that there is still more reassurance and consultation required.

**Professor Webb:** Certainly, as I look at the information that I get back on ORAN, there is a lot more scepticism than optimism throughout the sector about its ability to do anything in the short term. We have talked a bit about why that is the case.

There is potentially more promise from the vendors that are somewhat established—the Samsungs and the NECs—and there is generally better comment about their ability to do something. If I had to look at what I am seeing around the industry and bring some advice, it would be focused on those vendors, rather than ORAN, as the most likely source of diversification over the next few years.

**Emily Taylor:** I can talk about the feedback that I have been getting. I come from a segment of the internet environment that has not historically been highly regulated at all. I would reflect that, if this Bill were brought forward to cover that sector, you would hear the screams. One thing that has really surprised me, and reassured me to a certain extent—it came through in the evidence you have heard—is that there is a degree of comfort with the direction of travel, and I think that speaks to the strong relationship that the industry has with Government on that.
The Chair: We have five minutes left; I am afraid there is a hard stop at 10 minutes past 10 o’clock. Two Members are seeking to ask questions, so would our witnesses treat this as a quickfire round, with punchy, pithy responses?

Q95 Mr Jones: Can I ask for your thoughts about Ofcom being the regulator of security? Has it got the capacity or culture to ensure the security of the network, particularly in light of the ISC’s 2013 report on critical national infrastructure? That suggested that civil servants did not even tell Ministers about security threats. Would it not be better to place security with an agency that is responsible for security, rather than with a regulator that has a wide range of responsibilities?

Professor Webb: I think that has already been mooted. I doubt Ofcom has that capability at the moment. In principle, it could acquire it and hire people who have that expertise, but the need for secrecy in many of these areas is always going to mean that we are better off with one centre of excellence, where the threats are analysed, assessed and understood. We have that, of course, in NCSC.

NCSC would advise Ofcom, perhaps at a high level. Perhaps they would not need to detail exactly what the issue was, but they could talk to Ofcom about the mitigation, and Ofcom could be the entity that performs the proportionality of understanding whether a threat needs to be addressed and to what extent, in the midst of all the other things. That is how I would arrange these organisations.

Emily Taylor: Thank you for this question, which goes to both the capabilities and the culture. With the capabilities, as I have said in earlier remarks, Ofcom is going to need to upskill. In reality, as Professor Webb has said, they are going to be reliant on expert advice from NCSC, at least in the medium term, until there is a significant transfer of skills and technology, and in terms of the need for secrecy and a broader view.

Ofcom’s historical role has been much less interventionist than is foreseen in this piece of legislation. Those cultural changes go deep into the organisation and into the character of the people who work there. Cultural change is always difficult and takes time, so I would not underestimate the challenge.

Q96 James Sunderland (Bracknell) (Con): This is a very explicit question to finish with, but could I ask of both of you whether, from a security perspective, you agree with the decision to kick out high-risk vendors from the network? If so, why?

The Chair: You have about 30 seconds each, I am afraid.

Emily Taylor: I think it was inevitable after the US sanctions on semiconductor chips. It is something I regret, because the more difficult part is what we had been trying to do for 17 years, which is to treat all the networks as potentially vulnerable and adopt an evidence-based approach.

I do not think there is a going back from there. Unfortunately, the effect of the US sanctions has not just been on our domestic market. It will have hardened the resolve of China to have an entirely indigenous supply chain, and therefore will hasten exactly the outcomes that it is intended to avoid. We need a much more positive approach, investing in innovation and research, matching the capability and advocating for the benefits for a single, open and free internet.

Professor Webb: I do not have strong views. I think it depends, but clearly if it is high risk then it is probably appropriate to exclude them. The worry I have is that you end up focusing predominantly on vendors that you think are high risk, rather than on the overall security challenge, which will be across all vendors.

The Chair: May I thank both our witnesses very much indeed for your informative evidence this morning, and for giving us the benefit of your wisdom and expertise? We are very grateful to you. That brings us to the end of the time allotted for the Committee to ask questions in the first session.

Examination of Witness

Dr Alexi Drew gave evidence.

10.9 am

The Chair: We now move on to our next panel, which is a solo performance from Dr Alexi Drew, research associate at the Centre for Science and Security Studies at King’s College London. Good morning, Dr Drew. Would you be kind enough to introduce yourself and make a brief introductory statement?

Dr Drew: Good morning, and thank you for inviting me to present and give evidence as part of this Committee. My name is, as stated, Dr Alexi Drew. I have actually recently changed my position. I currently work at the Policy Institute at King’s College London, and my area of research is emerging technologies and their security and geopolitical implications. I have done a few pieces on Huawei in particular and the implications of supply chain security issues and risks, with publications in the Financial Times and so on, and that is why I find myself in your company today, I believe.

The Chair: Thank you very much indeed. I am in the hands of Members. Who would like to ask the first question?

Q97 Mr Jones: Thank you for appearing before us today, Dr Drew. I would like your opinion on what the strategy is behind Huawei, possibly in terms of linking Huawei with the Chinese Government’s strategy in the telecoms sector. What is the bigger picture or vision they have for this sector?

Dr Drew: I think the bigger picture is bigger than purely telecoms when it comes to China. China treats all its emerging technologies and its advancement of technologies—including telecoms, artificial intelligence and quantum research—as part of a broader means of advancing its influence, its economic strength and its geopolitical power on a global, regional and domestic stage.

Telecoms is a large component of that predominantly because, as I am sure you are all aware, the future of telecoms is essentially the provision of what will be the backbone of most of those other technologies; you require a good, advanced telecoms network to gain the full benefits of applications of artificial intelligence or quantum networking, for example. I think China and the CCP have essentially seen that telecoms is a key component of that and have thus done as much as they
can both to strengthen the sector within China, and to export that to gain further routes for the future stages of implementing more technological growth and economic and political growth through the next stages of their emerging technology portfolio.

**Q98 Mr Jones:** So the strategy is about market domination in certain areas?

**Dr Drew:** I would say that is definitely the case. It is market domination primarily for domestic, good use: it is a mistake to think of all that China generally does as primarily internationally orientated. The primary interest is domestic strength, security and stability. The fact that that can be achieved through gaining dominance in markets outside China is an added benefit.

**Q99 Mr Jones:** Clearly there is Huawei’s domination in Europe, but what is the strategy when it comes to belt and road? We have seen investments in certain strategic areas such as the ports in Pakistan, Sri Lanka and other places. What is its strategy for telecoms? Is it a similar type of initiative?

**Dr Drew:** It is very similar. That is a great point to make. Pretty much wherever you see belt and road initiatives in, say, a port or supply chain of a physical good, you will see simultaneous investment and market input in a telecoms sense. There is a digital silk road as much as there is a belt and road initiative in the physical goods and supply chain sense.

They are becoming increasingly entwined fields; 10, maybe 15 years ago you could easily have seen a distinct separation between the physical supply chain and the digital supply chain. That differentiation is fading as we progress through time, and I think the Chinese have worked that out perhaps faster than we have and they are rapidly making inroads in order to amplify that effect and gain the benefits of it.

**Q100 Chi Onwurah:** Thank you for providing your expertise, Dr Drew. We heard from one of our previous witnesses that the security aspects here might be part of, if you like, a battle for the heart of the internet when it comes to embedding values into the standards that drive it. You seem to be saying that that is a part of China’s requirements to monitor and surveil its domestic population, so I wondered what your thoughts were on that expressly.

Also, you have great experience in evolving security threats. In your view, does the Bill address major telecommunications threats to national security—future and evolving threats? For example, do you think this Bill would have helped to mitigate the impact of the recent SolarWinds Orion network monitoring hack, which was also mentioned by a previous witness?

**Dr Drew:** I will start with the question of values. I am a great believer that technology and values and norms of behaviour are implicitly connected: you cannot separate them. It should be explicitly understood that it is an implicit truth. I believe—and I have stated this before to some of your colleagues and civil servants in various Departments—that the CCP has realised that the great firewall of China, which tries to police content within China, has holes in it and is not going to last, or was not going to last, given the direction that the internet, freedom of communication and transfer of information is going.

The next logical step, and what I believe is happening, is that if you cannot control the internet within the great firewall, it is better to be able to shape the internet everywhere, both outside and inside it. I would argue that a lot of the technological standard-setting that you see take place in the ITU and elsewhere is essentially that taking place, as is the use of social media platforms to harvest data, which is then used to aid in the censorship of domestic content within China.

With regard to evolving threats and the Bill specifically, I think that the Bill goes a very long way towards pre-emptively meeting threats that are likely to come in the future. My biggest issue echoes what I caught of the previous witness statements: the fact that it is a matter of capacity for the institutions that are given this responsibility—that is, Ofcom—and the ability to change their culture to actively engage within that framework and take action to ensure these standards are met and kept to. Those are my biggest queries about the ability of this Bill to be as forward-looking as we would like it to be.

Finally, with regard to SolarWinds, I think this Bill is aptly timed in a way, given the context of this particular threat. SolarWinds was a perfect example of a supply chain security risk, and a vector of attack that went through a diverse supply chain to meet what should have been some of the most secure systems that the United States had.

Telecoms will, as I have already said, be the backbone of all the UK’s future advancements of technology in all the things we are seeking to develop within our borders. The hardest thing to do as an attacker is to gain access. We should be making it as hard as possible to gain access; we should be making sure that there is as much oversight and understanding as is possible of where our supply chains go, the standards that they should meet, and whether those standards are being met, and I think this Bill goes some way towards that. I would argue that it needs to be continually updated, checked and maintained. This is not a one-off: times change, and the internet changes faster. Those would pretty much be my recommendations.

**Q101 Chi Onwurah:** Thank you very much for that. The Bill does not create any incentives for network operators to diversify their supply chain, or place any requirements on them to make notifications of changes to their supply chains or their networks that could have security implications. There is no proactive requirement on network operators to do that, or to actively participate in standards development—and we have heard about the importance of standards development and the huge presence of China in that space. Do you have any thoughts about how we could address those incentives, and also the power of standards development?

**Dr Drew:** The two essentially go together. If you look at the membership and those who take part in ITU standard setting committees and groups, you will see a predominance of not only state representation from China, but also representation of Chinese companies.

I think it needs to be made clear to our providers the benefits to them of being able to set standards; I believe this has been overlooked. The easiest way to do that is to simply look at some of the technical standards that have been set or lobbied for in this group by companies such as Huawei and ZTE, which are essentially entrenching
their technical standards into a global standards body—that
obviously gives them an advantage in producing that
output. I think our companies could benefit in exactly
the same way, and they would certainly benefit from
taking part.

On having providers be more proactively involved, I
think it would make complete sense for these actors to
be made to inform Ofcom, or whichever regulator is
chosen, of significant changes to their supply chains. It
would be akin to having a black box where we go,
“Okay, this black box must output something secure,
but we don’t need to know how it gets there.” I think we
should know, as much as is possible, who is involved in
the supply chains to reach our eventual telecoms network.

**Q102 Sara Britcliffe:** Good morning and thank you
for joining us, Dr Drew. In July last year, the Secretary
of State made it very clear that the ban on procurement
by the end of last year would have an effect on the
roll-out. My question is: what will be the impact of the
Bill on telecoms providers and infrastructure roll-out,
as well as the 2027 deadline?

**Dr Drew:** It is undeniable, as the previous witness
stated, that this Bill will increase costs and potentially
slow down the pace at which development of these
technologies, to the standards that are now being asked
for, can be done. I have been asked similar questions
before about what is the cost of us not getting to 5G
roll-out as soon as possible. My general response has
been to point out that although 5G is a backbone
technology that provides access, we have very few practical
applications of the speeds and connectivity that this
network will provide with.

It is something that you might see on your phone, but
the increase in speed from having a 5G connection will
be almost so fast as to be unnoticeable to the normal
user. We have not got to the point where we have large
city-wide technologies that will draw on this infrastructure,
such as traffic management, health systems and economic
production systems.

Although there might be a delay and an increase in
cost—which again, I think we should try to meet in a
way that incentivises more players to come into this
market—I think this delay is not crippling. That is
because, at the moment, although the 5G technology
itself is maturing, the uses of that technology are still
immature and I do not think we are losing out too much
if we have a slight delay, with the benefit of reaching
greater security.

**Q103 Sara Britcliffe:** Can I just quickly follow up on
that? I think you have answered it. Were the Government
right not to quantify the impact of any delay in roll-out
of 5G and full-fibre networks in their impact assessment?

**Dr Drew:** I believe they were. I have seen a lot of
tries to quantify the damage or impact of limiting
our vendor net, as it were. With the removal of Huawei,
I have seen multiple efforts to put a value to that—of
the slowdown and having to go to different vendors. I
am uncertain as to the accuracy of any of those, and
I think that it would be very difficult to put a number on
that in any useful sense.

My impression is that there is nothing that should
stop us from being able to enact the goals of this Bill
and the incentives to diversify the market, while also
being able to develop and invest in the next stage of 5G
use, which is its actual application, and to marry those
two up together in a manner that provides us with both
security and financial and economic benefit from putting
these systems in place.

**Q104 Matt Warman:** Thank you for what you have
said thus far. Some of it has touched on the National
Security and Investment Bill, which I think is a
complementary part of this. A lot of what you talked
about regarding any reservations you might have was
around, essentially, the resources for Ofcom—something
that I think we will be talking about quite a lot in
Committee. I am looking forward to saying that Ofcom
will have all of the resources that it needs. I wonder how
you think the Government could best demonstrate,
beyond that short statement, that Ofcom is getting the
resources that it needs.

**Dr Drew:** I think what needs to be considered in that
question is the type of resources that will be the hardest
for Ofcom to acquire. I frankly believe it is not necessarily
technology; I believe it is actually personnel. The edge
that is given to companies that have already been mentioned
in your hearings today—Google, Microsoft, Facebook
et al—is not necessarily in the technology, but in those
who design the technology. Those people are hard to
come by at the level that we require them at. They are
also very hard to keep, because once they reach that
level of acumen and they have Google, Facebook or
Amazon on their CV, they can pretty much choose
where they go and, often, how much they ask for in the
process.

I think the biggest issue that Government face—not
only in Ofcom, but in regards to future technology
policy—is attracting and keeping those individuals who
can provide the services and understanding, as well as
develop the tools, that a future Government will need.
If you can demonstrate a way to capture that talent and
retain it, I think that would go a long way to soothing
any potential questions about whether Ofcom will be
capable of meeting the requirements of this and other
Bills. This goes across all Departments, I feel.

**Q105 Matt Warman:** Although is it fair to say that
the best way that we demonstrate that capability currently
is in the capabilities that we see clearly demonstrated at
NCSC and GCHQ?

**Dr Drew:** Yes. I believe that this is potentially one
thing where, as much as possible, greater co-operation
between these Departments should be encouraged, to
the extent that it is possible to do, given how the
security dynamics of the different Departments work.
Quite frankly, Government do not have enough of this
kind of personnel and expertise. What you do have, you
must ensure is used as effectively as possible. That
means that you cannot let them languish in one silo or
Department, when their expertise would be highly useful
in another where suddenly they find themselves dealing
with types of issues that are far beyond their normal
remit.

**Matt Warman:** I am, of course, talking about
collaboration between NCSC and Ofcom.

**Q106 Mr Jones:** Can I just come back on that? I agree
with you that GCHQ has difficulty in retaining staff, as
you quite rightly say, Dr Drew, when they get to a
certain senior level. I think it is about more than that; it
is about culture, as well. Ofcom has a wide number of
responsibilities in this sector. Would it not be better, for the security element of this, to give that to the National Cyber Security Centre and GCHQ, rather than leaving it to an organisation, which—we have been told—even if it got the culture right, would take a long time to get there?

I think the Minister is relying on good co-operation between the two organisations, but it is clear from the 2013 ISC report on critical national infrastructure and Huawei that civil servants with a bent for looking at economic development did not have their eye on the ball in terms of security, and they did not even tell Ministers about security concerns that were clear then.

Dr Drew: That is a fantastic question. The best way for me to phrase this is that I believe there is an imbalance that is natural to those who have a particular role within Government or the civil service. Those with responsibility for economic advancement will have a different take on the same issue from those of their colleagues with a security bent to their work.

I find this is a complex topic that needs to be balanced across those different interests. That is why I would generally lean towards co-operation between these groups as opposed to others. I also suspect—although, due to the nature of their work, I cannot be certain—that GCHQ and the NCSC have significant work already, which is only likely to increase. Although they might have the technical capability that Ofcom lacks, I am not sure they have the capacity to take on the sheer volume of work that this is likely to create. I would argue that, actually, more resourcing in general is required for whatever co-operative body is created to carry out the actions of this Bill and other Bills attached to it. That is needed.

Q107 Mr Jones: I do not disagree with you about the balancing act between security and economic development, which will be important. This Bill leaves it with the Secretary of State for Digital, Culture, Media and Sport, who is not a natural fit for security, and there will clearly be tension between the two. Do you therefore think that it could have a different effect on those potentially two or three or four companies that you are attempting to incentivise. It would have a different effect on those potentially two or more categories. If you take one category to be pre-existing companies that previously have not operated within the UK, such as NEC from Japan, they are likely not to be put off to such a great extent—they have already had to deal with some level of security commitment within their normal markets. However, I suggest that it could be more of a barrier to entry for the smaller companies that we are attempting to encourage to get into this market. Emerging companies would find a culture of components and cultural risk to how they view their work, as well as the technical and financial cost of meeting the new standards. Yes, I believe there would be an impact, but it would be different between types of vendors that you are seeking to encourage.

Dr Drew: As to the second question first, I believe that security should be a component here. In fact, I believe it fits with what Ofcom is likely to be responsible for, and with the Online Harms White Paper as well. Security is fundamentally and inexorably linked with technology, culture and communications in the modern sense, so I believe that it would be important for that to be included as a key provision for DCMS.

With regard to the differences between fixed networks and 5G and the implications of this Bill, in the efficacy of its methodology towards the other, there are technical differences in how 5G operates right now and how we perceive the next generation of telecommunications to operate, but those differences will change over time, I believe. They will become less distinct. It is likely that fixed networks will move towards the concept of computing on the edge, and this is indeed already happening in some senses.

As for the actual efforts to control security risk, I do not see any major differences between telecommunications suppliers and fixed network suppliers. There is the same potential risk. You mentioned the SolarWinds hack earlier. That was a fixed network supplier in a way—it was not telecommunications—but there was the same risk involved and the same means of access, through a diversified chain with limited oversight at Government level, because it is a private sector actor with limited responsibilities. That is as true in that case as it would be for a fixed network with Cisco, and as it would be with a telecoms provider by ZTE, Huawei, Ericsson or any other. I do not think there is a significant technical difference to mean that the goals and direction of this Bill could not, and perhaps should not, be applied to others.

Q110 Chi Onwurah: We have talked a lot about 5G—indeed, we have been accused of fetishising 5G. The Government are currently consulting on security issues and fixed networks. Do you see major architectural differences or market differences in the security threats for fixed networks? Are they similar, and should a similar approach be taken to the removal of high-risk vendors? With regards to Ofcom, its principal duties are set out in the Communications Act 2003—I know this very well, having worked for it. They are “to further the interests of citizens in relation to communications matters; and to further the interests of consumers in relevant markets, where appropriate by promoting competition.”

Dr Drew: Do you think there is an argument to add a further security duty, if that is going to take such a large portion of Ofcom’s capacity?

Dr Drew: As to the second question first, I believe that security should be a component here. In fact, I believe it fits with what Ofcom is likely to be responsible for, and with the Online Harms White Paper as well. Security is fundamentally and inexorably linked with technology, culture and communications in the modern sense, so I believe that it would be important for that to be included as a key provision for DCMS.

With regard to the differences between fixed networks and 5G and the implications of this Bill, in the efficacy of its methodology towards the other, there are technical differences in how 5G operates right now and how we perceive the next generation of telecommunications to operate, but those differences will change over time, I believe. They will become less distinct. It is likely that fixed networks will move towards the concept of computing on the edge, and this is indeed already happening in some senses.

As for the actual efforts to control security risk, I do not see any major differences between telecommunications suppliers and fixed network suppliers. There is the same potential risk. You mentioned the SolarWinds hack earlier. That was a fixed network supplier in a way—it was not telecommunications—but there was the same risk involved and the same means of access, through a diversified chain with limited oversight at Government level, because it is a private sector actor with limited responsibilities. That is as true in that case as it would be for a fixed network with Cisco, and as it would be with a telecoms provider by ZTE, Huawei, Ericsson or any other. I do not think there is a significant technical difference to mean that the goals and direction of this Bill could not, and perhaps should not, be applied to others.

Q110 Chi Onwurah: I have just one quick follow-up question. Thank you very much for your evidence. The Bill separates out the diversification strategy, and in fact
it does not refer to the diversification strategy. Is it possible for the UK to have secure networks without a diverse supply chain for them?

**Dr Drew:** That is a great question that comes with a very simple answer: no. The worst-case scenario for creating a risk in this sense is when monopoly meets supply chain—in secure supply chain in this case. Arguably, the reason why SolarWinds was so successful is that it provided the same service to so many different organisations and departments in the United States. Therefore, if you access one—SolarWinds—you access almost all. That is the risk.

The same is true in this sense if you transfer these issues to telecommunications or fixed networks. If you have only a single supplier, all it takes is that supplier to be compromised for your whole network to be compromised. As I said earlier, with any form of cyber-attack, the access is always the hardest part if you are the attacker, so if you have an easy target or if the target is just one point, they can throw all their resources at it and it is easier. I would argue that diversification is one of the most basic and probably most effective means of limiting the damage that could be caused in any attack against one of those vectors.

**Chi Onwurah:** Thank you very much.

**The Chair:** Dr Drew, there are no further questions from Members, so I thank you very much indeed for your time this morning and for sharing your expertise with the Committee.

**Dr Drew:** It was a pleasure. Thank you.

### Examination of Witnesses

**Simon Saunders and Lindsey Fussell gave evidence.**

10.38 am

**The Chair:** We now move to the next panel, which consists of Simon Saunders, director of emerging technology at Ofcom, and Lindsey Fussell—I hope I pronounced that correctly—group director for networks and communications, also from Ofcom. In the previous two sessions we have been talking about you quite a lot, and now is your chance to respond. Could I ask you to introduce yourself and give a brief opening statement, starting with Lindsey?

**Lindsey Fussell:** Thank you, Chair; that was the correct pronunciation of my name. I am Lindsey Fussell, I am the group director for networks and communication at Ofcom. My group oversees all of our telecoms regulation, including the new responsibilities for network security that we will be talking about today. I am sure we will have a lot of conversation about the nature of our responsibilities, but I think by way of opening I would say that we very much welcome the Bill. The National Cyber Security Centre found in carrying out its telecoms supply chain review that our existing responsibilities and the existing approach that operators took to telecoms security—and our powers as a regulator alongside that—really needed substantial strengthening, so it is great to see that happening in the Bill, giving operators the certainty of what they need to do to promote telecoms security.

**Simon Saunders:** Good morning, I am Simon Saunders, Ofcom’s director of emerging and online technology. I have worked on mobile network technology since 1991, before there was 1G, all the way through to current work on today’s and future implementations of 5G. Last week we published a round-up of technologies that could form the basis of future 6G networks. I have worked for mobile equipment vendors, operators, large end users and software companies. I founded and chaired an industry association, the Small Cell Forum, where I led a previous initiative on interoperability and open standards—in that case, in 3G—and I have invented a number of mobile technologies.

Today, I lead Ofcom’s technical work on diversification, including Open RAN. I provide technical advice on behalf of Ofcom to the telecoms diversification taskforce. I hope I can help the Committee with issues on diversification, Open RAN and Ofcom’s potential role in that area.

**The Chair:** Thank you very much. James Wild will start the questions, followed by Sara Britcliffe.

**Q111 James Wild** (North West Norfolk) (Con): Clearly, these are new substantial duties on network providers and on you as the regulator to enforce them. What assessment have you made of the resourcing and additional expertise that Ofcom will require to take on these new duties?

**The Chair:** Simon Saunders?

**Lindsey Fussell:** I think I will lead on that one, if that is all right. Thank you for the question. I will start by clarifying Ofcom’s role in the two parts of the Bill—I am sure we will talk about both. We have a significant role in relation to the telecoms security requirements, where we will have the obligation of monitoring and enforcing operators’ compliance against them. In relation to high-risk vendors, our involvement is rather more limited. The Secretary of State will have the power to direct us to collect factual information from the operators, but the question of monitoring, compliance and enforcement then rests with the Secretary of State. I thought it might be helpful to clarify the two different roles before we got going.

In relation to telecoms security, as you say, these are important new responsibilities. We have existing responsibilities for network security—and have had since 2011, albeit in a more limited way—so we have a network security team in place. We are also very familiar with monitoring clients and enforcement, and with working with precisely the same set of operators that we will hear about on the remit of other responsibilities, so we have a base to start from. That absolutely does not underplay the difficulty, importance and challenge of building up our resources to deal with this. We anticipate that the cost will be around £6 million to £7 million in steady state, and we will build up a team of probably 40 to 50 new people and new resources to cope with those responsibilities.

**The Chair:** Simon, do you have anything to add?

**Simon Saunders:** On our capabilities relevant to the expectations end of things, we are building on our existing capability, working with mobile operators and network providers on the equipment and the software. That is spread across Ofcom, in the leading networks group that Lindsey leads, the spectrum group, and indeed in our technology group, which I look after. In
the relevant teams, we have been adding capabilities in with recent experience, with the mobile operators and mobile networks applying the formal diversification.

Q112 James Wild: You refer to needing 40 to 50 new additional staff. Have you begun recruiting those people yet and how confident are you that you will be able to get them? The security world is a competitive space and these are highly sought skills. How confident are you that you will be able to get those people in place in order to monitor and enforce the powers in the Bill?

Lindsey Fussell: We have indeed already started to build up our team, and have had some success in recruiting people with experience of network security—from the operators, for example. We do not underplay the difficulty of doing that; I completely agree that those are sought-after resources. Frankly, it is unlikely that we will be able to compete on salary. The type of people we attract are those who are interested in looking at these questions from that broader perspective—looking across the industry—rather than in their previous roles in companies.

We have found that we can have some success in that, but we will also have to be creative in the way that we approach this. We are thinking about how we can build up a pipeline, for example. The NCSC has accredited a number of university courses, and we are looking at how we, alongside the NCSC, can pick graduates up from those courses, for example, to build up a future pipeline of staff, as well as bringing in people with more direct experience.

The Chair: Simon, do you have anything to add?

Simon Saunders: No, not in that area. It might be relevant to mention, just to make the point that it can be done, that I actually joined Ofcom from a role at Google.

Q113 Sara Britcliffe: You never know, you might become shadow Minister when you move on from the job at Ofcom, as we have seen. My question is quite simple: do you believe that the Secretary of State is the right person to exercise the powers?

Lindsey Fussell: Are you referring there to the high-risk vendor powers?

Sara Britcliffe: Yes.

Lindsey Fussell: Yes, I think so. It is important to say that, across the scope of the whole Bill, it is not Ofcom’s role to make national security judgments. That is really important. Clearly, that is the Government’s and the Secretary of State’s role, taking advice from the NCSC and the intelligence agencies. In relation to telecoms security, that has enabled us to take the very detailed work and the threat assessment that the NCSC has done, which have been translated into a set of requirements in the code of practice, and to apply those and work with operators to monitor and enforce that compliance without having to make those national security judgments ourselves. On high-risk vendors, I think it inevitable that there will be more national security judgments to be made, so it is quite proper that that role sits with Government rather than the regulator.

Q114 Mr Jones: Your responsibilities are quite broad, and this is an expansion for you. You have already talked about recruiting staff for this task. How many of those staff will have to have STRAP clearance?

Lindsey Fussell: As I say, we have existing networks security responsibilities, so the issue of security clearance is one that we already need to deal with. I think the point that I have just made is important: we will not be making national security judgments, and that means that we will need access to less national security information than you might imagine. I do not think that we will be routinely handling national security information, but where the NSCS feels that it is required, there are clearly provisions in place for that.

Having said that, as now and in future, there are occasions when we have to handle sensitive information, and we do have the necessary security clearances in place at different levels for our staff to do that. As we recruit, we will obviously ensure that people have those necessary security clearances so that we can handle any sensitive information that we are given.

Q115 Mr Jones: I am sorry, but I do not accept what you have just said. If you are going to be the guardian of security as a member of the ISC who has STRAP clearance, you are talking about highly sensitive information to which, quite rightly, is guarded by the agencies for national security reasons. You will have to have a number of people who are STRAP-cleared. All I am asking is what that number is.

Lindsey Fussell: We would clearly take guidance from the NSCS and others on whether they think STRAP clearance is required, because of course, it is for the agencies to have STRAP clearance and to classify information. I have had STRAP clearance in the past, in my previous roles in Government, for example, so I am well aware of the different security classifications that are required and the nature of the information that is to be handled. At the moment, the NCSC has not signalled to us that it thinks we require staff with STRAP clearance, but clearly, if it feels that that is needed for the type of information that we may need to handle, we would make sure that happened.

Q116 Mr Jones: Personally, I do not see how you can do the job without having STRAP clearance making these decisions. As you know, you may have had STRAP clearance in the past, but it is not historic; you need to have it currently.

Lindsey Fussell: Of course.

Q117 Mr Jones: You said in response to Sara’s question about whether the Secretary of State is the right person to make these decisions that you are not necessarily making the decisions. Clearly, however, there will be a pull between your role in promoting the sector in terms of economic development, and national security. You will have an opinion on that. How will you balance that judgment?

Lindsey Fussell: Our role in relation to the requirements is pretty clear. The Government, through the legislation that is being considered by this Committee, are setting out a series of duties on providers and then giving us a code of practice, which has been developed through the work that the NCSC did. That sets out in some detail what operators, in particular the larger operators, will be required to do to meet those requirements. What we will be doing is monitoring, discussing with and talking to those operators as they go on that journey, and ultimately—of course—enforcing compliance, if we think that is needed. Of course, our trade-off is always to be
proportionate in the application of our powers, but it is quite clear that the expectation is that we will enable, encourage and require operators to comply with the requirements.

Stepping back from that, there is clearly a balance of judgment that the Government have taken in bringing forward these measures. We all want, for example, to see people across the UK getting the best connectivity possible as fast as possible. This Bill may well have an implication for some of those plans, albeit that operators are well aware of what is coming. But of course the balance of judgment is the importance that security plays for consumers, in making sure that they have access to secure networks, and bearing in mind the significant costs that can be incurred by companies and ultimately by consumers if there are cyber-attacks.

Q118 Mr Jones: That will be a very difficult judgment to balance. I suggest that you read the 2013 ISC report, which is very informative on this issue and about where the balance went the other way, in terms of civil servants arguing then that economic development was better than actual security. So I think it will be a very difficult judgment to make.

Can I ask you about an issue regarding oversight? Frankly, I am not a great fan of quangos, because I think their accountability is limited and they allow Ministers to offload difficult responsibilities on to people who have very little parliamentary oversight. Regarding the oversight of your organisation from Parliament's point of view, some of these decisions will clearly be highly classified. The Digital, Culture, Media and Sport Committee will not be able to look at them, because of the security classification. So how will we ensure that you and Ministers will consider the importance of security around these issues?

Lindsey Fussell: That is a really important question. Clearly, we are accountable to Parliament—

Mr Jones: Sort of.

Lindsey Fussell: And we are ready to come and give evidence about our work to any Select Committee that would like to hear that evidence.

As I say, we ourselves will not make national security judgments, but I hear your point that the relationship and the role that we play in monitoring telecoms security, and enforcing those obligations on operators, is a very important one. Under the legislation, we are required to provide an annual report to the Secretary of State about what we find on the state of play regarding how operators are moving towards compliance, and indeed on any security compromises or incidents that we have uncovered and the action that has been taken in relation to those, and on any new threats or other issues that we have identified.

It will then be for the Secretary of State to consider whether they publish that report, and how much of it they publish. We will publish a summary of our work in our annual Connected Nations reports; we do that now. And as I have said, of course we will be ready to talk to any Select Committee that wishes to hear evidence of our role and how it is playing out.

Q119 Mr Jones: But the Secretary of State is not Parliament. The Secretary of State can hide behind things, or choose what he or she wants to put in the public domain. Do you think that the Bill needs to establish some role for Parliament at least to have an annual report, whether it is to the DCMS Committee or, if it has classified information in it, to the ISC?

Lindsey Fussell: I think that is really a question for Government rather than the regulator. We will be ready to provide whatever accountability the legislation requires of us, as well as providing direct accountability by talking to Parliament and Select Committees.

Q120 Christian Matheson: To follow up on one of Mr Jones's questions, you say that you will not be taking decisions on national security matters. Who decides within Ofcom whether it is a national security matter or not?

Lindsey Fussell: I think the structural framework helps us a great deal here, as I have already indicated. Clearly, the NCSC carried out a really detailed supply chain review, which identified the threats that could occur in different elements of the network, and it has now turned that into telecoms security requirements and, ultimately, into the code of practice. We will be giving—indeed, the legislation requires us to—considerable weight to that code of practice and the judgments that the NCSC has reached on what is required to combat those threats. That will then enable us to judge and monitor whether operators are doing what is said in the code of practice.

If, for example, an operator were to say to us that it was not going to meet something set out in the code of practice because it considered that an alternative way would meet that threat, we will have arrangements in place with the NCSC to enable us to seek its advice and guidance at that point on whether that satisfies the requirements of national security.

Q121 Christian Matheson: Who takes the decision, then, to refer it to the NCSC?Where in Ofcom does that decision sit?

Lindsey Fussell: Clearly, we would start that conversation within the team and escalate it if necessary, but I do not think that it will actually be an issue in practice. We already have very good working relationships in place with the NCSC, and regular collaboration and discussion. The legislation enables us to share information with the NCSC to enable either it or us to perform its duties. I do not think that there will be any issue in practice, or any surprise in terms of our regular interactions with it.

Q122 Christian Matheson: Can I ask something slightly different now? Do you have much internal movement in Ofcom? Do you have an internal jobs board? Do people move around and develop their careers there?

Lindsey Fussell: Yes, we do. Of course, like any organisation, you would expect that. Ofcom has a range of people with different skills in it, as you would expect. It is actually far broader than, for example, some of the Government Departments that I have worked in before. We have people who are specialist technologists. Simon has talked about his experience. We have economists, lawyers, colleagues who specialise in enforcement, colleagues who specialise in policy, and many other professions. Although people absolutely do move and develop their career, and certainly in relation to these kinds of new responsibilities we will look to upskill existing colleagues where that is possible and where it makes sense to do so, we also employ an awful lot of specialists who will tend to stay more in that specialism and apply that to our work.
Q123 Christian Matheson: That is the point I am getting at. If I think about recent changes at Ofcom, you have had responsibilities for monitoring the BBC, for example. Online harms is coming to Ofcom. It seems that quite a lot is being asked of you, and demanded of you. How can we be sure that you have the capacity to manage the workload, and the technical capacity to manage these very challenging issues?

Lindsey Fussell: I am certainly not going to deny that there is quite a lot going on, and the organisation is expanding, as you say, albeit with different deadlines and different timescales for the new responsibilities. I have already talked about our recruitment plans to ensure that we have the specialist skills in place to focus particularly on network security, as well as the enforcement and legal support that we will need to deliver this regime, which is a very important part of it.

It is also worth reflecting, though, that there are some really interesting overlaps between different areas of our new responsibilities. If I think of the responsibilities that we have just taken on in relation to video sharing platforms, we are having to understand, as part of those responsibilities, network infrastructure, data analytics and so on. All that actually calls on similar skills and experience that we will need for the regime that we are responsible for, in terms of the law. That is an important part of it.

Q124 Chi Onwurah: Thank you very much for sharing your expertise with us. As a previous employee of Ofcom, for six years, I am, not surprisingly, perhaps, a huge admirer of your work, and, to reflect what was implied by the hon. Member for Hyndburn, I think that Parliament will always benefit from increased telecoms expertise here.

I want, with permission, to ask a question about three areas: security, assets and costs, and duties. I share some of the scepticism of my right hon. Friend the Member for North Durham about the statement that Ofcom will not be making decisions on national security. You will clearly have duties with regard to national security and one of the key duties is to ensure compliance of our entire network—all our networks—with national security requirements. So how are you going to ensure that compliance without taking decisions on security? You seem to suggest that it is just going to be a set of protocols, if you like, from the National Cyber Security Centre, and you are just going to look at ticking the boxes to see that they are met; but in practice that cannot be the case. It is far more complex than that, particularly with regard to emerging technologies.

Another issue is that the Bill puts all the requirement to ensure compliance on Ofcom, in terms of Ofcom seeking information, Ofcom requiring information, Ofcom setting out notices to inspect, and so on. For example, let us say that one of our network operators—I shall not name one—decides to buy all its cloud or virtualisation equipment from a Chinese manufacturer that is not designated a high-risk manufacturer. Would Ofcom be informed of that change in its network? How would that pass to the National Cyber Security Centre—or would it not? Without that kind of duty in place, is there a risk of what you do becoming a meaningless tick-box exercise and, particularly, of its not addressing future and emerging security threats? That is my first question.

Lindsey Fussell: The point that you raise about this needing not to be a tick-box exercise is absolutely vital. I think actually what we are talking about in this legislation is changing culture—crucially among operators but also in terms of giving the regulator new responsibilities and changing the culture that we have, and the responsibilities and the range of the role we take on in relation to this. So this is absolutely— the legislation in fact specifically says so—about future technology as well as about existing networks. It is critical, I think, that we and the operators go on this journey together in terms of promoting that security by design, in everything that is done.

Picking up your question specifically in relation to assets, I think it is more or less impossible to meet the requirements set out in the covid practice for the operators unless they have a detailed asset register of everything that is in their system. We would expect to see evidence of that, and that it is regularly checked, audited and so on. That would be an expectation for us.

On the relationship with the NCSC, as I say, we have specific provisions in place that enable us to share information with the NCSC. As we collect that information with operators, we will discuss with them in advance what type of information they want to see on a routine basis, sharing that and clearly taking guidance from them as necessary if they think there are national security issues that we need to be aware of.

I mentioned earlier about having security clearance in place. To expand on that answer, we have a small number of STRAP-cleared staff in Ofcom, and we will expand that if need be. Those relationships with the NCSC are already in place and will be productive. I should say also that if the NCSC identifies new threats, or if we identify new threats, I think the legislation is flexible and it is right to be so, in that the code of practice can be updated to reflect that.

Simon Saunders: Could I also add that, in respect of our role in emerging technologies, we are not only awaiting others to tell us which emerging technologies to pay attention to? We have our own independent programme of monitoring and horizon scanning for technologies that could appear and have an impact on the networks and the sectors that we regulate. Clearly, the implications are not only about security. They cover a wider range of issues of performance and costs and flexibility and so on. We actively monitor across these sectors for those technologies.
I mentioned earlier that we recently published something about technologies heading for the future generations of mobile. That also covers fixed networks, the advent of quantum technologies and distributed software technologies in networks, and so on. That programme yields an advance look for colleagues about threats and opportunities that are coming towards us into the markets, so that we can build the skills and consider the implications well in advance of their actually impacting on those networks.

Q125 Chi Onwurah: How can you make that assessment without taking decisions about national security? If you are relying, as you seem to be saying, on the National Cyber Security Centre to make those decisions for you, how are you, or they, accountable to Parliament for that? There is a basic issue here, in that you feel that you are not responsible for national security. However, we do not see how that responsibility for national security is made accountable if you do not have any responsibility for it but you have responsibility for compliance. You have not answered my question as to how a change in the networks would be made known to you or the National Cyber Security Centre when there is no requirement for that at the moment, as far as I can see.

Lindsey Fussell: We would, as I say, expect providers to keep detailed records of the components that they use in their networks. I would expect that that is the type of information that, if a significant new vendor is brought into the market, the NCSC might well be interested in. It is worth saying that, while we do not have any direct regulatory powers over the vendors themselves, under these arrangements operators are required to assess the maturity of the vendors and suppliers they use, and the NCSC has issued guidance to them to enable them to assess that maturity. If the question is: if we see a brand new supplier starting to appear, is that the kind of information that we would expect operators to provide to us and for us then to share it with the NCSC? The answer to that question would be yes.

Q126 Chi Onwurah: With regard to asset registry and expectations of having that, having spent a significant amount of time looking in the back offices of operators as to what they have, I know that they are certainly not up to date. We have heard from other witnesses that they do not always have up-to-date and comprehensive asset registers. To rely on an expectation seems a low bar.

Can I come on to duties? I have the Communications Act here, which has got a lot thicker since I left Ofcom. The two duties are the “interests of citizens” and the “interests of consumers” with regard to competition, but there is not a duty on security. Does that not suggest that if there is a conflict between competition or communication matters, that will be prioritised over security if there is not an explicit duty to maintain the security of our networks?

Lindsey Fussell: I think this legislation quite clearly does place explicit duties on us to monitor and enforce the compliance of operators on network security requirements. I do not see that there is any risk that we would downplay the importance of that duty in comparison with others. Clearly, it is for the Government to put forward any changes to legislation to change the balance of our duties or to add new ones, but I think the Government—and, indeed, Parliament—are asking us very clearly to take on those responsibilities through this new legislation.

To pick up on a point I made earlier, in terms of the interests of citizens and consumers, it is important to say that of course it is in the interest of citizens and consumers to have excellent networks functioning that provide them with great connectivity. If we have learned anything from this most recent period, it is how important connectivity is to everybody’s daily life. Of course, that comes across in pricing and support for more vulnerable consumers, and all those other things that we have responsibility for in telecoms.

Actually, promoting secure networks is absolutely in the interests of consumers and citizens as well, not just because of the really damaging consequences of cyber-attacks, but because, ultimately, if we are able to have better networks, that should enable greater economic innovation through 5G use cases and things like that, for example. I think in promoting the interests of citizens and consumers, telecoms security is clearly part of that.

Q127 James Sunderland: The Bill provides powers to fine vendors up to 10% of their annual turnover or up to £100,000 per day for failing to meet standards. Could I ask for your view, please, on how that compares internationally, and whether you feel that that is appropriate?

Lindsey Fussell: It is probably worth saying that, from an international perspective, although there are some other countries—notably Germany and Australia—that have started to explore strengthening their telecoms security framework, I am not aware of another country that is quite as forward leaning in terms of the framework that is being put forward in this legislation.

In terms of the fines, this is an important point—those fines match the level that we are currently able to levy in relation to our other telecoms requirements, such as breaches of our general conditions. Previously, under our past responsibilities, our fines were limited to £2 million, so really quite a small amount compared with the wealth of the largest operators. I think it is appropriate that the telecoms security fines match what we are able to do elsewhere.

The final point I would make is that fining is an incredibly useful power to have because it acts as a significant deterrent and a strong incentive for companies to comply. It is actually not the first lever that we reach for, certainly not maximum fines; it is there and we are ready to use it if we need to, but our starting point would be to work with operators on this journey as they move towards compliance as they respond to new and emerging threats.

Q128 Matt Warman: Thank you for all the work you have done on this matter so far. I wonder if you could just say a little bit more about the responsibilities that Ofcom has had, as you put it, since 2011 on telecoms security. I think that perhaps the extent of that is not as well understood as it could be.

Lindsey Fussell: Yes, of course, I am very happy to do that. As you say, we have responsibility now to monitor and enforce compliance on security. The difference, which is why I think this legislation is so welcome, is that at present we do not have any obligations set out as to how operators need to meet those security requirements. It has been basically up to them to decide what is
necessary. While many companies have invested very heavily in their security—I would not want to suggest otherwise—clearly there is a journey to go on and improvements that need to be made. It is very welcome that we now have this much clearer framework, so that operators know what they need to do and we can enforce against it.

The other point that is worth bringing out is that, at present, operators are under a requirement to report incidents to us, but the nature of that reporting tends to be around incidents that cause outages. We do get a lot of those—caused not just by cyber-security but by wind, weather and other issues. Quite a lot of cyber-security incidents are, frankly, precisely designed not to cause outages, because it is in the interests of the malicious actor to allow the network to keep operating while they do whatever they are up to. The new requirements on operators are to tell us not just if there is an outage but if there is an incident where they believe their system may have been compromised. They are wider ranging and welcome powers.

Q129 Matt Warman: I think you are also aware that this legislation is backed up by a number of statutory instruments to give further powers.

Lindsey Fussell: Absolutely.

Q130 Matt Warman: Would you like to give an assessment of whether you think that is sufficient to address the concerns around, for instance, asset registers, which we have talked about before?

Lindsey Fussell: Yes, so the way the legislation works, as you say, is that there is a primary duty on operators to promote security of their networks, and on us to enforce and monitor compliance against that. My understanding is that the secondary legislation will set out around 40 to 50 sub-duties on operators, which they will all need to meet—that is all operators and providers of electronic communications services.

Underpinning that, each of those sub-duties will be reflected in the code of practice, setting out the details of what the operators need to do to meet each of those sub-duties. As I explained earlier in relation to the questions we discussed on national security, we are entitled, as the regulator, to place quite a lot of weight on the national security judgments that the NCSC and the Government have made in drawing up both those sub-duties in the code of practice, in responding to the threats identified.

The Chair: Any other questions from Members?

Q131 Chi Onwurah: A word on costs, perhaps. You said in your opening statement that you expected it to cost about £6 million to £7 million for Ofcom. How will those costs be funded or raised? In terms of costs on operators, clearly a requirement to do a complete asset register, for example, could be a very significant cost for an operator. What kind of costs do you see? Do you see limits being placed on the costs that operators could incur in complying with Ofcom demands or requests?

Lindsey Fussell: In relation to Ofcom’s costs first, Ofcom is funded in two ways: first, by a levy on the sectors and companies that it regulates and, secondly, through the collection of fees, primarily from our spectrum duties. Our overall funding is obviously agreed by our board but also subject to a cap agreed with Government each year. We are currently in discussion with the Treasury about the exact technicalities and which of those routes will be used to fund this, but it will be in line with Ofcom’s normal funding arrangements.

In relation to company costs, clearly the Government have looked into that, in discussion with operators in relation to the impact assessment for the legislation. I know that there is a plan to do further work on that in relation to telecom security requirements, once companies have had a chance to see the SI and the code of practice.

The point here, which is built into the legislation, is the concept of proportionality. Although we would expect the largest operators—we would work with them intensively throughout the process—to take part in, for example, penetration testing, it is likely we will be more proportionate with the smaller operators and, for example, respond on an incident-based approach, rather than expect them to carry out the same level of detailed work and interaction with Ofcom. In all of that, we would want to be proportionate in the costs imposed on operators, as we are in all our responsibilities, bearing in mind that these are really important responsibilities, as we have been discussing.

Q132 Chi Onwurah: Could you therefore confirm that the costs will be in line with the size of the operator, so small start-ups will not be expected to pay the same as Vodafone, for example? We have not talked at all about the diversification strategy, yet there is agreement that we cannot have secure networks without effective diversification of the supply chain. Are you in a position to monitor the diversification of operator supply chains, and is that something you would expect to be doing?

Lindsey Fussell: If I may, I will bring Simon in on the question of diversification. In relation to costs, the bulk of Ofcom’s own costs are paid by larger operators rather than smaller ones, and we have talked about proportionality in the way we operate that. Again, although I understand the tiering of the system will be set out in the code of practice, that will also be based on size and scale. Simon, may I turn to you on diversification?

Simon Saunders: The diversification strategy that the Government have published has set out a desire to attract new suppliers to the UK and further expand suppliers through open solutions, among other means, and to ensure that that is supported by an appropriate regulatory framework. We are ready to do what comes from that, in terms of any objectives the Government set on the level of diversification and to support measures to enable that. There are clearly synergies between the security aspects and the diversification aspects: in determining how diverse the supply base is, having a fully populated and up-to-date asset register from the operators for the security needs will also support the requirement to assess the diversity, if that is what we are required to do.

Q133 Chi Onwurah: But currently your duties are all to do with the stick, in terms of the enforcement of security requirements, and nothing to do with diversification or the incentives for that?

Simon Saunders: Our existing duties around ensuring the health of the communications market for consumers and citizens point in the same direction in many ways, even if diversity is not spelled out explicitly. We see that a functioning, competitive market for network equipment supports the operators’ ability to provide cost-effective
networks that perform well, and that supports the needs of citizens to get great services wherever they are and for those services to be reliable and so on. I do not view this as an entirely separate area from our existing duties; whether specific duties around this are needed is part of the work we are doing to support the taskforce and the plans that come from that.

**The Chair:** This will have to be a very quick answer, because we have to stop at 11.25 am.

**Q134 Mr Jones:** You have said that you will take advice from the National Cyber Security Centre. What happens if you disagree with its advice? Who takes the final decision on what is national security?

**Lindsey Fussell:** I think that the National Cyber Security Centre takes the decision on national security. Of course, the Government ultimately have the power for that but on the advice of the NCSC. Decisions on enforcement and compliance are for Ofcom, following the code of practice that the NCSC has created for the Government.

**Q135 Mr Jones:** Yes, but what happens if you disagree with it?

**Lindsey Fussell:** Sorry, I had some feedback there; I was having trouble hearing you. Is the question what would happen if we disagreed with the advice given to us by the NCSC on national security?

**Mr Jones:** Yes.

**Lindsey Fussell:** I think in that case we would take the guidance of the NCSC. In practice, I really don’t think that is likely to occur. Ultimately, the final decision on whether an operator has complied and whether we enforce is with us. The NCSC would not be able to overrule that decision, but we would be taking that decision in the light of the information we would have been given from NCSC about what is required to meet national security.

**Q136 Mr Jones:** May I suggest that you read the Intelligence and Security Committee’s report from 2013 on critical national infrastructure, because exactly that happened when a Department overruled the Security Service? I think you will find yourselves in a similarly sad position with this legislation.

**Lindsey Fussell:** I have read that report, thank you.

**The Chair:** Thank you very much indeed to our two witnesses. We are very grateful to both of you for your time this morning and for the expertise you have shared with us.

11.25 am

*The Chair adjourned the Committee without Question put (Standing Order No. 88).*

*Adjourned till this day at Two o’clock.*
PUBLIC BILL COMMITTEE

TELECOMMUNICATIONS (SECURITY) BILL

Fourth Sitting
Tuesday 19 January 2021
(Afternoon)

CONTENTS

Examination of witnesses.
Adjourned till Thursday 21 January at half-past Eleven 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

Saturday 23 January 2021
The Committee consisted of the following Members:

**Chairs: MR PHILIP HOLLOBONE, † STEVE MCCABE**

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

† attended the Committee

**Witnesses**

Dr Andy G Sellars, Strategic Development Director, Catapult Compound Semiconductor Applications

Dr Nick Johnson, Independent consultant

Heba Bevan OBE, CEO, Utterberry

Helen Duncan, Managing Director, MWE Media

Mike Fake, Director and Co-founder, Lumenisity

Dr David Cleevely CBE, Independent investor in many telecoms companies

Doug Brake, Director of Broadband and Spectrum Policy, Information Technology and Innovation Foundation
2.1 pm

The Chair: Good afternoon. We come to our fourth panel of witnesses today, consisting of Dr Andy G. Sellars, Dr Nick Johnson and Heba Bevan OBE. We have until 2.45 pm for this session. I will ask the witnesses to introduce themselves for the record, starting with Dr Sellars.

Dr Sellars: Good afternoon, Committee. I am Dr Andy Sellars and I am the strategic development director with the Compound Semiconductor Applications Catapult. We are a non-profit research and technology organisation that helps UK companies to exploit new technologies, predominantly for electric vehicles, quantum technologies and advanced telecom products. I look forward to answering and helping the Committee with their inquiry.

Heba Bevan: Good afternoon, and thank you very much for having me. My name is Heba Bevan, and I am the CEO and founder of Utterberry Ltd. We are a company that deals with artificial intelligence and very heavily with wireless sensor networks or internet of things solutions. We provide our solutions to major companies such as BT; the hardware community could work on: the communication aspect, which is probably provided by companies such as Airtel, and the cyber-security and encryption element of that infrastructure.

Dr Johnson: Good afternoon. My name is Nick Johnson, and until a month ago I was chief technical officer of ip.access, a UK-based small cell vendor that was bought in September last year by Mavenir—I think you guys interviewed Mavenir on Thursday—but I left at the beginning of this month, so I am now independent. I just want to stress that, on the connection with Mavenir, I am truly independent; I am not speaking for Mavenir in any sense at the moment.

I think ip.access came up a couple of times in the conversations with Mavenir last week, but we are a small cell radio access network vendor, a RAN specialist for cellular technology, global system for mobile communications, 3G and long-term evolution, and to some extent 5G. We are deployed in many networks. Historically, over the 20-year life of the company, we have been deployed in more than 100 networks worldwide, and are probably active in a little more than 50 of them.

Those networks include T-Mobile in the US, AT&T in the US, Airtel in India, BT One Phone in the UK and others of that sort. Those are my credentials.

Q137 Dean Russell (Watford) (Con): As you know, there are very many benefits to a 5G network in terms of the speed, application development and the new era that it can bring, but would you mind focusing for a moment on the new security risks that 5G will also bring, please?

Dr Sellars: You are quite right that 5G opens up a whole load of new benefits, predominantly high-speed access/lower latency. I think some of the security risks are around who is providing the infrastructure to support 5G. The concern that we have at the moment is that we need to have security of supply—both resilience of the supply chain for that infrastructure, and the cyber-security and encryption element of that infrastructure.

I think it is fair to say that 5G is likely to support a much broader selection of services. It is likely to have an impact on commercial, governmental and security transmission, just because of the widespread access and its very high-speed capability. It is also likely to support a very large number of internet of things devices—the sort of devices that UtterBerry develops. Some of those devices are another potential attack vector, if you like; they are another potential vulnerability. It is broadening the access into the network, which is potentially opening up new sorts of vulnerabilities that we need to take into consideration.

Dr Johnson: Let me start by saying that some aspects of security in 5G networks are actually much more secure than in previous generations. Looking over the lifetime of cellular, you will know that you could just listen into first generation analogue networks with a very high frequency radio. GSM—the global system for mobile communications—was secure, partly at least. The network and the phones would authenticate to each other, but only asymmetrically, so the phone could be captured by a surreptitious network. That sort of attack is still used.

3G is much more secure, with symmetric authentication. It is harder for devices to be captured by the wrong network, but it is still possible. It is also possible for the IMSI—that is to say, the international mobile subscriber identity—of an individual or group to be found from that network. The same is true of 4G. In 5G, that is much more difficult. In terms of the security of the user of the network, 5G has tightened up a lot of the loopholes in previous generations in a way that is very hard to unpick. That creates tactical problems for some law enforcement agencies, which rely on some of the insecurities of earlier generations to do their job.

From the network side of things, there are some issues. There is a new network model in terms of the way nodes are connected in the core network. No longer are there physical interfaces as in previous generations of network, where there would be an S1 connection from the base station to the core. There are still connections, but they are much more in a publish-subscribe-type model. I think those, conceivably at least, bring a little more opportunity for attackers to probe nodes within the core network to find weaknesses and vulnerabilities. That is my take on 5G.

Heba Bevan: We have three elements that the telecoms community could work on: the communication aspect, which is provided by companies such as BT; the hardware aspect, which is probably provided by companies such as Utterberry; and the software element within the system. So there are three types of vulnerability that...
could be introduced in the path of these three elements. The only problem with these paths is this: who is responsible if there is an attack? Usually, the communication aspect is the most important part to get protected.

Currently with 5G, there is a huge opportunity for opening up a huge economic impact from the sector in terms of healthcare, education and tech industries. These industries will need to move on and having 5G is definitely an important element, but how can we make sure it is secure in providing an effective communications network that provides an end-to-end solution and security? That is where I think we need to concentrate on the telecommunications and how can we make sure that what we are getting from that communication is totally secure, and that the encryption within it passes certain thresholds.

We can follow a certain standard within the hardware and software, but if the network is weak and has not provided us with good reliability, that is where things could be broken.

Q138 Christian Matheson (City of Chester) (Lab): Thank you for those answers. I have just a couple of questions. First of all, following on from Mr Russell’s question, the impression I get—I am not an expert—is of a network that is a bit like a bowl of spaghetti. There are bits here, there and everywhere. and there are bits of different generations that are all added on. How easy would it be from your point of view, with your different areas of expertise, to audit and identify within any part of that chain in the network exactly where there is equipment—hardware, software, chips or whatever—that perhaps needs to be removed or checked?

Is there a shelf-life of the older versions? I am surprised that we are still talking about 2G—that it has not been removed. Is there a shelf-life for those elements and will they be removed from what I term “the network”, which is of course the whole global telecommunications infrastructure of the UK? Nick, do you want to start on this question?

Dr Johnson: Yes. Let me start on that shelf-life question. GSM is a little bit like Radio Four longwave, right? I do not think that it is ever really going to die: there are just too many people who depend on it for one reason or another, whether that is for emergency calls, or just for coverage in remote locations or wherever. I think GSM will stay there forever, despite its security issues. They are well known and understood, and managed in due course.

The shelf-life of network components is an interesting aspect. Our experience of deploying into cellular networks is that there is always a security audit involved. When we take a piece of equipment into a new operator, there is always a hurdle to be overcome. They have their own audit procedures and those include a sort of paper audit, where they look at the particular software components that the software is built from, some of which we build ourselves, some of which is open source and some of which is commercial off-the-shelf software libraries and so on. They want to make sure that those are all up to date and properly patched, with all the latest security patches and so on. I think that will just continue on. To some extent, that is just the baseline hurdle.

I am not sure this is exactly what you are asking, but what has changed in my mind as we go forward is this idea that there can be software in the network that is not so much interested in security—as in, somebody hacking into it—but is more of a Trojan horse type of software, completely undetectable until some signal or some date comes by and it springs to life and does bad things. The example I have in mind is the SolarWinds example from December last year, where software had been inserted in the supply chain and had been sitting there quite happily for a while. That, to my mind, is very difficult to detect. Until it goes off, you do not know there is a bomb inside it, and that is an issue.

Coming back to the shelf-life question, keeping the software up to date is a major issue. It sounds easy, but practically speaking, I know it is an operational dialogue all the time within vendor businesses: they are striving for revenue from new customers, for new features to be added, and that is acting against updating the software libraries and so on to bring them up to date. There is a continual dialogue in every vendor company to ask, “Do we need these features to get more revenue, or do we need to update these libraries because we need to maintain secure software?” I guess to some extent, the whole reason for this Bill is to try and force that to the front of the conversation; to say, “Look, you can’t go on. That dialogue has to stop now. The software needs to be secure.” That has to be the baseline, it has to be a basic hygiene factor in selling software that it must be secure to a certain level, and the features need to come as value added. If you have some questions coming up on the code of practice, designated vendors and so on, we might talk about that, but those are my comments on shelf-life.

I think I missed your first question. I apologise.

Q139 Christian Matheson: No, that is grand. Heba or Andy, do you want to add anything to that?

Dr Sellers: I can add a little bit. Your question about auditing systems is very pertinent to the experience we went through at the end of the 1990s with the Y2K bug. Lots of companies were required to do an audit: financial institutions, companies using software-driven automation, were required to do an audit of their systems in response to that threat. It would probably be a fairly similar exercise for telecoms. I am sure they must have a register of the equipment they use.

Nick has made all the points about software shelf-life, but from a hardware point of view, there is a capacity that the hardware can deliver. My understanding is that as they put in a new service such as 5G, it is quite often built on existing infrastructure such as 4G and 3G. Clearly, each piece of hardware has a bandwidth and can support a certain amount of data throughput, so in terms of shelf-life, I would argue that it is mostly capacity-related. I do not think there are any major concerns about things wearing out as such from a hardware perspective.

Q140 Christian Matheson: Heba, did you want to add anything?

Heba Bevan: If we are auditing basically hardware, it becomes very difficult. You can audit maybe 10 main base stations, 20 or even 100, but every single one of them is quite hard and intensive, and it might also be locking to a certain competition in who the supplier is. If you are getting it from one supplier, you are able to audit that supplier, but if you are getting it from multiple suppliers, how would you audit every single supplier? Would you go 10%, or 20%?
The other thing I would like to highlight is that back in early 2018, Intel had a problem with the security of one of its chips. I can provide written evidence later on to give you the full details on that. One of their chips, as well as AMD and Arm, had a problem, and they knew about it, but it has not been fixed. The problem is that if you put it out there into the community, it becomes a major threat, and a bigger threat.

In terms of hardware, as long as it is supported, maintained and updated on a regular basis, its shelf life will be built to a certain recognised standard. However, if it has not been built to a certain recognised standard and it has not been tested and maintained yearly, it will come to an end very quickly and will need to be replaced. We have a huge problem with a lot of networking in smaller areas and bigger areas in the UK. Some of the areas have an amazing network and speed, and some of them are very bad and are actually degrading. We can see that even in education. Schools currently rely on these networks to have Zooms and Teams meetings, as well as normal meetings. Some areas have not been maintained as other areas in the UK have. Maintaining and auditing them is bound up with the maintenance and making sure that, whoever the supplier is, they maintain the system on a regular basis, update the software and keep a track on that.

**The Chair:** I am sure Members would appreciate further details on the Intel example, if you can provide that.

**Q141 David Johnston (Wantage) (Con):** Can I ask about the diversification strategy, which is a question I asked some of the other witnesses? The Government are rightly investing a significant amount in this. We all agree that it is needed. What do you think success looks like? Our problem at the moment is that if we take out Huawei, we have only two vendors we can use. What range would you like to see, and in what sort of timeframe?

**Heba Bevan:** The problem with Huawei is a bigger problem. The technology was freely created by BT and got sold to Huawei. I think that such an important technology should not have been allowed to be sold in the first place. I am sorry; this is my personal view, not a technical view. I think there is a problem with the technology. We have only two vendors we can use. What range would you like to see, and in what sort of timeframe?

**Heba Bevan:** The problem with Huawei is a bigger problem. The technology was freely created by BT and got sold to Huawei. I think that such an important technology should not have been allowed to be sold in the first place. I am sorry; this is my personal view, not a technical view. I think there is a problem with the technology. We have only two vendors we can use. What range would you like to see, and in what sort of timeframe?

**The Chair:** I am sure Members would appreciate further details on the Intel example, if you can provide that.

**Q141 David Johnston (Wantage) (Con):** Can I ask about the diversification strategy, which is a question I asked some of the other witnesses? The Government are rightly investing a significant amount in this. We all agree that it is needed. What do you think success looks like? Our problem at the moment is that if we take out Huawei, we have only two vendors we can use. What range would you like to see, and in what sort of timeframe?

**Heba Bevan:** The problem with Huawei is a bigger problem. The technology was freely created by BT and got sold to Huawei. I think that such an important technology should not have been allowed to be sold in the first place. I am sorry; this is my personal view, not a technical view. I think there is a problem with the technology. We have only two vendors we can use. What range would you like to see, and in what sort of timeframe?

**Heba Bevan:** The problem with Huawei is a bigger problem. The technology was freely created by BT and got sold to Huawei. I think that such an important technology should not have been allowed to be sold in the first place. I am sorry; this is my personal view, not a technical view. I think there is a problem with the technology. We have only two vendors we can use. What range would you like to see, and in what sort of timeframe?

**The Chair:** I am sure Members would appreciate further details on the Intel example, if you can provide that.

**Q141 David Johnston (Wantage) (Con):** Can I ask about the diversification strategy, which is a question I asked some of the other witnesses? The Government are rightly investing a significant amount in this. We all agree that it is needed. What do you think success looks like? Our problem at the moment is that if we take out Huawei, we have only two vendors we can use. What range would you like to see, and in what sort of timeframe?

**Heba Bevan:** The problem with Huawei is a bigger problem. The technology was freely created by BT and got sold to Huawei. I think that such an important technology should not have been allowed to be sold in the first place. I am sorry; this is my personal view, not a technical view. I think there is a problem with the technology. We have only two vendors we can use. What range would you like to see, and in what sort of timeframe?

**The Chair:** I am sure Members would appreciate further details on the Intel example, if you can provide that.

**Q141 David Johnston (Wantage) (Con):** Can I ask about the diversification strategy, which is a question I asked some of the other witnesses? The Government are rightly investing a significant amount in this. We all agree that it is needed. What do you think success looks like? Our problem at the moment is that if we take out Huawei, we have only two vendors we can use. What range would you like to see, and in what sort of timeframe?

**Heba Bevan:** The problem with Huawei is a bigger problem. The technology was freely created by BT and got sold to Huawei. I think that such an important technology should not have been allowed to be sold in the first place. I am sorry; this is my personal view, not a technical view. I think there is a problem with the technology. We have only two vendors we can use. What range would you like to see, and in what sort of timeframe?

**The Chair:** I am sure Members would appreciate further details on the Intel example, if you can provide that.

**Q141 David Johnston (Wantage) (Con):** Can I ask about the diversification strategy, which is a question I asked some of the other witnesses? The Government are rightly investing a significant amount in this. We all agree that it is needed. What do you think success looks like? Our problem at the moment is that if we take out Huawei, we have only two vendors we can use. What range would you like to see, and in what sort of timeframe?

**Heba Bevan:** The problem with Huawei is a bigger problem. The technology was freely created by BT and got sold to Huawei. I think that such an important technology should not have been allowed to be sold in the first place. I am sorry; this is my personal view, not a technical view. I think there is a problem with the technology. We have only two vendors we can use. What range would you like to see, and in what sort of timeframe?

**The Chair:** I am sure Members would appreciate further details on the Intel example, if you can provide that.

**Q141 David Johnston (Wantage) (Con):** Can I ask about the diversification strategy, which is a question I asked some of the other witnesses? The Government are rightly investing a significant amount in this. We all agree that it is needed. What do you think success looks like? Our problem at the moment is that if we take out Huawei, we have only two vendors we can use. What range would you like to see, and in what sort of timeframe?

**Heba Bevan:** The problem with Huawei is a bigger problem. The technology was freely created by BT and got sold to Huawei. I think that such an important technology should not have been allowed to be sold in the first place. I am sorry; this is my personal view, not a technical view. I think there is a problem with the technology. We have only two vendors we can use. What range would you like to see, and in what sort of timeframe?

**The Chair:** I am sure Members would appreciate further details on the Intel example, if you can provide that.

**Q141 David Johnston (Wantage) (Con):** Can I ask about the diversification strategy, which is a question I asked some of the other witnesses? The Government are rightly investing a significant amount in this. We all agree that it is needed. What do you think success looks like? Our problem at the moment is that if we take out Huawei, we have only two vendors we can use. What range would you like to see, and in what sort of timeframe?

**Heba Bevan:** The problem with Huawei is a bigger problem. The technology was freely created by BT and got sold to Huawei. I think that such an important technology should not have been allowed to be sold in the first place. I am sorry; this is my personal view, not a technical view. I think there is a problem with the technology. We have only two vendors we can use. What range would you like to see, and in what sort of timeframe?

**The Chair:** I am sure Members would appreciate further details on the Intel example, if you can provide that.

**Q141 David Johnston (Wantage) (Con):** Can I ask about the diversification strategy, which is a question I asked some of the other witnesses? The Government are rightly investing a significant amount in this. We all agree that it is needed. What do you think success looks like? Our problem at the moment is that if we take out Huawei, we have only two vendors we can use. What range would you like to see, and in what sort of timeframe?

**Heba Bevan:** The problem with Huawei is a bigger problem. The technology was freely created by BT and got sold to Huawei. I think that such an important technology should not have been allowed to be sold in the first place. I am sorry; this is my personal view, not a technical view. I think there is a problem with the technology. We have only two vendors we can use. What range would you like to see, and in what sort of timeframe?

**The Chair:** I am sure Members would appreciate further details on the Intel example, if you can provide that.

**Q141 David Johnston (Wantage) (Con):** Can I ask about the diversification strategy, which is a question I asked some of the other witnesses? The Government are rightly investing a significant amount in this. We all agree that it is needed. What do you think success looks like? Our problem at the moment is that if we take out Huawei, we have only two vendors we can use. What range would you like to see, and in what sort of timeframe?

**Heba Bevan:** The problem with Huawei is a bigger problem. The technology was freely created by BT and got sold to Huawei. I think that such an important technology should not have been allowed to be sold in the first place. I am sorry; this is my personal view, not a technical view. I think there is a problem with the technology. We have only two vendors we can use. What range would you like to see, and in what sort of timeframe?

**The Chair:** I am sure Members would appreciate further details on the Intel example, if you can provide that.

**Q141 David Johnston (Wantage) (Con):** Can I ask about the diversification strategy, which is a question I asked some of the other witnesses? The Government are rightly investing a significant amount in this. We all agree that it is needed. What do you think success looks like? Our problem at the moment is that if we take out Huawei, we have only two vendors we can use. What range would you like to see, and in what sort of timeframe?
My background is similar to Heba’s. I am an electronic engineer by trade. I have designed electronic systems that have been manufactured in the UK and I have written software to drive those systems. In the UK, we have something like 5,000 companies that design and manufacture electronic systems. Something like 600 of them are involved in telecoms. I am not suggesting that all of those 600 become equal players. That would be a crazy scenario. But there are certainly some parts of the telecom network where the UK is pre-eminent. There are some backhaul and fibre technologies that we are very good at. As we deploy 5G into rural communities, that is likely to require low Earth orbit satellites; we are very good at satellite communications.

We have clusters of activity with these things around the UK. There is a cluster of radio frequency, backhaul and satellite communications in the north-east, and of satellite manufacturing in the central belt of Scotland. We have clusters of activity in the Western Gateway and around small-cell base stations. In south Wales, we have clusters of activity in compound semiconductors, which are the next generation of chips required for 5G and other high-data rate communications. So, I think the diversification strategy goals of opening up and disaggregating the markets are certainly going in the right direction.

Ultimately, it comes to the telecom operators and how many suppliers they would like in their vendor supply chain. If we can disaggregate the network and come up with open standards for various parts of the network, such as open RAN and backhaul network gateways, that opens the playing fields and enables companies to compete equally. As I say, there are a number of UK companies that could compete. They are globally competitive and could compete on equal grounds with other companies to get access to those markets.

In terms of the timescale to do this, at the moment we have three monolithic suppliers and we are going down to two. Patching that scenario feels like a very short-term timescale, but I would indicate that a broader diversification would probably be in the order of three to five years.

The Chair: Thank you. I want to try to squeeze in both Sara Britcliffe and Chris Matheson before we go the Minister and the shadow Minister, so we need short questions and succinct answers.

Q143 Sara Britcliffe (Hyndburn) (Con): Mine is quite a simple question: what do you support in the Bill? Can I come to you first, Nick?

Dr Johnson: I think broadly the Bill is okay. I have a couple of questions about the wording. The definition of a security compromise is too narrow. At the same time, the first clause would cover every single bug in every single system, regardless of whether they were to do with security or not. Does it affect availability, performance or functionality? Every bug on the planet would qualify for that. The Bill does not cover the issue of prepositioned viruses that are implanted in software, which are crucial to the next phase of network security, but it broadly makes sense.

I have one other comment around the designated vendors. What do the friends of the Bill think about a designated technology register? Designated vendors are all very well, but the technology that is being incorporated into telecoms networks is itself subject to security concerns. Should such a register of the specific technology generations or of particular operating systems and libraries, which are known to be buggy or compromised from a security point of view, be included in the Bill? It might be too late in the day for that, but I guess some of this will be picked up by the NCSC.

The Chair: I am sorry to interrupt, but I want to move on to Heba Bevan. The question was, what is there in the Bill that you really approve of?

Heba Bevan: One of the things in the Bill that, to me, is essential is that whoever is providing the telecommunications system has to be liable for providing the security on it. I totally agree on that. They have to make sure it is secure. There are a few bits and pieces on how that is being achieved but, because of time, I can send you a few points around that.

The Chair: That would be helpful, thank you.

Dr Sellass: I agree with the points made by the other two witnesses.

Q144 Christian Matheson: Thank you for squeezing me in, Mr McCabe. I will direct this question to Ms Bevan; it should really be directed to the Minister, but unfortunately procedure does not allow that. There is a quote on the UtterBerry website:

“I am delighted UtterBerry has been selected as a champion of British technology excellence through the TechHub programme—just one of the new initiatives we have launched in partnership with industry and the Chinese government.”

That is from Sherry Madera, the deputy director general of the Department of International Trade at the British Embassy in China. Are our firms still being pushed to share communications technology with China as this Bill is going through?

Heba Bevan: No, we worked with the Department of International Trade in 2016. The Chongqing Government were interested in having UtterBerry there. We spoke with our lawyers about the amount of IP we have and decided that we would not pursue this. We do not manufacture anything in China. Everything in UtterBerry is manufactured in the UK—software, hardware and everything we do. We mainly have graduates from the UK. We have European engineers, but recruitment is mainly kept closer, because of the IP sensitivity.

The Chair: Thank you for clearing that up. Chi Onwurah.

Q145 Chi Onwurah (Newcastle upon Tyne Central) (Lab): It is a pleasure to serve under your chairmanship, Mr McCabe.

I will be brief, as we are running out of time, but thank you for your expertise. My question to Andy Sellass and Heba Bevan is about the diversification strategy. In what areas do you think the UK has the capability to exploit the opportunities of this diversification strategy, particularly in hardware versus software? We have been told that hardware is beyond our manufacturing capabilities, yet you seem to be making a success out of it, Heba. What barriers are new entrants and smaller companies likely to experience and what kind of interventions should the Government make that are not fully addressed by the diversification strategy in order to ensure a UK capability in this area?
Q146 Chi Onwurah: What interventions would support them?

Dr Sellars: For interventions, I would suggest that the Advanced Propulsion Centre is a really good model to look at. It is in a different sector. It is funded through the Department for Business, Energy and Industrial Strategy, and its remit is to help to transition the automotive industry from petrol and diesel engines to electric drivetrains using batteries. Have a look at that as a model. It is an incredibly good model for transitioning an entire industry from one technology to another. It brings together supply chains and is very effective. That is one of the interventions I would suggest. Other interventions could be cyber-certification and just helping UK companies to access some of the standards bodies. That would be very effective. We have a lot of SMEs.

Heba Bevan: Thank you for your question. On hardware, as a company—and to be honest in the UK as a nation—we do not have the essential foundries. We can design and prototype the silicon, and we can work on, from the beginning, how actually it would work, but the actual manufacturing of the chip—not the hardware: that one chip which is like the CPU or a piece of DSP—those actually require very high-intensity foundries. If we want to build them in the UK it will cost around £10 billion today—probably over that number. Andy can correct me on that.

In the far east, they have unlimited resources with the state aid rule; and Europe, in the last few years, passed something, for the state aid rule, called IPCEI, which is important projects of common European interest. Germany was able to fund €1.2 billion from its money to support these foundries. France put in €0.8 billion, and Holland put in €0.4 billion. In the UK in the last few years, in terms of building these foundries, the UK has not supported that type of manufacturing. In chip manufacturing, we do not. However, on the hardware scale we are able. The way we see it, we build the hardware; we build the software—but the actual components and the chips, today we do not have the capabilities in the UK to manufacture that.

The Chair: I am really sorry to do this to you, but I think I had better interrupt and go to the Minister or we will run out of time completely.

Q147 The Parliamentary Under-Secretary of State for Digital, Culture, Media and Sport (Matt Warman): Thank you, Mr McCabe, and thank you to all the witnesses, and particularly Dr Sellars for the map of UK brilliance, which is really appreciated. In short—given that we have four minutes—we have £250 million of this diversification funding to spend over the next three years or so. My question to you three is simply how you would spend it. Thirty seconds each: 250 million quid.

Dr Sellars: I would prioritise the funding in terms of where the vulnerabilities are in the network, in terms of the ability of the UK to fulfil those vulnerabilities and in terms of what markets it would open up. There are specific parts in the telecoms stack that are likely to be more vulnerable than others, where the UK has prime capability and where we could then develop an export opportunity. I can provide some more detailed answers in writing if that is helpful.

Dr Johnson: For my 30 seconds I would spend it on basic research, cementing the intellectual property position of the UK.

Heba Bevan: I would agree with Dr Sellars—Andy: we need to increase the amount of spending around vulnerability and strengthening the network. One other point is about spending it on areas outside the UK so it would generate more jobs around the north.

The Chair: Chi, I think you had something outstanding, and you have got just about a minute and a bit to do it.

Q148 Chi Onwurah: It was a question to Dr Sellars with regard to open RAN maturity as an IP.

Dr Johnson: So, the 45-second answer: Mavenir is using IP access GSM 3G technology in its open RAN development. Pardeep, I think, said that it would be ready within 12 months, and I agree that that is a true statement.

The Chair: Did you have anything else, Minister?

Matt Warman: Not that we can do in 90 seconds.

The Chair: I am sorry we had to hurry you a bit, there, but we are trying to get through quite a lot this afternoon. Can I just thank all our witnesses for your evidence and the extra bits that you said you would possibly forward to us. That would be much appreciated. Thank you, on behalf of the Committee. That brings this session to a close.

Examination of Witnesses

Dr David Cleevely, Helen Duncan and Mike Fake gave evidence.

2.44 pm

Q149 The Chair: We move on immediately to the fifth panel. We are going to hear now from Helen Duncan, who is the managing director of MWE Media, and Mike Fake—have I pronounced your name correctly?

Mike Fake: It is Mike Fake, as in genuine.

Q150 The Chair: I apologise. I have got it now; that is very clear. It was kind of you to clear it up for me. Mike Fake, director and co-founder of Lumenisity, and Dr David Cleevely CBE, who is an independent investor in several telecommunications companies. We have until 3.30 pm for this session. Could we start with Helen Duncan? I ask you to introduce yourself for the record.
Prior to that, I was a practising engineer in the high-frequency electronics industry. I have been writing about this industry for the past 30 years.

I am director and co-founder of Lumenisity, and I have spent the past 30 years in telecoms fibre optic components.

Lumenisity is a spin-out from the University of Southampton, and we have developed a new fibre optic cable technology, in which data travels 50% faster than in a conventional cable, which would digitally shrink the UK; provide a more responsive internet; increase the physical separation of data centres, moving them out of big conurbations; and potentially reduce the cost of deploying 5G. We are building a company to engineer telecoms solutions and innovatively scale up the manufacturing base in the UK.

Our opening statement is that we support the principles of the telecoms security Bill. We see the diversification strategy as critical for successful execution. It is a real opportunity to build a secure, UK-leading network, fostering new entrants and technologies in the UK telecoms supply chain, and to leverage innovative solutions in manufacturing scale in the UK.

A challenge for SMEs, which I would like to highlight, is ensuring sufficient scale-up investment. This is an expensive step and it is difficult to raise this level of capital independently, so we need a combination of public and private funding. Lumenisity is part of an overall eco-system to improve the UK competitive position in a growing next-generation economy. In summary, we would like to see this as an opportunity for a positive change, rather than a retrospective solution to a singular problem.

**Dr Cleevely:** My name is David Cleevely. As you have pointed out, I have invested in a number of telecoms companies and sold a few of them successfully. I have been an adviser to the Government and Ofcom. I was one of the experts who helped with the Communications Act 2003. To ensure I have full disclosure, I was on one of the boards of the MOD for eight years, looking after our ICT for all of defence, in theatre and the back office.

If I may, I would like to make three points very briefly. First, I would like to explore perhaps outside of this Committee a little bit more the edge cases for what constitutes a telecommunications network. Although provisions in the 2003 Act, sections 125 to 128 or so, cover quite a lot of things that are extended in this Bill, I think we need to think rather more carefully about what a telecommunications network actually is, in a world where many of these things are distributed, both in hardware and software.

The second point I would like to make is about the spending on R&D and procurement. I am sure we will get on to that. We need to solve a problem that is deep-seated in the UK economy about the difficulty of translating R&D and deployment into real practice. I have some further comments I could make on that.

Finally, I note that in the previous session last week, Miriam Cates picked up on one of the contributors, saying we could not forecast 20 years into the future, and Alex Towers asked about a contested story to do with Huawei back in 2005. I would like to point out that I had a small part in all of that and can verify that that was discussed. I will not go into details, as you would probably imagine I would not.

One of the things I participated in then was the Foresight cyber trust and crime prevention project. A lot of the things that we are talking about today were indeed forecast 20 years ago. There are some lessons that we can explore later in the Committee from that experience, if you wish to do so.
number of suppliers has come down in this business. We need to be careful in thinking about how we intervene to set the rules of the game and to encourage certain kinds of behaviour. I am very familiar with one example that relates not only to Government but also to large corporates: the notion that you go through a procurement department that is forcing you down on price, and it does not have the notion of innovation as one of its key performance indicators. The notion of innovation, on the other hand, is built into a lot of the systems that are employed in other countries, primarily the United States, as a way of evaluating whether a technology should be procured or not. We need to think rather more carefully about how we foster that development and growth of smaller companies into larger companies, particularly with this view about innovation.

For example, Ofcom is an economic regulator—one of 11 or so economic regulators in the UK. It has always, below the radar, treated innovation as one of the things it ought to be fostering. I would suggest, for example, that alongside the consideration of this Bill, we think about how we push innovation rather more firmly and put some money behind it in terms of procurement.

**Q152 Dean Russell:** I would like to understand what the impact would be of bringing forward the 2027 deadline with regard to many of these measures. If I could ask Mike in the first instance, please?

**Mike Fake:** Obviously, we have got two things to do here. We need to replace the existing vendors’ equipment, but in parallel, if we can invest in the UK supply chain—we have a very healthy supply chain in the sense that there are a lot of companies which provide optical components and subsystems into the equipment manufacturers. We need to do both things at once. We need to swap out the equipment, and also invest in the new companies coming up, so that in the future we can have a much more future-proof, innovative, secure and leading network.

Pushing the timescales forward, we have to recognise that in the short term we are going to be stuck with two alternative vendors that we need to swap out, but if we can invest in the up-and-coming, innovative, small SMEs and really foster those, as the previous speakers have said, I think we have got a real opportunity to change things and to have a world-leading, British, high-UK content network moving forward.

**Dean Russell:** Thank you. Could I ask Helen the same question?

**Dr Cleevely:** I would like to echo what Helen said, but in a rather different way. There is an engineering problem, which is what we have been dealing with, but there is also a human behavioural problem. Anybody who has worked in a large corporation or worked on these large projects will know that the way in which people approach the problem, and the way they think about it, the way they want to programme it and the urgency they feel, is driven as much by the psychological issues as it is by the technical. I would urge you to think through how you would encourage the behaviour that you want to see. Now, obviously Government can do that by simply issuing an edict and forcing a deadline, but there may be other ways that you can get more innovation and a more rapid shift than the 2027 deadline, simply by thinking through with the industry—going back to Helen’s point about the engineers on the ground—about what is required. A little bit more detailed thinking on that could yield some very positive result.

**Q153 Mr Kevan Jones (North Durham) (Lab):** Could I just follow up on Dean’s point about the actual date? The date that has been set is 2027, and the equivalent that is going to go in is basically going to be two vendors, Ericsson and Nokia. I think it was you, Mike, who said earlier that there are opportunities for UK diversification. What will drive that? If you have operators who have put brand-new equipment in in the lead-up to 2027, what will be the incentive for those companies to look at alternatives to that?

**Mike Fake:** That is a difficult problem to solve, but I think it is important that innovation is a powerful force, and you can turn around things in this new world very quickly. Although you have old legacy systems, and you replace everything from overseas vendors with old legacy systems, you need to keep moving forward. In terms of optics, we probably have one of the world’s leading telecom fibre optics innovation capabilities in the world, through the universities. We have a whole bunch of small and medium-sized enterprises out there, and they are struggling to make that step to some scale and to get that innovation deployed in the network. But I think innovation—

**Q154 Mr Jones:** Not to cut across you, but, while I accept all that, if from the operator’s point of view they have just invested a lot of capital in ripping out equipment and putting new equipment in up until 2027, what will the incentive then be for those operators necessarily to look at new technologies?

**Helen Duncan:** I do not think it is necessarily the case that they will just use Ericsson and Nokia equipment. Vodafone, for instance, has committed to equipping something like 2,500 cell sites with open RAN equipment, so they are taking a forward-looking view and trying to stimulate that themselves.

**Dr Cleevely:** If I may intervene here as well, it is curious, is it not? The economists will tell you that sunk costs are sunk costs and you should always move forward, and that is something to hold on to. Human nature says, “Well, we’ve invested in this—let’s see if we can sweat that asset to make the most of it.” A constructive dialogue with your finance director or chief financial officer is always an essential part of all this, and, for example, it is important to understand what is driving the risk that a company is running, its weighted average cost of capital and its cost of borrowing on the market.
Essentially the point is this: if you can get more business and improve your service, and get more customers and make more money, as a result of doing investment, then that is what you will do. The key point here is whether we can find a way of making it clear and straightforward to the most truculent of finance directors or chief financial officers that this is a good investment for the future. In there lies the key, because you need to get the incentives right.

Q155 Chi Onwurah: Welcome to all of you, and thank you so much for joining us. May I say, particularly to Helen Duncan—I should also have mentioned this earlier when we had Heba Bevan—that it is great to have two other female electrical engineers giving evidence to the Committee. I hope we have many more such qualified representatives of the technology sector in Committees in the future.

We have talked a little about how we got here; Helen, you worked for Marconi, and I worked for Northern Telecom, which bought STC, one of our last UK companies providing telecoms equipment. Without putting words into your mouth, I think the situation could be characterised by a lack of investment in innovation and in British sovereign capability. Now that we are seeking to reverse that, or to jump ahead of that, what interventions could best guarantee the long-term security and resilience of the UK telecoms network, with UK sovereign capability supporting it? Is the £250 million diversification strategy set to achieve that? Can you give examples—I am looking for quite concrete examples—of what you might add or change? David, you talked about needing to give the right incentives to the mobile operators. The telecoms supply chain review was quite clear that there is not an incentive right now in the supply chain to deliver security in mobile networks. What interventions and what incentives should there be?

Helen Duncan: Starting from how we got into this situation, in the 1990s we had three incumbent base station manufacturing companies in the UK, which were Orbitel in Nottinghamshire, and Motorola and Lucent Technologies, both in Swindon. They survived for different lengths of time: Orbitel closed down in 1996 when Ericsson took over, Motorola ceased base station manufacturing in 2002, but stayed open and was then sold to Nokia, and Lucent became Alcatel-Lucent and was closed down. Mergers and acquisitions have clearly played a huge part, as did the dotcom bubble and, as I mentioned, the removal of funding from the defence sector.

Heba made the point that to support semiconductor manufacture in the UK, the £250 million would not even start to scratch the surface. We need to concentrate a little bit further up the food chain. We have some very good capability in this country in component and subsystem manufacture based around the chips. We have some good design capability for chips that are then manufactured in the larger foundries elsewhere in the world. Supporting those activities, the design and the manufacture of components and subsystems, would give us a good basis and improve resilience.

I also want to mention that we have some capability in this country in the test and measurement sector with Spirent and VIAVI Solutions—although VIAVI is an American-owned company, it manufactures RF and wireless test equipment in the UK. By definition, test is ahead of the curve on development. If you can make equipment to test something, you can actually make that equipment, because it is much more complicated to make the test equipment than it is to make the base station or the handset itself. Those companies deserve our support as well. That was a very long question, Chi; I am not sure I covered every aspect you were asking about.

Q156 Chi Onwurah: That’s great, David?

Dr Cleevely: Thanks, Chi—nice to see you. One of the things that was mentioned in the session a little bit earlier was standards, and I think one of the things that changed telecommunications between the 1970s and the dotcom revolution was the emergence of some of these more open standards, such as TCP/IP for running the internet and so on, and HTML for doing the web browsers. I think we could be putting a lot more money and effort into defining some of those standards, because if you define the interfaces for pieces of equipment correctly, you can allow people to come in and provide bits of equipment that can conform to those interfaces. That is one very concrete thing.

You are right to say that, until relatively recently, the penalties on security and so on—the consequences—have been very small, but in terms of behaviour, you need both carrot and stick on things like this. You need to have something that will give the telecom operators a real reason to do something, which might be as simple as a kitemark that says, “The telecom network you are using has been certified as secure.” That may or may not be the kind of thing that would engender the behaviour change, but it is noticeable that with a number of things like Telegram and WhatsApp, that is seen to be quite an important thing.

Finally, the networks of people are important in all of this. I noticed that the Government have spent some money on the 5G networking across the UK, which is being run by Cambridge Wireless, which I am very proud to have helped set up. We talked in the previous session about the cluster of people down in Bristol working on semiconductors and so on, and I think the Government should be putting some money into networking people together across the UK, and between regions in particular, to have ways in which we can be exchanging ideas and getting to understand what each other is doing. We complain about silos in Government and siloes in corporate, but we have siloes across every single component of this industry, and it is no good to sit in a part of the west midlands, Cambridge or Belfast and not talk to other people about the issues, the standards and the technology. While we seem to think that that gets delivered by the free market, in reality that is not happening, and I think the Government in particular need to intervene to connect up all these people.

Today, I launched the Northern Ireland Engineering Hub for the Royal Academy of Engineering—I am chair of the enterprise committee—and that was specifically picking Northern Ireland because of its deep engineering history in order to start to connect it with a lot of the other things that are happening in the rest of the United Kingdom. I think we need more of that, and I think that out of it will come the same blossoming of innovation and engineering that we have seen previously when people have been connected up together. I am a great optimist on that.

Chi Onwurah: Great. Thank you very much.
The Chair: Mike, did you want to say anything else?

Mike Fake: I would just add that the radio part of this network is very important, but there is also a fibre optic network that connects it back to the core, and if we can invest in innovation—which means investing in the people who are coming up with the ideas, at the universities and so on—and in the SMEs, there may be clever ways in which we can get to scale manufacturing. That is not just for radios, but potentially hardware boxes, looking at gateways and so on, and also optical fibre, for instance. I support wholeheartedly what the other two witnesses have said, especially the point on open standards that David made.

The Chair: I am just going to go to the Minister, and then I will come back.

Q157 Matt Warman: Thank you for the evidence you have given so far. It seems to me, over the course of a lot of the evidence that we have heard over the last several sessions, that there is a lot of consensus on standards being hugely important and on building on clusters, in both existing businesses and the networks that David was just talking about. If you look into the short and medium term, what are the immediate interventions that you would make, rather than the longer term things to build up in the next few years?

Dr Clevely: Thank you, Minister. On the short-term stuff, I am very reluctant to dash in on some of these things. I have started a few businesses. It is always a mistake to try to spend money too quickly, because you do not quite know how it is working, but if you are asking me where I would specifically spend some money, I would start to spend it on groups of people and existing researchers, connecting them up, having seminars and workshops, starting to fund little bits of research, opening up some competitions, and getting some ideas for where the standards might be—putting oil in a mechanism that has seized up and become somewhat rusty.

With relatively little money—we are talking about nothing like Heba’s amounts that you need to spend on a fab plant—I think you could free up a lot of stuff, but you need to put in, at the same time, quite a lot of investment in monitoring all of that, so that you are learning from the process. There are a lot of brilliant engineers and brilliant people in the United Kingdom. My impression is that we do not do enough to connect them up, so my first action would be to use the catapults, the academies, our brilliant universities and fabulous corporations.

Honestly, as we have already heard, we have some marvellous stuff going on in telecoms manufacture. Start to bring those people together. That costs money to service and to actually make it work. That is where I would start, and I would have a framework for what kind of information we were going to get out of that, so that it was not just a nice party, as good as that is, or a talking shop. A distributed catapult would be one way of thinking about it.

Helen Duncan: I absolutely agree with what David has just said. I would also suggest one specific area where some intervention could be very timely, given that a lot of antenna engineers were made redundant just before Christmas when a company called Axell Wireless went into administration. Antennas have not been mentioned, but Huawei holds an awful lot of intellectual property in antennas. That will be a weakness going forward. In the past, we had some significant antenna capability in this country, most of which was bought up by Cobham, which has now said it has no interest in telecoms at all. It was because they sold Axell Wireless that it has now gone into administration. That is a specific case, but it is just one example of an area where it is not too late to reverse a particular trend.

Mike Fake: I completely support David and Helen’s comments.

The Chair: We have about 11 minutes left. I will go to Kevan Jones, who I think had a question that was prompted by a reply to the Minister. Then I will try to go back to Chi and to the Minister before we finish.

Q158 Mr Jones: It is just a quick one. We are talking a lot about Government, and what Government can do, which is fine. But when it comes to attracting sufficient private sector investment in some of these emerging technologies, how will you kick-start that? I ask because that will be the acid test for growing some of these companies.

Helen Duncan: I think hardware technology has a very poor image with investors and we could probably take an initiative to try to improve that, including trying to attract the right people to take up careers in hardware rather than software, as it is seemingly becoming not so glamorous but it underpins the whole thing.

Dr Clevely: Helen, I think you are right. It is very interesting that these days, if you want to get investment in a company—I have personal experience of this—you present it as a software company that needs a little bit of hardware to make the software work; you do not say at all that it is a hardware company. That is one thing to note.

More seriously, on the general point about private investment and interest in these things, this is a matter of setting up the rules of the game so that it makes sense for the private investors and the private people to get involved. None of this is achieved by Government; none of it is entirely achieved, indeed, by the private sector. This is one of these areas where you need to think about how Government set the rules up and set the incentive structure so that the private sector explores the environment—because Government cannot work out exactly how this is going to turn out. The private sector can then explore it. That is why, for example, procurement is so important. If you can procure from a number of different sources and encourage people to move forward, you will explore the possibilities of innovation much more rapidly than any single company or any single Government can. We need to construct the rules of the game so that the private sector can start to deliver what the private sector is really good at. I talked about oiling the wheels; I am talking about unblocking drains at this point. We really need to make sure that the mechanism is working properly.

Mike Fake: I would support that. I will just add that some of the mechanisms that we could explore are things like the competitions where Government put in a certain amount and private industry puts in a matching amount, but it has to be significant; it has to be a large investment—something that will make a difference, something that will take the thing from the early innovation stage through to full-scale manufacture, in the UK.
Q159 The Chair: When you say that that has to be significant and large, do you want to put a figure on it? [Laughter.]

Mike Fake: I walked into that one, didn’t I? I just come back to my earlier point, which was that it is really great that the Bill is proposing £250 million of money for research and development over five years, but if that turns out to be £50 million a year and then you think just about BT, which is spending £500 million a year just on its network, the £50 million really is not very much, is it? It is appreciated—it is really appreciated—but it is not a significant amount in the context of that.

The Chair: Thank you for that. Chi Onwurah.

Q160 Chi Onwurah: Helen, you were absolutely right to emphasise, in terms of how we got here, with no UK telecommunications network capability, that as well as being about under-investment, which I mentioned, it was about acquisitions—many acquisitions of UK capability and capacity. We have the National Security and Investment Bill going through the House; in fact, that is coming back for Report tomorrow. It will make national security—although not economic security—a ground for intervening in acquisitions and investments, but it will not make investment in companies any easier.

We are talking about concrete measures—what measures could Government take, or could be taken, to make significant additional investment available or easier?

Helen Duncan: That is an interesting question.

Chi Onwurah: We could perhaps have a telecoms business bank?

Helen Duncan: You cannot stop mergers and acquisitions happening, but if you can put in some sort of criteria that companies that buy British companies need to give a commitment to continue to invest in this country for a set period of time—whether or not that is practicable—that would help.

The most important thing is to make the companies themselves strong enough so they are not targets for asset stripping, as has happened in the past. All the measures that we are talking about to oil the wheels, as David says, will make our companies stronger and able to compete in what is still a global market. I think making our companies competitive is the key to this.

Dr Cleevely: There was a thing called the Macmillan gap, which led to the emergence of the Industrial and Commercial Finance Corporation in the late 1940s. Translated into modern terms, that gap is investments required of around about half a million to £5 million or £10 million. We are still living with that, and that gap was identified in the 1920s. We have a structural problem in the United Kingdom about the way in which we invest in some of what would in Germany be called Mittelstand—those smaller companies. I think you are quite right, Chi, to draw attention to that as a particular risk profile. People do not want to put money necessarily past the seed stage into what I would call late series A and into series B.

The other point is procurement. As I have mentioned before, if you have a client or two who is prepared to buy kit from you, you not only get money but you get experience and expertise and you develop your company. We need more incentives for procuring from those kind of middle-sized companies, because out of those will come the giants of tomorrow.

My experience in Cambridge and elsewhere is that quite often, many of those companies say they are entirely private sector driven, but actually they have been the subject of lots of Government procurement and interventions along the way. That is particularly true in the United States where the SBIR scheme is very important.

The Chair: Do you have anything you want to add to that?

Mike Fake: I do not have anything to add to that. I support what has been said.

The Chair: I am going back to the Minister, Chi, because I am conscious of time.

Q161 Matt Warman: Thank you. It is a very simply question in some ways in that it follows up on a lot of what David has been saying. Obviously, when we have talked about £250 million, that is to work with the private sector, and where we have run test beds and trialled programmes, we have talked about match funding. Presumably, you would think that is a sensible approach, but I wonder what you think the limits, or what a reasonable proportion of Government investment in a company might look like, rather than simply the traditional match-funding model. I know this is sort of “how long is a piece of string”, but in terms of stakes and all that sort of thing, there is obviously a spectrum, isn’t there?

Dr Cleevely: Well, Minister, my instinct is not for the Government to not take stakes in companies, so I think that that is beginning a distortion of—

Matt Warman: That is perhaps not the phrase, but you get the gist.

Dr Cleevely: The primary way to do it is: first, let’s set the rules and regulations. Secondly, let’s put some pump priming into the networks to allow people to talk. Thirdly, let’s see if we can get the procurement sorted out so that these companies can actually get the lifeblood pumping through them. Fourthly, if you really need to, because of security or other strategic interests, are there things such as the British Business Bank or other mechanisms that can act as intermediaries? You do not want the Government directly intervening in this stuff. That is the hierarchy in which you deal with this. On exactly how that works in a particular case, I have not spent enough time thinking of a detailed response.

The Chair: I am afraid we have run out of time. I know we could have gone on a bit longer, but thanks very much to our witnesses. That concludes this session.

Examination of Witness

Doug Brake gave evidence.

3.30 pm

The Chair: We will now hear from Doug Brake, director of broadband and spectrum policy at the Information Technology and Innovation Foundation. We have until 4 o’clock for this session.

Good afternoon, Mr Brake. Will you introduce yourself for the record, please?

Doug Brake: As you mentioned, my name is Doug Brake. I am the director of broadband and spectrum policy for the Information Technology and Innovation...
Foundations. We are a think-tank based in Washington DC, focused on policies that we believe advance innovation, with the basic belief that innovation is the key to economic growth and human flourishing over the long term.

**The Chair:** Thank you. I call Sara Britcliffe.

**Q162 Sara Britcliffe:** I have a quick question that I asked the previous witnesses. What is it that you support in this Bill?

**Doug Brake:** At a very high level, I would say cybersecurity generally. The goal of Government intervention should be to make it easy, cheap and desirable for the private sector to do cyber-security well. I have some vague concerns that some increased costs might come from the Bill—the compliance costs—but identifying this as a serious issue that needs to be looked at and giving Ofcom the tools that it needs to investigate security challenges, especially with regard to the equipment and working with the private sector to mitigate those risks, is a big step forward.

On the diversification strategy, I think it is a very wise document. That to my mind is one of the best opportunities that we have to mitigate long-term risks, particularly where there are high-risk vendors in the area. So I think the diversification strategy is quite wise and would make the UK a real leader in this space in terms of policy.

**Q163 James Wild (North West Norfolk) (Con):** What is your view on the implications of the Biden Administration for potential American involvement in the diversification strategy in telecoms more broadly?

**Doug Brake:** That is a good question. A lot of people are asking that question and trying to figure out exactly where this will go. I think that at a high level we have passed through the confrontation with Huawei and China over some of these innovational mercantilist policies that we have seen, which have undermined the global innovation of wireless equipment. I don’t think that will change at a high level. No politician in Washington in the US wants to be seen as soft on China. I think that at a high level we have some areas of that—high-performance, generic server infrastructure, as well as software—that the US does quite well. However, I think that opening up the supply chain would allow for a number of companies internationally to compete quite strongly.

Also I think there is a question about the extent to which different countries are willing to aggressively pursue an industrial strategy to support the sort of change that could give them a potential comparative advantage in pursuing this sort of transformational change to the telecommunications supply chain.

**Q165 Mr Jones:** Regarding the ban on semiconductors, obviously that is worth a lot to the US in terms of exports, mainly to China. Do you see that changing? Also, do you think there is a danger—not in the short term, obviously, but in the longer term—that China will then create a separate semiconductor market, which could be a threat not only to the US but to others, in that they will buy into markets and try to get standards that are different from those of the US?

**Doug Brake:** I think it is absolutely right that there is a real risk if we cut off supply to China, particularly in semiconductors. We have already seen an aggressive action on their part to stand up an indigenous semiconductor industry. This is getting a little outside of my area of expertise; semiconductors is not some place that I know super well. However, I think that it is absolutely correct that there is a real risk that the extent to which we try to cut off Chinese companies will see them double down efforts to create their own indigenous supply chain. So—absolutely.

I am hopeful that we see either a change to that or a much broader international coalition to double down on those efforts. I think that it is more likely that we will
see a Biden Administration ease some of those restrictions, or work through the current legal means to allow for licences for companies to sell semiconductors to Huawei and others.

Q166 Dean Russell: During my previous career as a physics researcher many years ago, I was fortunate to work at places such as the Advanced Photon Source synchrotron facility in Argonne, Illinois. I worked extensively in the semiconductor space, looking at materials such gallium nitride and other group III nitrides. What I learned back then, working very extensively with American scientists and scientists from around the world, was the importance of that root-and-branch look at semiconductors, innovation and having a decades-long view. From your perspective, how much does that fit in with a joined-up international approach to create diversity, both at the end stage and at the really early research stage?

Doug Brake: That is absolutely right. This is a long-term effort. I worry about some who tout ORAN as something of a silver bullet that we can make a quick transition to, that it is a flash cut for existing equipment providers to an open RAN sort of system—a more modular and diverse ecosystem. It is something that is going to take a number of years. I honestly worry that it is late for ORAN to be incorporated into 5G, at least on a broad scale. For greenfield networks, it is a different story and it might make sense to go with these open and modular systems from the get-go.

I worry that this is much more a conversation about putting in the tools, resources, testing facilities, the labs, R&D, et cetera, to put us on a path for years down the road so that this becomes the industry standard. I do think, absolutely, that this is the time to be looking at those early stage investments to be driving further and, frankly, looking down the road to 6G, to be able to put in place the policies and efforts to transition the industry to this more diverse future, and put those in place now for years to come.

Q167 James Sunderland: Thank you for coming in. A quick question: can you put in layman’s terms what the change very obscure technical parameters to make for LTE and 4G today. At the same time, you can also very reliable, with very low latency. For example, if you want to stream a football match while travelling on a train, it can do that quite well, or quite a bit better than LTE and 4G today. At the same time, you can also change very obscure technical parameters to make for simple communications that require very little battery on the device side to be able to communicate. If you want to have massive deployments of sensors for smart agriculture, or something like that, that have battery life in the order of decades, it can do that. The hallmark of its flexibility.

Given that flexibility, it is anticipated that 5G is going to be much more deeply integrated within the economy and trade sectors, and will be a key tool to boost productivity. There is an important hope that we see a broad deployment, not just in urban areas but in rural areas. Again, I go back to that note on differences depending on the spectrum that is used to deploy—unless it is of interest, I do not want to get too bogged down in the details, but there are real differences in what we would expect to see deployed in urban versus rural areas. But, again, we would also expect to see very different use cases in those areas. Admittedly, there will likely be a performance difference between urban areas and more rural areas. But at the same time, like I said, the use cases look very different—you are not likely to have massive crowds of people all looking to share video from a stadium or something like that in rural areas. There will be a real difference in the roll-out, but I worry that sometimes the challenges with that have been overstated.

Q168 Chi Onwurah: Thank you very much for joining us, Doug. It is particularly interesting to have your American perspective. As you may have heard, my first job as a hardware engineer was with Nortel, a Canadian-American company that had just bought one of the last UK companies in this area. Nortel ended up seeking chapter 11 and having most of its IP bought by Huawei.

What are your views on how we got ourselves into this position of not having a single UK or US supplier that can supply to our UK networks? How do you think we can work together to rebuild our telecoms sectors? You talked about pursuing transformational change and an industrial strategy to do that. What might you say to the Minister about how the UK Government should be working with the US, and about what sorts of vehicles there might be to work together and with other allies to achieve that?

Doug Brake: That is a great question. We talk now about needing diversification and seeking entry of a US-UK equipment supplier, but the question and lessons from history are about why we need this in the first place. In the past, we had quite successful telecommunications supply companies, especially in the US. The president of our organisation, Rob Atkinson, set out to answer that question. You may have seen an article in the American Affairs journal, titled, “Who Lost Lucent?” It is a long and interesting article—I will not go into all the details of history. I would say that it is fair to characterise the failures and decline of Lucent as a complicated story, but it stems from a combination of unique challenges imposed by the Anglo-American economic system, systemic failures of US Government policy—particularly with regards to anti-trust and some of the regulatory policy throughout the 1990s—and very strong and aggressive foreign industrial policies, particularly with regards to China, to acquire market share.

I am happy to go through that in some detail, but feel free to cut me off if I go on too long. You are absolutely right to say that we had Lucent and Nortel. Lucent was
absolutely massive—it was three times larger than Nortel—and originally spun off from AT&T’s equipment arm, Western Electric. It had the famous Bell Labs. Throughout the ’90s, it was the largest telecoms equipment company and was still growing dramatically overseas, but due to a number of strategic decisions within the company and decisions within the US Government, it ended up really suffering as a result of the dot.com bubble.

Setting aside all the competitiveness questions, particularly with regards to Chinese companies, a hands-off, free market globalised system reigned in the US and UK throughout the ’90s. It was finance-focused capitalism that saw Lucent and Nortel cut their R&D budgets and staff dramatically, particularly as a result of the 2001 crash—much more so than some of their international competitors. With that financial system, it was harder for those companies, which were designed to be growth companies—much more so than a valued company. They were focused on growing quarter after quarter and meeting their financial targets, which made it very difficult to focus on long-term growth. You can contrast that with Ericsson in Sweden, where the Wallenberg family control a lot of the voting shares. Ericsson was able to focus on much longer-term value creation, and they did not cut staff or R&D by nearly as much as Lucent did.

Before that, I think there are a lot of lessons to be learned from the aggressive anti-trust action that broke up Bell Labs and restructured the entire industry. Up until the restructuring of the US telecom market in 1984, Bell Labs had a fantastic situation in order to generate innovation. It had the commercial drive, focus and flexibility that is often lacking in a Government research lab. It also had a long-term focus and an interest in broad technological change, which many R&D efforts in industry do not see. It had steady revenue from telecom rates. There is a complicated story there. It is hard to tell what concentration is good for innovation and where competition is really the order of the day, but it seems clear that the decline of Bell Labs was a real loss.

**Q169 Chi Onwurah:** Perhaps you could contribute the article you mentioned and the key points made as written evidence.

**Doug Brake:** Absolutely. We would be happy to do that.

**Q170 Chi Onwurah:** The second part of my question was about how we can work together.

**Doug Brake:** Absolutely. I think the diversification strategy is a very strong document. I would say, when it comes to open RAN generally, there are clear benefits that you have heard a lot about, I am sure, including diversification and faster innovation when software is decoupled from hardware. Generally, lower margins on generic components eliminate the risk of the entire sector tipping to a single vendor or a gradual narrowing of trusted suppliers, but there are real challenges with this process. Again, this is going to be a gradual effort. There is not a need to transition immediately.

First, there is a real risk of bandwagoning. There is real complexity with transitioning to this sort of system. It is not immediately clear how well open RAN will scale. Actual implementation at scale in urban areas is adding a tremendous amount of complexity. There is a much larger attack surface. It is worth keeping in mind SolarWinds, a US company trusted by many within the Government, which saw this massive damaging breach.

I think there is a real challenge that remains to be addressed in the manufacturing of stand-alone radios. I think that is a potential opportunity for real co-operation: identifying companies that are interested in focusing purely on radio. There is still hardware that needs to be provided that historically was integrated with the broader system, when you only have relatively small providers that are interested in scaling up manufacturing.

**The Chair:** I am just going to interrupt you there. I am sorry, but I am conscious of time and I want to give the Minister a fair opportunity.

**Q171 Matt Warman:** Thank you for that interesting evidence. This follows on from Chi’s question, in a sense. I think it goes without saying that we will be very keen to work with America in the future, and the opportunity to do so is significant. I have held conversations with my Swedish and Finnish counterparts, but when it comes to further international co-operation, if you were in my position, where would you look to first? Do you think the Bill is forward leaning enough to bring that collaboration up a gear, if that makes sense?

**Doug Brake:** I think there are two different opportunities. First, in the efforts of diversification, this is necessarily a globalised sector. The incumbents are massive companies with huge global economies of scale, so in order to transform the industry structure, it is going to have to be a global effort. We need all the countries aiming in this general strategic direction.

I think the document is sufficiently forward leaning. At a high level, one of the most important first steps is identifying this as a strategic imperative—that this is a goal that is shared by Governments across the world—and taking a genuine interest and focus, especially on the level of venture capital investment. Just the creation of the document is a hugely important first step. As for continued research, the real focus is on research and development and test beds. They are the key tools that we need to test and scale up, to identify real challenges and complexity.

I am not sure if this quite fits the answer, but there is a challenge around systems integration. We need to identify real leaders in systems integration. When you have real risk in pulling together different components from different suppliers, into what is essentially critical infrastructure, the risk of failure—at least, the downsides of failure—is extreme, so operators are often eager to have a single company that they can go to if something goes wrong, which can integrate all the different components. There is an important opportunity, to the extent that policy can help support those efforts.

There is all sorts of opportunity for global collaboration and for rowing towards the direction of this diverse supply chain. I think you have put together a very thoughtful piece in moving that forward. Then again, I go back to saying that this is not a silver bullet in addressing the long-term challenges around innovation mercantilism from China and Chinese companies. I think there should
be more co-ordination and collaboration, especially when it comes to trade policy. Again, this is outside my area of expertise—I am 5G, specifically—but the more we can co-ordinate to be honest and up front about the real challenges and work to scale back the problem, the better.

Q172 Matt Warman: On that long-term point, do you think that both the Bill and the strategy allow Government to retain the kind of flexibility we will need for them to persist for the long term? We do not want to be revisiting primary legislation too often on this, even though we obviously need to keep aspects of it under review?

Doug Brake: I think that this is absolutely the right direction to be moving in. Clearly, you need the tools to be able to analyse the risk, identify high-risk vendors and work away from potential security risks associated with that. So, absolutely, you need the tools, but there is always a broad challenge when it comes to cyber-security of the negative extra challenges, where private-sector providers might not always face all the downside of cyber-security breaches.

You can solve that by increasing the cost and increasing the downside to cyber-security risk. I think it is much wiser to help work with Government to lower the cost of doing cyber-security well. The UK, from what I can tell, is a real leader in this regard, setting up NCSC. To be able to work closely the private sector, to identify those risks and eliminate them, is much better than just turning up the dial on the downside to cyber-security breaches, or things of that nature.

I would tweak the Bill in that direction. I guess much of this can be done through implementing regulations, but, to my mind, focus more on collaboration and co-ordination with the private sector, rather than simply increasing the downside as well as the compliance costs with the legislation.

The Chair: I think that brings us virtually to time. Thank you, Mr Brake, for your evidence. That was the final evidence session for the Bill, so I thank all the witnesses. The Committee meets again on Thursday morning for line-by-line consideration. I believe that will be at 11.30 am in Committee Room 14.

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

Adjourned till Thursday 20 January at half-past Eleven o’clock.
Written evidence reported to the House

TSB 07 Simwood eSMS Ltd

TSB 08 Dr Louise Bennett, Director, Digital Policy Alliance
TELECOMMUNICATIONS (SECURITY) BILL

Fifth Sitting
Thursday 21 January 2021
(Morning)

CONTENTS

Clause 1 under consideration when the Committee adjourned till this day at Two o’clock.
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 25 January 2021
The Committee consisted of the following Members:

**Chairs:** † Mr PHILIP HOLLOBONE, STEVE MCCABE

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

Sarah Thatcher, Huw Yardley, Committee Clerks

† attended the Committee
Public Bill Committee

Thursday 21 January 2021

(Morning)

[Mr Philip Hollobone in the Chair]

Telecommunications (Security) Bill

11.30 am

The Chair: Before we begin, I have a few preliminary announcements.

Members will understand the need to respect social distancing guidance. I am told here that I shall intervene if necessary to remind everyone. Mr Speaker has asked that Members wear masks in Committee, except when speaking. Please switch electronic devices to silent. Tea and coffee are not allowed during sittings. Hansard colleagues will be grateful if Members could email their speaking notes to hansardnotes@parliament.uk.

We now begin line-by-line consideration of the Bill. The selection list for today’s sitting is available in the room. This shows how the selected amendments have been grouped together for debate. Amendments grouped together are generally on the same or a similar issue. Please note that decisions on amendments do not take place in the order that they are debated, but in the order that they appear on the amendment paper. That is often confusing for Members, young and old alike. The selection and grouping list shows the order of debates. Decisions on each amendment are taken when we come to the clause to which the amendment relates.

Clause 1

Duty to take security measures

Chi Onwurah (Newcastle upon Tyne Central) (Lab): I beg to move amendment 7, in clause 1, page 1, line 19, at end insert—

“(ba) the presence in the network or service of supply chain components which represent a threat to national security;

This amendment would add the presence of supply chain components which represent a security threat to the list of “security compromises” which network and service providers must take security measures against. “Supply chain components” are defined by Amendment 8.

The Chair: With this it will be convenient to discuss amendment 8, in clause 1, page 3, line 17, at end insert—

“‘supply chain components’ means the sequence of processes involved in the production, distribution and maintenance of networks and services.

This amendment defines “supply chain components” for the purposes of Amendment 7.

Chi Onwurah: It is a great pleasure to serve under your chairship, Mr Hollobone, and to see the Bill Committee present. I thank all its members for taking part, and I observe that the room is a lot warmer than it was in December, when the National Security and Investment Bill was in Committee. I hope that we will continue like that. I also thank the Clerks and all the members of House staff who have supported us with the amendments and on the Bill more generally.

I crave your indulgence, Mr Hollobone, to start with a few opening remarks that will be helpful in understanding the Opposition’s approach to this amendment and to the Bill as a whole. To give the context, I worked as an electrical engineer for 20 years before entering Parliament. I am still a chartered engineer and proud of that. As an engineer, I worked all over the world helping to build out the networks—fixed, wireless and mobile—that became the internet and on which this Bill is intimately focused.

I should also declare an interest. Many of the provisions of the Bill deal with the regulator, Ofcom, and I joined Ofcom in 2004, just a few weeks after it was born, when it was to be a light-touch regulator, small and nimble. Over the years, it has acquired responsibility for critical national infrastructure, the BBC, the Post Office, and the entirety of online harms and now, it would appear, national security as well. I have been calling for greater security, in particular for our mobile networks, for many years now, so I and the Opposition welcome the aims of the Bill, and the Bill itself. However, many areas within it need to be addressed.

As I have declared my personal and professional interest in the telecoms network, Mr Hollobone, you will not be surprised to hear that I am thrilled that we will spend so many hours of our parliamentary democracy time here in this room, dedicated to debating our telecommunications infrastructure. But, to my regret, the Committee is not taking advantage of the very telecoms infrastructure with which it is dealing. I would like to place on the record that we believe holding this Bill Committee physically rather than virtually is putting Members of the House, Clerks and House staff at risk from the coronavirus pandemic, and we feel that it is our duty, as a reasonable and responsible Opposition, to ensure that that risk lasts for as short a time as possible. Therefore, we are going to crack on as quickly as possible through as many clauses as possible, while maintaining appropriate levels of scrutiny. I want to put the Government on notice that we expect as a consequence to have more time on the Floor of the House on Report to consider the Bill, because we do not feel that it would be wise to dwell on many of its important themes when we are meeting physically in one room at a time of national pandemic and lockdown.

To keep all Members and staff as safe as possible, we will have a laser-like focus on three primary areas. The first is national security. Labour prioritises national security, but failings in the Bill show the Government are taking risks with our security-critical national infrastructure and economic security, and we will highlight those failings constructively whenever we can. Secondly, the security of our networks depends on an effective plan to diversify the supply chain, which should include support for UK capability, and we are very concerned that the Bill short-changes both our national security and our telecoms infrastructure by not including more references to the Government’s diversification strategy; it is a weak strategy and we will try to overcome that. Thirdly, the Bill also gives sweeping powers to the Secretary of State and Ofcom, including sweeping powers over security. As my hon. Friend the Member for Cardiff South and Penarth (Stephen Doughty) said on Second
Reading, the Department for Digital, Culture, Media and Sport is not known for its understanding of or expertise on national security, and we want to take measures to address that.

Security is the primary concern of amendment 7, which was tabled by my right hon. Friend the Member for North Durham. It seeks to add the presence of supply chain components that represent a security threat to the list of security compromises that network and service providers must take security measures against. Supply chain components are defined in amendment 8, for the purposes of amendment 7.

James Wild (North West Norfolk) (Con): Amendment 7 refers to national security. I note that the Opposition have not tabled a definition of national security, which is an issue we have considered in other debates. Is there a reason why the hon. Lady now accepts that we should not define national security?

Chi Onwurah: I thank the hon. Member for his intervention, which raises a really important point that I will say something about. As I am sure you are aware, Mr Hollobone, yesterday was the Third Reading of the National Security and Investment Bill. I refer Members to the report by the Select Committee on Foreign Affairs, published on Tuesday, on the critical issue of national security and its definition. In fact, the Opposition sought to put into the National Security and Investment Bill not a definition of national security but a minimum standard of what national security should refer to. We wanted to include elements such as critical national infrastructure—of course, telecoms infrastructure is a part of that—and supply chains, which the amendment deals with, and also human rights. I do not want to anticipate what we might table in future, but one reason we have not so far tabled a framework for guidance in national security is that we had hoped that the Minister responsible would recognise both the advice of the Foreign Affairs Committee and the Intelligence and Security Committee in giving greater guidance on what national security was, and that that was a better place for it.

Christian Matheson (City of Chester) (Lab): The other opportunity for the definition to be addressed would be when the Government next produce their defence and security review, which comes out no more than every five years. They might address what national security is or whether it is indeed desirable, as my hon. Friend has said, to specify that in an ever-changing world.

Chi Onwurah: I thank my hon. Friend for that helpful intervention. I do not want to take up too much of the Committee’s time on the way in which national security should be defined, or guidance given, although it is relevant to the Bill. As my hon. Friend says, there are other places where a framework for understanding national security would be better placed. One of our concerns about this Bill is that, as I have alluded to, Ofcom and the Department are not experienced in security issues, and they are not the best organisations to make security decisions. Putting a framework to define national security in the Bill might not be as helpful, but if as our debates progress we see a need for greater clarity on guidance around national security, and it is not to be found anywhere else, we might take up his challenge, and I hope to have his support if that should happen.

With regard to the amendment, it is important that the supply chain components are understood. As we proceed through the Bill, we will come to understand better that the steps to remove high-risk vendors from UK networks that the Minister is in the process of taking are welcome, but that is not enough to secure our networks. We also need an effective diversification of our network supply chains. Part of the challenge here is that if we remove high-risk vendors, as the Bill enables, and leave only one or two approved vendors, our networks remain insecure because they are less resilient. In fact, they are not resilient at all. The loss of one vendor would mean that there would be only one vendor for our entire 5G network supply chain, as things stand.

Chi Onwurah (Newcastle upon Tyne Central) (Lab): The amendment to focus on and consider the supply chain. There has been much concentration, quite rightly, on Huawei—not just the history, but the threats. As the Minister knows, I was a keen supporter of the amendment that I tabled in the National Security and Investment Bill, which addresses some of the same issues.

I hope the Committee will approve the amendment and I look forward to contributions from the Minister and others.

Mr Kevan Jones (North Durham) (Lab): It is a pleasure to serve under your chairmanship, Mr Hollobone. I apologise for my late arrival, but I was asking a question of the Health Secretary on the vaccine roll-out. When we look back at the time before the pandemic, would we have thought that part of our critical national infrastructure would be vaccine production? As my hon. Friend the Member for Newcastle upon Tyne Central said, that is a good example of the changing nature of these things. Will the threats to telecoms change? Yes, they will. Last night we discussed the National Security and Investment Bill, which addresses some of the same issues.

I tabled the amendment to focus on and consider the supply chain. There has been much concentration, quite rightly, on Huawei—not just the history, but the threats. As the Minister knows, I was a keen supporter of the Government’s initial response to Huawei. From a technical point of view, I think allowing 35% and making sure that Huawei was not in the core network was the right response. That all changed with the US sanctions on semiconductor exports to China, which changed the security advice. Again, I agree with that.

It will be interesting to see whether, if President Biden were to change that, we would change the security advice back. Frankly, I doubt that because of the direction of travel. I do not think there will be great change in the new Administration’s approach to China. It might be more nuanced and less belligerent, but I do not think it will fundamentally change. I know from sitting on the NATO Parliamentary Assembly and meeting fellow members from both sides of the House in the US Congress that there is a pretty unified bipartisan position on China.
The debate around Huawei has concentrated on the hardware. My amendment, which is a probing amendment, tries to see what coverage we will have in the telecoms network supply chain. There has been much talk about compromising the main components, but each of these networks are very complicated. We need only look at any electronic equipment used today, whether that is a telephone or a microwave oven, to see that they are very complex pieces of kit. The components are not all sourced here in this country—it would be impossible to do that—but are supplied from around the world. However, in terms of electronics, the major suppliers of a lot of these components are the Chinese, or Chinese companies that manufacture in different parts of south-east Asia, for example.

This is not just about how we get diversification in this sector, although trying to get some home-grown innovation is going to be important. To be honest, I think the opportunity is going to be in software and open RAN, because that is where we can get an advantage if we get our ducks in a row, not only through investment but through Government initiatives and other things. It is about trying to minimise the risk that will be there now that we are going to have two vendors. Now that Huawei is no longer in the network, we are going to have Ericsson and Nokia, both of which are going to be there for the foreseeable future. What will the regulator do to look at the supply chain around their components, for example? From the evidence we took from Dr Drew, it is quite clear that China is using not just these networks and the components that go into telecoms, but other things, including the belt and road initiative, for geopolitical purposes.

Chi Onwurah: I thank my right hon. Friend for giving way, and for the excellent points he is making. He mentioned the evidence we took in our session with Dr Drew. Is it not true that in those evidence sessions, we heard about the complexity of our networks and the extent to which network operators were not always aware of where their components were or, in this case, the level of components? Is it not the case that my right hon. Friend’s amendment will not only increase the visibility of the different components in the supply chain, but should help the Department and Ofcom understand where these components are, where they are going and the way they are changing through soft upgrades?

Mr Jones: I agree. The issue with both Ericsson and Nokia is that they will have Chinese components in their hardware. This is an incredibly complex situation, as my hon. Friend said: we are talking about not just one piece of kit that most of us have in our pockets, but hundreds of thousands of components, pieces of software and other things. What I am trying to put on the record, and what I want the Minister to respond to, is the question of how we get an understanding of any risks that are involved in that, and how the regulator and the Government are going to look at ways in which national security could be compromised, not by the main company being owned by a Chinese state entity, a Russian state entity or any actor that we feel is a threat to us, but by a key component.

I have not yet really understood how the regulator will look at that issue further down the supply chain, and whether it will ask a supplier of kit to the telecoms network, “What is the level of threshold or security that you need?” That is hard enough with hardware, but with open RAN and software—we are talking about bits of code—it is going to be incredibly difficult. One of the issues is around vulnerabilities, and various things have been said about the vulnerability that Huawei poses to our telecoms network. However, I suggest people read the Huawei assessment centre’s annual reports—I am rather sad, because I read such documents. One thing sticks out every single year, and it is not that the Chinese are doing anything nefarious. The reports are highly critical of Huawei for its shoddy workmanship and engineering, but that type of shoddy engineering and a lack of attention to security will lead to security concerns in our telecoms network.

Amendment 7 is designed to tease out from the Government their thinking about the supply chain. We do not want to be over-burdensome on it, because we want to get innovation in the supply chain. We do not want to suddenly give researchers and other people in the supply chain huge regulatory hurdles to jump over, because that would stifle the development that we are looking for. It is about how individual components and the overview of the supply chain will be regulated. I have tabled a later amendment about Ofcom, but again it comes back to the point I made yesterday about the National Security and Infrastructure Bill. What has to be at the heart of it all, every single time, is not to stiffle innovation and prosperity, but what has to come first every time is national security.

As I say, amendment 7 is a probing amendment, and I want to understand where the Government are at in terms of the supply chain, the security they feel they need over the supply chain and, more importantly, the visibility of the supply chain.

Chi Onwurah: I thank my right hon. Friend for giving way, and for the excellent points he is making. He mentioned the evidence we took in our session with Dr Drew. Is it not true that in those evidence sessions, we heard about the complexity of our networks and the extent to which network operators were not always aware of where their components were or, in this case, the level of components? Is it not the case that my right hon. Friend’s amendment will not only increase the visibility of the different components in the supply chain, but should help the Department and Ofcom understand where these components are, where they are going and the way they are changing through soft upgrades?

The Parliamentary Under-Secretary of State for Digital, Culture, Media and Sport (Matt Warman): It is a pleasure to serve under your chairmanship, Mr Hollobone. I echo the thanks of the hon. Member for Newcastle upon Tyne Central to you and the House staff for facilitating this Public Bill Committee. I also echo her praise for the temperature of the room and especially her commitment to crack on and not fill it with further hot air. That is to be welcomed.

Like the hon. Lady, I will briefly talk about the broader context of the Bill before I directly address this group of amendments. As we all know, security should be the first priority for any Government, and the Bill demonstrates this Government’s commitment to securing the UK’s telecoms networks.

Clauses 1 to 14 raise the bar for security across the whole telecoms sector, and the subsequent clauses—15 to 23—provide the mechanism for the Secretary of State to manage the role of high-risk vendors. The part that telecoms plays in our security is undeniable and has become even more evident in the midst of this global pandemic. At present, the internet provides absolutely everything for workplaces, schools, families and friends, and the Government are committed to improving that through our gigabit programme. New technologies have the potential to be transformative, but they have the opportunity to reach their full potential only if they are secure, and the Bill will ensure that.

Before I explain the Government’s response to amendments 7 and 8, it is necessary to explain briefly how they would interact with clause 1. New section 105A
in clause 1 places a duty on providers to take “appropriate and proportionate” measures. Those measures oblige providers to identify and reduce the risks of security compromises and require them to prepare appropriately for those risks. New section 105A also addresses the interaction between the duty and the national security and law enforcement activity, such that these activities are appropriately excluded from the definition of a security compromise. I will return to new section 105A later—I know that will excite the Committee.

Alongside the overarching security duty in new section 105A, new section 105B gives the Secretary of State the powers to make regulations that impose duties to take specific security measures. Clause 1 creates a duty for providers to take “appropriate and proportionate” measures to protect their networks and services from security compromises. “Security compromise” is then defined in new section 105A.

12 noon

Amendment 7 seeks to extend the definition of a security compromise to include

“the presence in the network or service of supply chain components which represent a threat to national security.”

It is accompanied by amendment 8, which provides a definition of supply chain components. I take it from what the right hon. Gentleman said that the intention of the amendment is that providers should not necessarily need to be directed by the Government not to use such components, but should proactively reduce their use of such equipment or take other appropriate measures. In many ways, these are the sorts of things that we would expect see in documents such as the code of practice. We are very keen to be as transparent as we can, as quickly as we can, and I hope that the right hon. Gentleman would say that we have already tried to adopt that spirit in some of the documentation and draft legislation that we have published around the Bill.

Mr Jones: I would, and this is really a probing amendment to get an understanding of what the Government think, but may I ask the Minister a direct question about the national security bodies—GCHQ and others? If they came across a component or something that a supplier was producing that raised concerns, how would their concerns be translated into saying that a red warning should be put on a certain component in a supply chain?

Matt Warman: I simply say that, as the right hon. Gentleman knows, the NCSC and others already work very closely with the networks. What he seems to be talking about, in some ways, is a very day-to-day way of talking about security concerns. That happens a lot already, and what the codes of practice and other documents will do is set up the framework by which that is formalised. As he knows, that process of very quick action being taken as soon as something is spotted, both by the networks themselves and by our agencies, is already well established, and the Bill gives considerably greater force to it.

As the right hon. Gentleman knows, the Bill is aimed at ensuring that providers take responsibility for the security of their networks and services in a way that has not happened, in legislative terms, in the past, and it then provides the Government with the powers that we need to enforce that. In so far as any supply chain components give rise to risks to the security of a network or service, new section 105A already requires providers to take appropriate action and proportionate measures to identify those risks. I appreciate that this is a probing amendment, but in a sense what the right hon. Gentleman is seeking to do through it is already there, and it will be enforced in the documents, such as the code of practice, that I have mentioned.

Furthermore, the addition of the presence of a supply chain component as a security compromise would not be consistent with the security framework’s definition of a security compromise, but I do not think that we need to get into too much detail about that in the context of a probing amendment. The concept of a security compromise is used in other provisions in the Bill, and it is important that we are consistent.

More fundamentally, the right hon. Gentleman’s amendment would put the onus on providers, rather than the Government, to determine a national security risk, but, as he implied, it is absolutely down to the NCSC and, ultimately, the Government and agencies to make that definition. Placing the responsibility for determining what does and does not constitute a threat to national security on the shoulders of all individual providers is not the right thing to do, and I think, to be fair, the right hon. Gentleman is not really suggesting that it is, either.

Chi Onwurah: I thank the Minister for the way in which he is addressing these important proposals. I think that his concern is that this amendment would put the responsibility on the providers rather than the National Cyber Security Centre, and I understand that, but can he say a little about the following matter, because it is the providers that know their networks? The National Cyber Security Centre is excellent, and we have huge admiration for it, but in terms of the supply chains, changes to the supply chain and new components evolving, how does he envisage that, day to day, working effectively without an amendment of this kind to put this requirement on the providers?

Matt Warman: As I have said, new section 105A partly provides the legal basis that the right hon. Gentleman seeks, but in practice no one is suggesting—the Secretary of State talked about this on the Floor of the House—that it is solely the name on the box of a piece of kit that defines international security status. We are not naive to the possibility of the supply chain being another vector of attack. That would be reflected in codes of practice and elsewhere around the legislation.

Public telecoms providers can and should consider the security of the resilience of their networks and services throughout the supply chain in a sensible and proportionate way. National security considerations are inevitably much broader than the issues that can be addressed solely by private companies. I think that is reflected in the distinction drawn up in this Bill.

The amendment would have implications for Ofcom’s monitoring and enforcement of providers’ compliance. The Bill includes provisions for Ofcom to collect information on behalf of the Secretary of State in narrow and specific areas related to national security, but this amendment would require Ofcom more actively to take some of the compliance judgments. In the evidence session the right hon. Gentleman was keen to see that it was not asked to make those judgments.
Mr Jones: Clearly NCSC does a tremendous job in terms of education of members of the public and companies—as the Minister outlined, that is a key part of its role. Does he see, therefore, a role for Ofcom as part of that, in terms of ensuring that the supply chain and operators are aware of their responsibility not only under the Bill, but to ask the right questions about supply chains from what might be deemed as high-risk vendors?

Matt Warman: In so far as codes of practice will be published by Ofcom, the answer to the right hon. Gentleman’s question is yes. The more nuanced answer is that it is a co-production between Ofcom, the Government, NCSC and others.

To conclude, the Government are immensely sympathetic to the issues that the right hon. Gentleman and the hon. Lady seek to probe, but we take the view that this amendment would do something that is, ultimately, already covered in the Bill. I hope that, in that spirit, she will withdraw the amendment.

Chi Onwurah: I thank the Minister for his response. I am concerned that there is not greater clarity on the role of the supply chain components and the supply chain more generally. We will come to that in further amendments. Given where we are and how we got here, we must take a forward-looking approach to future risks and vectors for risks. This amendment is important in probing that, but I do not seek to put it to a vote. I beg to ask leave to withdraw the amendment.

Amendment, by leave, withdrawn.

Mr Jones: I beg to move amendment 9, in clause 1, page 3, line 26, at end insert—

“(2A) The Secretary of State must provide the Intelligence and Security Committee of Parliament with a report on the specified measures.

This amendment would ensure that the Intelligence and Security Committee of Parliament is provided with any information relating to specified security measures which the Secretary of State requires the provider of a public electronic communications network or a public electronic communications service to take.

We are now going to have a debate reiterating a speech I gave yesterday on the National Security and Investment Bill, because it covers the same issues. I will go into the details in a minute, but the amendment attempts to ensure parliamentary oversight of the way in which this Bill will operate. Such scrutiny traditionally comes from the Select Committee that mirrors the Department—the Select Committee on Digital, Culture, Media and Sport—but the decisions taken by the Government and the Secretary of State will be based on evidence that cannot be put into the public domain, because much of it is highly classified. In Parliament, only the Intelligence and Security Committee has the required STRAP clearance to see that evidence. It is important to ensure that the Executive is held to account for taking such decisions and for the public and Parliament to know that decisions have had parliamentary oversight from the ISC.

I do not want to give the impression that the ISC is looking for work, because I have been a member for a number of years and we are busy with a lot of inquiries—I have three to four hours’ reading every week looking through reports from the agencies. However, it is important that the ISC can at least look at the intelligence that lies behind decisions. The amendment does not propose that the ISC should have a veto or be a regulator, because that would not be correct. Decisions about high-risk vendors are for Ofcom and the Secretary of State.

We had the same debate yesterday on the National Security and Investment Bill, because the same issues come up there: decisions will be taken on national infrastructure, and the justification for them will be based on highly classified secret intelligence to which the Business, Energy and Industrial Strategy Committee will not have access. People might say, “Isn’t this the ISC getting involved in the day-to-day work of the BEIS Committee?” No, it is not. The ISC already has such a responsibility for Defence Intelligence and the National Cyber Force—military cyber-security—and we stick just to that; we do not go into wider Defence policy issues. Likewise, we scrutinise MI6, whose home Department is the Foreign, Commonwealth and Development Office. Again, we do not get into general foreign policy issues, which are rightly for the Foreign Affairs Committee. I do not think there is an easy way for the Government to provide for parliamentary scrutiny at the moment, but I want to go through and explain one.

I have some sympathy with the Minister, just like I had some sympathy with the Secretary of State for Business, Energy and Industrial Strategy yesterday on the National Security and Investment Bill. I know exactly where the problem is, and it is not in the Minister’s Department or the BEIS: it is in the Cabinet Office, which seems to regard an issue with the ISC and jealously guards anything that we ask for, ensuring we get only some information even though we are legally entitled to it under the Justice and Security Act 2013. There is usually a tug of war, and on every occasion I have seen it the ISC has won—it is legally allowed the information—but that does not stop the civil servants. I must say that this is not Ministers’ fault; it is the culture in the civil service.

12.15 pm

The point was quite well summed up in yesterday’s debate by the right hon. Member for New Forest East (Dr Lewis). We have departments that we scrutinise—MI5, MI6, GCHQ and defence and military intelligence. Section 2(1) of the Justice and Security Act refers to those intelligence agencies. It also lays out the various agencies that we have the responsibility for monitoring and scrutinising. However, section 2(2) sets out the broader context. It says:

“The ISC may examine or otherwise oversee such other activities of Her Majesty’s Government in relation to intelligence or security matters as are set out in a memorandum of understanding.”

The memorandum of understanding is between the Committee and the Prime Minister, as section 2(5) explains. It also explains that the MOU can be altered at any time. Therefore, all that is required is the Government’s activity in relation to defence and intelligence matters to be added to the list in the memorandum of understanding. There is a mechanism there—it already exists—to allow the ISC to look at that.

James Sunderland (Bracknell) (Con): Given that most MPs do not fully understand what the ISC does, does the right hon. Gentleman not agree that the Government are probably best placed to make the decision on this particular matter?

Mr Jones: No, I do not. I know the hon. Gentleman is a new Member, and I actually quite like him, but what is he arguing for? A dictatorship? What should the Executive decide everything? Knowing you, Mr Hollobone, you would take a very dim view of that. You have form on holding the Executive to account—all Governments.
The ISC is there to look at information and provide parliamentary scrutiny. As for the nature of the information we receive, we have all the clearances from top secret going up to STRAP, including STRAP 3, which is intelligence that has a limited circulation and people have to be added to the list. We have access to that as well, which allows us to consider that information.

Our annual reports, which we supply to Parliament, can be debated by Parliament. We can produce reports. For example, most recently, there was the Russia report, which highlighted what the Government had not done rather than what it should have been doing. The contention from the Cabinet Office is that if information goes to the ISC, it is in the public domain. That is a little bit insulting. We do public reports, which have information that can be put into the public domain, but there are always secret annexes that go to the Prime Minister and are not made public, which allow us to question decisions and highlight issues that we think the Prime Minister should take notice of. It is a valuable mechanism for scrutiny.

The argument that will come from the Cabinet Office is that DCMS is not covered. It is. The memorandum of understanding says:

“The ISC is the only committee of Parliament that has regular access to protectively marked information that is sensitive for national security reasons: this means that only the ISC is in a position to scrutinise effectively the work of the Agencies and of those parts of the Government whose work is directly concerned with intelligence and security matters.”

I accept that DCMS’s day-to-day work is not covered in the description of national security, whether or not this is an issue of concern to individuals. I think it is. There could be an argument as to why the Department for Digital, Culture, Media and Sport got this legislation and whether it should perhaps be put in another Department. I do not agree with that, because I think the general issue of telecoms fits well into the Department’s wider briefs.

Increasingly, a number of Departments are getting involved in, or taking responsibility for, areas that involve national security. BEIS and the National Security and Investment Bill is a good example.

Chi Onwurah: My right hon. Friend is far too modest to set out his vast experience with and long-standing membership of the Intelligence and Security Committee. Does he agree that the geopolitical and technological shifts in the last decade in particular—perhaps the last two decades—have meant that the threats to our security come from a broader range and, more specifically in a more technologically-based range, and we have seen our defence requirements move to cyber-security? Therefore, as he said, the increased need of Departments to consider security issues means that the Intelligence and Security Committee’s ability to review items that require security clearance is important. Does he understand why the Government will not allow the Committee to do that?

Mr Jones: My hon. Friend knows that modesty is one of my trademarks, but no, I do not— I do not understand it, nor do I understand where the Government are coming from; I do not think that the problem is with the Minister or his Secretary of State; I think it is the culture of the Cabinet Office, trying somehow to test the Justice and Security Act to destruction. Its argument, basically, is that DCMS is not on the list of organisations, but the Act and the memorandum of understanding are clear: we have jurisdiction over matters that relate to national security, which this clearly does.

Christian Matheson: I am grateful to my right hon. Friend for providing inspiration for a speech that I will make later, when I will make similar points on similar provisions. Listening to him and to the hon. and gallant Member for Bracknell—whom I also like, incidentally—talk about the alternatives, it strikes me that there are only three: to provide classified information to be laid before the whole House or the DCMS Committee; to do the right thing and to provide that classified information to the Intelligence and Security Committee, which was surely established for exactly that purpose; or to have no scrutiny at all. It is one of those three alternatives. Surely the Government are not pushing for no scrutiny at all.

Mr Jones: I must say that this is the first time I have heard that one of my contributions to a Bill Committee is inspirational. I shall mark that as something to be remembered. However, my hon. Friend summarises the position very clearly: the DCMS Committee cannot deal with this, because the nature of the information garnered could not be shown to them, given its classification. We would not want to do that because this is highly sensitive information—meaning no disrespect to the members of that Select Committee. Some of it is not our intelligence; some of it will come from our Five Eyes partners, so it is about guarding not just our secrets, but theirs. Any leaking or compromise of that type of intelligence affects not only our ability with this type of work, but our relations with our Five Eyes partners. The next option, the ISC, is the obvious one. The third option means that the Government must put through a Bill that does not allow Parliament to scrutinise these matters at all. I do not think that that is what the Minister, or his counterparts in BEIS, believe. I think we will have a to and fro on this, and will get there eventually, but it will be hard work.

As my hon. Friend the Member for City of Chester says, scrutiny is important in helping to ensure that there is not only public but parliamentary confidence that the decisions are at least being looked at. Some of the decisions will be very controversial and the Government need covering. Will that be onerous for the Department? No, because all it will entail is that the report should include the decisions taken and the reasons why. We can ask, and be supplied with that, and that, I think, is important.

Yesterday, speaking on the National Security and Investment Bill, the Under-Secretary of State for Business, Energy and Industrial Strategy, the hon. Member for Stratford-on-Avon (Nadhim Zahawi) said that the ISC can ask for the information and demand that the Secretary of State comes before it. There are two important points about that. First, yes, we could do that. However, and as I said yesterday I do not for one minute suggest that the Secretary of State or the Department would want to refuse, but there is no legal justification behind it. If a future Secretary of State said “No, I am not appearing or giving you the information,” there would be nothing at all that the ISC could do.

I remind the Committee as I reminded the two Ministers in yesterday’s debate that we are all, as the great Robin Day once said, “here today, gone tomorrow” politicians, so
any legislation we pass here must be future-proofed. Not only must we be satisfied with it; it must go on. The other important aspect of what the Under-Secretary said was the recognition of the ISC’s role in asking for information in relation to the National Security and Investment Bill. However, if it is possible to ask for information a mechanism is needed to guarantee it. I think that is also the case for the Bill that we are considering.

It will be interesting to see how the Minister responds, and whether he really believes what he will tell me, but there is a mechanism available and it would be easy and not burdensome. I stress that not for one minute is it suggested that for one minute is it suggested that the ISC would veto decisions or have any involvement in them. As with much of our work, apart from certain issues, it would be retrospective, looking back at decisions that had been taken. If mistakes, issues and concerns are raised, we can raise those directly with the Prime Minister and Departments. That is another check and balance in the system, of which I think you, Mr Hollobone, would approve, in view of your vociferous wish, whatever the Government, to hold the Executive to account. The mechanism is pretty straightforward. Either we put it on the face of the Bill or we get it into the memorandum of understanding.

There is an increasing problem with the involvement of more and more Government agencies that are not traditionally involved in national security, such as the new Joint Biosecurity Centre, which falls within Department of Health and Social Care. All the information that they will get is classified, so how, again, will Parliament scrutinise it? That will be important.

**Chi Onwurah:** I will not detain the Committee long, given that my right hon. Friend the Member for North Durham made such excellent points. I will add one point of consideration, which again, his modesty may have forbidden him from making.

The amendment goes to the heart of our concerns about the scrutiny of the provisions in the Bill. I say again for the record that we support the wide-ranging powers that the Bill gives the Secretary of State, but those powers must come with appropriate scrutiny, not because scrutiny is a “nice to have” or, as my right hon. Friend said, because the ISC needs further work, but because scrutiny of the provisions is essential to the good working of the legislation in practice.

Considering specifically the impact of the requirement to remove Huawei at this stage in our 5G roll-out—the economic impact, the cost to the providers and the cost to our economy—we recognise that it is the right thing to do, but we must also recognise the cost of doing it. Back in 2013, the ISC was one of the first parliamentary organisations to raise the issues around Huawei. I truly urge the Minister to accept this constructive amendment to support the appropriate provision of scrutiny.

My other point is more about the working of the clause, which gives the Secretary of State the power to make regulations that require providers to take specified security measures. As we know, the telecoms security framework and telecoms security requirement, to which all providers must adhere, will be set out in delegated legislation. In his response, will the Minister give us some idea of why the Secretary of State might need to set out additional specified requirements that are not in the draft of the TSR that he has published? Is the intention of the clause to enable him to set out additional specified requirements, or is it to enable him to highlight particular specified requirements that he does not think the providers are meeting quickly enough? In either case, does that not suggest that there are particular security concerns, either about providers or about the circumstances, that require these specific security measures? To come back to my first point, does that not highlight for those concerns to receive parliamentary scrutiny with the appropriate clearance, which is to say that of the Intelligence and Security Committee?

**Matt Warman:** I start by acknowledging the incredibly important work that the ISC does. Its role in overseeing the work of the UK intelligence community is vital to maintaining public trust, as the right hon. Member for North Durham described, and its members make important contributions to public debates on national security matters of all kinds. The right hon. Gentleman has done that for a number of years. Because he is a member of the ISC, he will know that I have proactively engaged with it on the substance of the Bill. I did so enthusiastically—if any Minister can ever regard a Select Committee appearance enthusiastically—and in recognition of the interest that I knew that Committee would have in the Bill. I will be writing again to the ISC on a number of matters raised in the Bill, and I have instructed officials from my
Department to continue to engage with the ISC as the Bill proceeds through Parliament, building on the work that it has already done and on the transparency that we have already demonstrated by publishing the draft of the security framework regulations on 13 January, copies of which have been provided to the members of the ISC and a number of other interested Committees. I hope that all that demonstrates the Department's commitment to working constructively with the ISC, despite the fact that, as the right hon. Gentleman said, DDCMS does not normally fall within the ISC's formal remit.

It is none the less important to acknowledge that the ISC is not the only legitimate avenue to scrutinise this framework. We fully intend to make use of all the appropriate parliamentary procedures.

The regulations and the explanatory memorandum accompanying them will all be there for the ISC to scrutinise. There is also further guidance to providers in connection with the measures specified in the regulations that can be provided in the code of practice, which must be published, with a copy laid before Parliament. Also, beyond the usual arrangements for secondary legislation, new section 105Z of the Communications Act 2003 provides for Ofcom to produce security reports. Clause 11 of the Bill enables those reports to be published by the Secretary of State, and clause 13 provides for a review of the effectiveness of the framework, including any regulations, after five years.

It is in that context that I point to the enthusiasm with which we have engaged with the ISC. We will continue to do so and ultimately—this is perhaps the reason why the right hon. Gentleman described this process as an ongoing campaign, rather than something that we should address piecemeal—the ISC is clearly defined in the Justice and Security Act 2013. I do not think it would be right to address the memorandum of understanding that he referred during our consideration of the Bill. We should not go at it in piecemeal fashion. The role of the ISC as set out in that MOU is to oversee the work of the security agencies, to provide oversight of certain intelligence or security matters within Government. Ultimately, if the right hon. Gentleman wants to change the MOU, that is a broader issue for him to take up. I note that he is not the only Member of this House to have made that point, but it is not my place to take a view on the role of the ISC; that should be for the ISC itself.

I am confident that we will continue to engage with the ISC; I personally will certainly do so. I know that the DCMS Committee will continue to take an interest, and I will simply say that we will co-operate as fully as possible. I will set out more in the letter I mentioned, and I look forward to the future salvos in the right hon. Gentleman's campaign.

Mr Jones: I make no criticism of the Minister, because he has been very proactive, as has his Secretary of State. The problem is this: we have two pieces of legislation going through Parliament. We do not have security Bills very often in this place, and now we have two in a very short period of time. Both make eminent sense and I support them, but this is not something that comes up regularly.

In terms of the Minister's co-operation, I have no complaints about the way he has operated, but he is not going to be there forever and neither is his Secretary of State, so we need to put in place something that will weather the passage of time, and create an arrangement whereby it will be seen that Parliament is scrutinising these measures. I do not know why the Government—I am sure it is not the Minister, or even his Secretary of State—are resisting this. Frankly, I am not really bothered whether it goes on the face of the Bill or in the MOU, but the Justice and Security Act 2013 is very clear that as a Committee, the ISC has the ability to look at this.

I accept that it would be wrong to get into issues around this Bill that are quite rightly, as the Minister said, for the relevant Select Committee—the Committee on Digital, Culture, Media and Sport—to deal with. We would never do that, so I will withdraw this probing amendment, but we will come back to this issue. I am not usually a betting man, but I suspect that by the time this Bill and the other Bill go through, we will have got to where both I and the Minister—I think, privately—think we should be. I therefore ask leave to withdraw the amendment.

Amendment, by leave, withdrawn.

Chi Onwurah: I beg to move amendment 21, in clause 1, page 3, line 26, at end insert—

“(2A) The Secretary of State must make regulations under subsection (1) requiring providers of public electronic communications networks and public electronic communications services to carry out an audit of the goods, services and facilities supplied, provided or made available for the purposes of the provision of their network or service to ascertain whether they present a risk to the security of that network or service.”

This amendment is a probing amendment designed to learn how the Government plans to ensure network operators have a comprehensive audit of hardware that is relevant because, for example, it is manufactured by a designated or high-risk vendor.

The amendment goes to the heart of two of our key themes: the scrutiny of the powers in the Bill and the effectiveness of the accompanying diversification strategy. It is a probing amendment, designed to enable us to understand—or to have the Minister clarify—plans to ensure that network operators carry out a comprehensive audit of hardware that is relevant to the Bill because, for example, it is manufactured by a designated or high-risk vendor.

We tabled the amendment for a number of reasons. The first is the Government’s decision, which we welcome, to strip Huawei out of our telecommunications networks.

There are questions about where that equipment is located, the level of software provision, and in particular the exact nature of the revision of the equipment within the network. In addition, the Government have not provided a plan for locating and removing Huawei from our networks; instead, they have opted to leave it entirely to private sector providers.

That might seem appropriate, but as someone with 20 years’ experience in the telecoms sector, I have to say that it is generally not the case—I am not insulting any individual provider—that providers know exactly where every bit of equipment is located and what level of software or build is associated with the equipment.

12.45 pm

James Sunderland: Given that the Bill mandates that vendors could be fined up to 10% of annual turnover or £100,000 a day for violating the terms of their obligations, does the hon. Lady agree that a full audit of all goods and services supplied could be quite draconian and onerous?
Chi Onwurah: I am slightly confused, to be honest, because there was a contradiction there. It is a basic, inherent requirement under the Bill to understand the security implications of a network—the security implications, the security threat and future compromises. It goes to the amendment tabled by my right hon. Friend the Member for North Durham. Given that different components might provide different threats, it is essential to understand the kit that is in the equipment in order to meet the requirements of the security framework. So no, I do not think it is draconian that there should be an audit of the equipment. Indeed, providers should have this information already, but I know from my own experience and the experience of those who gave evidence, which I will come to in a moment, that this is not always the case because networks are so complex, and because our networks today have built up over decades and decades. There is software running in some of our networks that has been around for 40 or 50 years, as well as copper lines that have been around for even longer. So it is not always the case that this information is known.

Christian Matheson: Does my hon. Friend agree with me that having the carrot of an audit might help firms to avoid the stick of a draconian fine that the hon. Member for Bracknell referred to?

Chi Onwurah: As always, my hon. Friend makes an excellent point. Indeed, the audit, which I agree is burdensome if the information is not already in the management systems, which it should be, would, I hope, be less burdensome than the potential fines for not meeting the basic requirements of knowing what is in the network and where it is. Also, that challenge has been made more complex by the subcontracting of different parts of the telecoms networks.

For example, network providers such as Vodafone or Three have primary vendors—currently Ericsson or Nokia—but there might be subcontractors who provide particular elements of the network and particular management elements. We hope that that will be increasingly the case as we seek to open up the supply chains and make them more diverse. A basic and critical requirement for the Bill to be effective is to have a more diversified supply chain. More suppliers go hand in hand with a diversified supply chain, and therefore different types of equipment, of which we will need to keep track.

Mr Jones: The hon. Member for Bracknell has argued that regulations are somehow burdensome on business and unnecessary. It is only when things go wrong that we look back and think, “Wait a minute. That regulation or audit, which was suggested in an amendment, was vitally important.” We must get the context right. These amendments are being tabled not for their own sake but to ensure that security is improved.

Chi Onwurah: My right hon. Friend makes an excellent point. As someone who worked for a regulator for six years, I might be expected to agree with my right hon. Friend on the point of regulation; in this context, regulation should not be seen as a burden. As my hon. Friend the Member for City of Chester set out, it should be seen as a carrot—an incentive—to get things right. Imagine we had known and been able to see how Huawei’s presence in BT’s network, over the last 15 years or so, would rise from small beginnings to becoming the principal vendor. That might have rung more alarm bells and been an incentive to have transparency.

Regulation is also about levelling the playing field and enabling more effective competition. The better providers will do that, but some providers may not. We want a level playing field, particularly because the 2019 UK Telecoms Supply Chain Review stated that there was not an incentive for security in mobile networks. It concluded specifically that there was no incentive for security in mobile networks. Given that conclusion and some of the points provided in the evidence sessions, the Bill does not address incentives to ensure security by design in our mobile networks. It has burdens and fines for not doing that, but it does not have positive incentives.

Christian Matheson: Was not that exactly the problem with Huawei, which has undercut and undermined so much of the telecoms sector elsewhere, either on price or on shoddy workmanship, as my right hon. Friend the Member for North Durham said? This amendment addresses that issue. By raising standards, we help existing and future contributors to the sector to come in and address the problem that Huawei caused.

Chi Onwurah: Again, my hon. Friend makes an excellent point with regard to the way in which Huawei grew in the telecoms sector. I do not want to detain the Committee on that history, but Huawei grew by under-cutting existing vendors, building up scale and making its profits by locking in network providers, despite issues with the quality of the equipment, which, as we have discussed, our security services identified.

Having visibility of network equipment, as well as the level of concentration of any one provider, will enable us, in part, not to get into such a situation of dependency in future. Again, I would emphasise that this is about incentivising what should happen but is unfortunately not always the case. That is not simply my view or that of the Labour party; it is the view of witnesses who participated in our evidence sessions. For example, Andrea Dona said:

“It is vital that the secondary legislation that accompanies the Bill clarifies assets in the telecoms network architecture that will be in scope of the security requirement, so that we can work knowing what we have audited, and knowing that the auditors always had shared with NCSC. We need a clear understanding between Ofcom and us as providers before the legislation is enforced, so that we understand exactly the boundaries and the scope, and we work together, having done the audits, to close any vulnerabilities that we might have.”——[Official Report, Telecommunications (Security) Public Bill Committee, 14 January 2021; c. 13-14, Q10.]
Ofcom said that it was more or less impossible to meet the requirements set out in the codes of practice for the operators, unless it had a detailed asset register of everything in its system. We will expect to see evidence of that, and we expect that it will be regularly checked, audited and so on. We recognise the potential costs of an audit, particularly for smaller providers, although most of them have newer networks and equipment and should have a lot of this information already available. Ofcom is anticipating that this is something it would need to have access to, yet there is no requirement in the Bill or, as far as I can see, in the delegated legislation that has been published to make that requirement.

I have mentioned that this is a probing amendment. I am not sure that it is necessary to have it on the face of the Bill, and it might be that it will be provided for in delegated legislation, but we need a clear and strong strategy for the detection and removal of high-risk components, vendor hardware and software. Otherwise, the Bill will not protect our national security effectively. I hope the Minister will give clarification on that.

**Mr Jones rose—**

**The Chair:** Order. Mr Jones wants to speak, but he will have to wait until this afternoon.

(Ordered, That the debate be now adjourned.—(Maria Caulfield.)

12.58 pm

*Adjourned till this day at Two o’clock.*
Public Bill Committee

TELECOMMUNICATIONS (SECURITY) BILL

Sixth Sitting
Thursday 21 January 2021
(Afternoon)

CONTENTS

Clauses 1 to 5 agreed to.
Clause 6 under consideration when the Committee adjourned till Tuesday 26 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 25 January 2021
The Committee consisted of the following Members:

*Chairs: Mr Philip Hollobone, † Steve McCabe*

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

Sarah Thatcher, Huw Yardley, Committee Clerks

† attended the Committee
The Chair: Before we resume, I have been asked by Mr Speaker to remind people that, when they are not speaking, they should wear a mask. I know this is extremely inconvenient for lots of people, not least me—my glasses steam up. I do not want to be taking names or issuing yellow cards, but may I ask you to try to be mindful of Mr Speaker’s concerns and do the best you can? Hopefully we will all be okay.

Clause 1

DUTY TO TAKE SECURITY MEASURES

Amendment proposed (this day): 21, in clause 1, page 3, line 26, at end insert—

‘(2A) The Secretary of State must make regulations under subsection (1) requiring providers of public electronic communications networks and public electronic communications services to carry out an audit of the goods, services and facilities supplied, provided or made available for the purposes of the provision of their network or service to ascertain whether they present a risk to the security of that network or service.’.—

(Chi Onwurah.)

This amendment is a probing amendment designed to learn how the Government plans to ensure network operators have a comprehensive audit of hardware of interest because, for example, it is manufactured by a designated or high-risk vendor.

Question again proposed. That the amendment be made.

Mr Kevan Jones (North Durham) (Lab): I am demasked. Welcome to the Chair, Mr McCabe. It is a pleasure to serve under your chairmanship. The amendment’s intention is similar to that of new clause 7, which we spoke about earlier. My hon. Friend for Newcastle upon Tyne Central is trying to probe, like I was, how we get operators to ensure that there is a full audit of their telecoms networks. This is not an easy situation. I accept what the Minister said about trying to strike a balance between prosperity—not wanting to put undue burdens on operators—and ensuring security. As my hon. Friend says, with her huge expertise in the field, these networks are not static entities; they develop over time. The example that she cited was that some of the kit in networks is many years old, which may now create security issues that were not evident when the equipment was introduced.

We are not talking about too onerous a burden on the network operators, because they are large companies. I accept that they will be resistant to anything that adds cost because, at our insistence of wanting cheaper phone calls and mobile technology, prices are competitive between the various operators. My hon. Friend therefore makes a good point that there must be a clear level playing field between the operators.

The Bill will ensure that existing Huawei kit is taken out by 2027, even though the networks did nothing wrong by putting in that kit in the first place. Without wanting to carry on my campaign against the Cabinet Office, the Intelligence and Security Committee’s 2013 report “Foreign involvement in the Critical National Infrastructure” shows that the Cabinet Office was made aware of BT’s contract with the Chinese company Huawei in 2003. That the Cabinet Office felt it was not important enough to tell Ministers so until 2006 reinforces my point about its role. That brings me to Ofcom and its capacity, which I will come to later. If we want the most robust system, we will need a system by which we know what is in the network.

There are two issues. I think it is possibly easier for future deployments, because we know what we are putting in. In the debate around Huawei and the security risks, I think it has been very clear. Let us be honest: an operator would be very silly to put in a piece of equipment that was deemed to be high risk for any future roll-out. However, as my hon. Friend says, it is what is already in the network. We accept that some of that will be taken out as a result of the Huawei issue, but a huge amount of equipment will still be in there.

That is before we look at software. What saddens me about the entire debate around Huawei and the telecoms sector is that it has been very hardware-centric. We know that the risks to our network from software are greater in some respects; we have seen examples of where network compromise is easier. Again, how do we get a robust framework in terms of the audit around software—not just what has already been used, but what will be used in the future?

Chi Onwurah (Newcastle upon Tyne Central) (Lab): My right hon. Friend is making some excellent comments. He has raised another issue, which I perhaps did not highlight in my speech, which is that there might be existing equipment that is not necessarily seen as having a security implication but that, as the network evolves, will pose a security threat in the future. I gave an example in the evidence sessions. Say Amazon Web Services was to be bought by a Chinese company. As our networks move the functionality into the software, that will be running in the cloud over the Amazon Web Services infrastructure, which would have a huge potential security impact. An effective audit of where that equipment is now would be critical to knowing the level of that threat.

Mr Jones: I do not disagree with my hon. Friend. That is why we need to get into the idea of the audit. As I said earlier, we basically need a level playing field for operators; we do not want one to have an advantage over another. We also need a clear picture of what we are asking in terms of the audit. On the point she makes regarding web services and the cloud, there is an issue there that I think is worth referring to. It links today’s Bill with the National Security and Investment Bill, which we were discussing yesterday. There was a lot of discussion around what we define as critical—a point she has already raised.

For yesterday’s Bill, the question was what is critical to national infrastructure—for example, a company that is developing software that is then acquired by a state that we deem is a security risk to us. If that equipment or software is being used in our telecommunications
network, does that mean that the network is compromised, and how do we guard against that? There are provisions in the National Security and Investment Bill that enable the Government to stop the acquisition of companies that we consider vital to our national security, but unless we know that in advance, how will we make that decision?

If we have a situation where a small company is providing software for part of our critical national infrastructure for telecoms, how will that be joined up? How will we be able to use the provisions in the National Security and Investment Bill, so that the Business Secretary can block the sale? Likewise, how do we get that connection? We can do that only by the Minister and Ofcom having a very clear indication from day one—I do not think it will be possible from day one, but from some time into it—what is in our network, not just now, but into the future. That will be important.

That brings us to the role of Ofcom. We have seen a development of regulators in this country. I am not a great fan of regulators, because I think it is a way for Ministers to palm off their responsibilities to third parties and then stand back and saying, “If it all goes wrong, it is nothing to do with me, guv—it is these independent organisations.” A long time ago—perhaps it is a bit old-fashioned—the General Post Office used to be responsible for this type of thing, and I am currently reading the excellent new history of GCHQ that has come out, which I recommend to everyone. It is fascinating to read about some of the challenges—things that apply to this Bill—such as, in the first world war, what was conceived as national security and who was responsible for it. Was it the GPO, the military or someone else?

How will Ofcom be able to look at a network and say, “Yes, we are satisfied that there is nothing in there that is a matter of national security”? They do not know. I do not think for one minute that we are going to have a situation whereby this Government or any future Government will suddenly throw so much money at Ofcom that a huge army of inspectors will be climbing up poles and going into operators’ offices to check source codes and so on. That is not going to happen.

From a practical point of view, the operators will have to be responsible for providing that information to Ofcom. Whether it is in the Bill or in the guidance, it must be clear what is expected of operators. It is no good looking back in hindsight and saying, “We should have done that,” when something happens. The operators will just say, “You did not tell us we had to do that,” or, “We didn’t know about that.” It has to be very clear, to prevent a competitive advantage between different companies, that there is one standard. They also have to know what we are asking for. Then, taking the telecoms hat off and putting the national security hat on, from the Government’s point of view, that needs to be very clear as well, because we need to be reassured that the components and software in those networks, now and in the future, are not a national security risk.

That brings us to an issue that I have already raised. I am not someone who thinks that every time we go to bed at night, we should look under the bed to see whether the Chinese are there, unlike some members of the China Research Group, but there is an issue about the way in which China will look at supply chains as a way of getting access, for two reasons. The first is national security. The second is commercial reasons—dominating the market, which is what China has done with Huawei. How will we identify that, without having some type of audit process? I do not think that everything to do with China is bad, but a huge number of the components in all our mobile phones in our pockets today will have come from China, including Ericsson and Nokia hardware.

James Sunderland (Bracknell) (Con): I am enjoying the right hon. Gentleman’s logic. He talks a lot of sense, which is great. I am really intrigued by his insistence that the Government place these obligations on the National Cyber Security Centre and Ofcom. In my humble view, and knowing how those organisations work, it is likely to be the case that the Joint Forces Intelligence Group, GCHQ or the National Cyber Security Centre inform Government where there have been transgressions of security and breaches. I am intrigued by the counter-logic with where I think we need to be.

Mr Jones: This is a remarkable day. This morning I was told that my contribution to the debate was inspiring, and now I am being told that I am talking sense—I thank the hon. Gentleman for making my day.

The hon. Gentleman is right, but he is also wrong. He is right in the sense that there are threats that will come through GCHQ and others—they will say to operators, “You’ve got to be careful of these things.” Where he is wrong, though, is with the idea that somehow GCHQ can take a guess at what is in the network. It does not have that capability. Going forward—the emphasis in this country, in the Bill, in terms of looking at telecoms security—yes, the bar has been raised substantially.

There will be occasions when GCHQ—it does it already—contacts operators and others to say, “Beware of this software or this thing.” I accept that as a proactive approach, but handling backwards will also be important. How do we have a gold-plated system, whereby we have GCHQ doing what the hon. Member for Bracknell suggested they are already doing, but one that also matches up with operators taking responsibility to say, “We have spotted something and are doing something about it”? It is pulling the two things together.

Chi Onwurah: Part of the challenge is that the operators do not know themselves and, as we have discussed, there are no incentives for them to find out. To give an example, Virgin Media took over from NTL, which I think took over from the 13 different cable providers in the franchises of the ’80s, and the BT mobile network was bought partially from EE—so there are takeovers and acquisitions, and partners may not know, and do not necessarily have an incentive to find out unless we put in a requirement.

Mr Jones: My hon. Friend makes the point precisely: the way in which telecoms have developed in this country has been piecemeal, only developing now into the four main operators. I hope we will try to get others into the market.

We are to blame for that, as consumers, because we have demanded ever lower prices for our mobile services. Does that suggest that the operators have taken shortcuts? No, I am not suggesting that, but consumer preferences
have driven down price, and therefore the costs of what those operators provide in delivering the services that we all take for granted. Let us be honest: the Chinese saw the opening door for Huawei—that is why they bought into and flooded the market, putting Government loans behind it. Can we blame the operators for saying, “Well, actually, this is a good deal—we can get good deals”? But they cannot.

I am interested to know from the Minister how, looking forward, we are going to do that. I accept that something will be done under the regulations that the Government will put out, but how will we look backwards as well? As my hon. Friend the Member for Newcastle upon Tyne Central said, there is a lot of legacy equipment there, and it is important for Ofcom to have a clear understanding of what is in the networks.

The Parliamentary Under-Secretary of State for Digital, Culture, Media and Sport (Matt Warman): It is a pleasure to serve under your chairmanship, Mr McCabe.

We are redefining UK telecoms security, but I worry that we are also redefining the aspiration of the hon. Member for Newcastle upon Tyne Central to crack on, so I will try to be brief. The good news that I can deliver, briefly, is how the aspirations of both the hon. Lady and the right hon. Member for North Durham are met in the legislation, and how we envisage those aspirations’ being implemented. As the Committee is aware, the Government have published an early draft of the security regulations. Certain draft requirements are relevant to the aims that we have talked about today. If hon. Members look at regulation 3(3)(a), with which they will be

Chi Onwurah: I had looked at those requirements. I appreciate that they are drafts, but they talk about identifying issues. They do not say “audit”.

Matt Warman: I think this would be impossible to identify without carrying out some kind of audit. There is a danger of a semantic argument, but I understand the point the hon. Lady is making. We want people to be in the position to make the kind of identifications that we are requiring. I do not see how they could do that without the records to which she refers, in terms of both the existing kit and future kit that they might put into their network.

Christian Matheson (City of Chester) (Lab): This is an important point. The criticism that I will articulate later is that too much of the Bill is based on an assumption that the players in the sector will automatically do the right thing. For example, there is an assumption of a dialogue between Ofcom and the major players. Will the Minister think about whether he is satisfied that an assumption goes far enough in something as important as this?

Matt Warman: The regulation that I cited is an example of the Government not relying on assumptions. It is an example of us publishing, in advance, exactly the sort of material that demonstrates that this is not assumptions, and that it is there in black and white. That is an important distinction and it demonstrates the cross-party consensus that we have had thus far. We continue to be on the same page in terms of the level of detail required.

The evidence sessions with industry demonstrated that national providers already maintain some asset registers. Witnesses were clear that those registers are maintained and updated as technologies are updated. That is an important part of the existing landscape, but our regulations will ensure this kind of best practice is extended across public telecoms providers.

In addition, the Bill contains measures with regard to the use of particular vendors’ equipment. Inspection notices under clause 19 enable Ofcom to carry out surveys of a specific network or service where Ofcom receives a monitoring direction from the Secretary of State to gather information on a provider’s compliance with a designated vendor direction. Alongside that, clause 23 enables the Secretary of State to require the provision of information about the use of goods, services or facilities supplied, provided or made available by a particular person. That could be used to require information about a provider’s use of a particular vendor’s equipment.

Taken together, the issues that have been raised are not only entirely legitimate, in the view of the Government, but are addressed in black and white already, both in the Bill itself and in the drafts that we have published. We are ensuring that “hardware of interest,” whatever that might be, is subject to proper oversight and monitoring. That objective does not need the approach that might come as a consequence of this amendment, because it is already there. For that reason, I welcome the probing nature of the amendment. I hope that my answer has satisfied some of the concerns, and I look forward to doing so further in future answers.

Chi Onwurah: It is a pleasure to serve under your chairmanship, Mr McCabe, and I thank the Minister for his comments. I also thank my right hon. Friend the Member for North Durham and my hon. Friend the Member for City of Chester for their comments. This amendment is probing, so we will not push it to a Division. I would like to say two things to the Minister. Although it is true that the providers were confident that they had an asset anywhere their equipment was, other experts who gave testimony in the evidence sessions were not. My experience of networks is that there are multiple systems and this information is not easily accessible or searchable.

I am reassured by the Minister saying that his view is that these requirements could not be met without there having been some kind of audit, to have that information ready. I ask him to write to me, if possible, stating which provisions in the requirements set that out. I beg to ask leave to withdraw the amendment.

Amendment, by leave, withdrawn.

Question proposed, That the clause stand part of the Bill.

Matt Warman: It is good to reach this landmark point. I do not propose to go over all the ground we have covered, because we have already covered a large chunk of this in discussing the amendments.
As I mentioned, proposed new section 105A means that telecoms providers will need to take appropriate action to ensure adequate security standards and limit the damage caused by any breaches. To support that duty, the proposed new section will create a new definition of “security compromise”. The definition is purposely broad. It includes anything that compromises the availability, performance or functionality of a network or service, or that compromises the confidentiality of the signals conveyed by it. That addresses some of the points made by the right hon. Member for North Durham a moment ago. This is a comprehensive approach that will help to ensure providers protect their networks and services properly in the future.

Earlier, I mentioned law enforcement and national security. This part of the Bill excludes certain conduct that is required or authorised under national security legislation or for law enforcement from the definition of “security compromise” in subsections (3) and (4). Those subsections also clarify the fact that, for example, disruption of the use of unauthorised mobile phones in prisons would not be a security compromise.

Proposed new section 105B will give powers to the Secretary of State to make regulations imposing duties to take specific security measures. The power will enable more detailed requirements to be imposed on providers, further to the overarching duty set out in proposed new section 105A(1). This will give greater clarity to providers about the measures that they must take. It will also allow the legal framework to be adapted as new threats arise and technology changes.

These security requirements deliver on our commitment in the telecoms supply chain review to place targeted, actionable and proportionate requirements on a statutory footing. Taken together, the new overarching security duty and requirements will, in secondary legislation, make clear what the Government expect of public telecoms providers. The provisions in the clause are crucial for improving the security of our telecoms infrastructure.

I am happy to support the clause.

### Clause 2

#### Duty to take measures in response to security compromises

**Question proposed,** That the clause stand part of the Bill.

**Matt Warman:** We are one thirtieth of the way there. The clause will place a duty on providers to take measures in response to security compromises through proposed new section 105C. When managing security, providers should seek to reduce the risk of security compromises occurring under their duty in proposed new section 105A. As security threats and attacks evolve, it will never be possible for providers to reduce that risk to zero. Therefore, should a security compromise occur, it is crucial that providers take swift and effective action to mitigate its effects. Taking action quickly will also help to mitigate the risk of any further incidents.

Mirroring the approach taken in clause 1, the new duty in proposed new section 105C is overarching and sets out a general duty on providers. It is supported by proposed new section 105D, which will provide the Secretary of State with powers to make regulations requiring providers to take specific measures in response to security compromises of a description specified in regulations. Although it will clearly not be possible to anticipate every security compromise that might occur and to set out how providers should respond, this will enable more detailed provision to be made in appropriate cases. Measures can be specified in the regulations only where the Secretary of State considers those measures appropriate and proportionate.
In practice, the first set of requirements will be contained in a single set of regulations made under the powers of proposed new sections 105B and 105D. A draft of the regulations has already been made available to members of the Committee, and published on gov.uk. Regulations made using this power will give providers clarity about the measures that they need to take, and having those measures set out in secondary legislation has the benefit of allowing the regulations to be reviewed as technology and security threats change over time.

In summary, this duty on providers is an integral part of the new framework, which will ensure providers take control of the security of their networks and services at a time when the UK stands on the cusp of a 5G and full fibre revolution. We must keep those technologies secure to enjoy their full benefit, and the clause is essential to doing that.

Chi Onwurah: We are cracking on: clause 2 is taking but a few minutes. The Opposition recognise the critical importance of our network providers taking responsibility for the security of their networks, and that there can never be a zero-risk network. Given that network communications are ever present in almost every aspect of our life and of our nation’s economy and security, it is right and appropriate that the Bill should put requirements in place, both on the operators and in response to specific security compromises.

I should like to have better understood how we would expect network operators to respond to a compromise such as the SolarWinds one, for example, but I expect that the clause will at least place the right duties on network operators, and I am content that it should stand part of the Bill.

Question put and agreed to.

The Chair: This must be down to that productivity seminar they sent me on. Still, nothing lasts forever.

Clause 3

CODES OF PRACTICE ABOUT SECURITY MEASURES ETC

Mr Kevan Jones: I beg to move amendment 6, in clause 3, page 5, line 4, at end insert—

“(ia) the National Cyber Security Centre;”

This amendment would require the Secretary of State to consult the National Cyber Security Centre on any draft code of practice about security measures under new section 105E.

The Chair: With this it will be convenient to discuss the following:

Amendment 10, in clause 3, page 5, line 8, at end insert—

“(iii) the National Cyber Security Centre;”

This amendment requires the Secretary of State to consult the National Cyber Security Centre before issuing a code of practice about security measures.

Amendment 5, in clause 4, page 7, line 41, after “OFCOM”, insert—

“and the National Cyber Security Centre”.

This amendment would require providers to inform the National Cyber Security Centre, as well as OFCOM, of any security compromise.

Mr Jones: We are romping through the Bill, aren’t we? Two clauses in less than 15 minutes.

Again, these amendments are probing. I might sound like a broken record, but my aim with them is to ensure that national security and those who deal with national security decision making are at the centre of the decisions that are taken. Amendment 6 would require the Secretary of State to “consult the National Cyber Security Centre on any draft code of practice about security measures under new section 105E.”

The Minister will say, “Well, it is self-evident that they will do that,” but going back to my Robin Day analogy from this morning, legislation needs to survive him, me and everyone else. The guidance will change over time, and we have to ensure that whoever is sitting in the Minister’s seat in 10 years’ time—hopefully, it will not be the current Minister, not for any unfair reason, but because he has gone on to higher and better things—the onus is on the Secretary of State to consult. Having that on the face of the Bill, or at least some discussion about it, would reinforce that, because the Secretary of State will move on, and there will be new civil servants, who might not have as clear an indication as the Minister will give today, or perhaps a Minister who thinks that this is the key part.

It might be a bit anorak-ish, but the problem with the national security world, which I inhabit occasionally, is that people can see everything through the national security prism—although I am not sure that that is the case for everyone. It will be important to ensure that the individuals at the National Cyber Security Centre have a real input, and not just to say that they will be consulted. The NCSC, which was introduced at the tail end of the coalition Government, is the only positive thing I can think of that that Government did. We now have a world-beating centre that protects our national security and also does a very strange thing: it looks to the secret world, but also looks outwards, engaging with the industry and individual citizens, too.

That is now being replicated around the world. I chair the science and technology committee of the NATO Parliamentary Assembly. On our visit to the UK the year before last, we visited the centre, and most of my parliamentary colleagues from across the world, including the US, were quite impressed with how it balanced complete secrecy about things that need to be kept secret and having that outward-looking approach. I am really just trying to see how we can ensure that going forward.

Amendment 5 seeks to ensure that the NCSC, as well as Ofcom, is informed of compromises and breaches. I am sure the Minister will tell me that Ofcom and the NCSC have such a symbiotic relationship that that information will automatically be transferred, but again we are assuming a lot about what will be done. It is important that this Committee at least discusses how we ensure that that continues. I will come to Ofcom personnel, but various comments have been made. I asked the head of Ofcom about Ofcom’s expertise in dealing with these issues, and this comes back to the point I made to that witness. This is about mindset. Whether we like it or not, people in the security world think differently from the rest of us in how they approach things. Ofcom will have a learning curve, not only in recruiting the individuals with the capability to do this work, but in ensuring the culture to react to these issues. My two amendments seek to ensure not only that
national security is at the heart of the Bill, but that practitioners have a clear focus on national security risk.

2.45 pm

Chi Onwurah: I rise to support my right hon. Friend’s excellent comments and to add a couple of points on amendment 10, which would require the Secretary of State to consult the National Cyber Security Centre before issuing a code of practice about security matters. My right hon. Friend spoke ably about the amendment’s intent to ensure security input on national security measures. That sounds basic, so I hope the Minister will explain why he feels it is unnecessary to make that explicit in the Bill. My right hon. Friend suggested that perhaps it should go without saying, but as we heard in the evidence sessions and have already discussed, the evolving security landscape and the change that the Bill represents, through the new powers for the Secretary of State and Ofcom, make it particularly important to set that out expressly.

The Bill looks at many issues to ensure the security of our networks from supply chains to requirements on network providers as well as raising technical issues, and Ofcom will need to do a lot specifically, so it is important to have a specific reference to the security function of the National Cyber Security Centre.

It came across clearly in the evidence sessions that Ofcom will not be making national security judgments. Lindsey Russell said:

“It is important to say that, across the scope of the whole Bill, it is not Ofcom’s role to make national security judgments. That is really important. Clearly, that is the Government’s and the Secretary of State’s role, taking advice from the NCSC and the intelligence agencies.”—[Official Report, Telecommunications (Security) Public Bill Committee, 19 January 2021; c. 89, Q113.]

In introducing the code of practice, it is essential to ensure that security input and expertise. I do not see why the Minister would object to including such a requirement in the Bill. Unfortunately, we are not always as joined up as we would like to be. There are numerous examples of issues that could have been prevented, had agencies of Government done what might have been expected of them and talked to each other. As the Bill involves network operations and deep technical and security issues, a requirement to consult the NCSC is particularly important, and that is what the amendment would achieve.

Matt Warman: I apologise in advance, having said that we should crack on, for detaining the Committee for a few minutes on this group of amendments. They relate to clauses 3 and 4, which deal with the codes of practice for security measures and informing others of security compromises. Ultimately, the new telecoms framework comprises three layers. There are strengthened overarching security duties set out in the Bill, there are specific security requirements in secondary legislation, and there are detailed technical security measures in codes of practice. Clause 3 deals with the final layer of the new security framework. Specifically, it provides the Secretary of State with the power to issue and revise the codes of practice and sets out the legal effects of any published codes of practice.

Clause 4 addresses what would happen should there be a security compromise. It puts in place a process for users to be informed of significant risks of a security compromise. The clause also places a duty on public telecoms providers to inform Ofcom of any security compromises with significant impacts, and it creates the power for Ofcom to inform other persons in turn, including users.

I turn now to amendment 5, which seeks to ensure that the NCSC is also informed of security compromises. From a drafting point of view, the NCSC is part of GCHQ, and I take the amendment to refer to GCHQ in that sense. Within the new telecoms framework, the Department for Digital, Culture, Media, and Sport will set the policy direction, Ofcom will regulate and the NCSC will provide technical and security advice. As the UK is an world-leading national authority on cyber-security, we expect the NCSC to share its expertise with Ofcom in order to support the implementation of a new telecoms security framework.

For that reason, the Government absolutely agree that it is crucial that the NCSC receives information about telecoms providers’ security. That is why such information-sharing provisions already exist. Under section 19 of the Counter-Terrorism Act 2008, Ofcom or the Secretary of State is able to share with the NCSC any information that would support the NCSC in carrying out its functions. That would of course include the passing on of details of security incidents. Under new section 105L of the Communications Act 2003, which this Bill inserts, Ofcom must report all serious security incidents to the Secretary and State and can pass on information about less serious incidents as well. On receiving such information, the Secretary of State could then share the information with the NCSC, as I have set out. Although these probing amendments are well-intentioned, it is obvious that the provisions are already there.

Chi Onwurah: I thank the Minister for his response to the amendments. He is focusing on the fact that it is possible for information to be shared, but it is not required. I understand that the Bill as drafted, and preceding best practice, means that it is possible for information to be shared. My concern is that it is not required.

Matt Warman: I understand the hon. Lady’s point, and I will come to something that I think will address it in a moment. Before I do, I will speak to amendments 6 and 10, as they would be functionally identical amendments to new section 105F in clause 3.

New section 105F sets out the process for issuing a code of practice. It requires a statutory consultation on a draft code of practice with the providers to whom the code would apply, Ofcom and other persons such as the Secretary of State considers appropriate. The amendments would apply an additional requirement to formally consult the NCSC when publishing a draft code of practice. I can reassure the Committee that we will continue to work closely with technical experts at the NCSC, as we have done over a number of years.

The telecoms supply chain review demonstrated the Department’s capability to work with our intelligence and security experts to produce sound recommendations, backed by the extensive and detailed security analysis that I know Members of all parties would like to see. That initiated the next phase of the collaborative work that culminated in the introduction of the Bill, and the codes of practice continue that theme. The purpose of such codes is to provide technical security guidance on the detailed measures that certain public telecoms providers should take to meet their legal obligations.
We have already been clear that NCSC guidance will form the basis of an initial DCMS-issued code of practice. The NCSC has already developed a set of technical measures that is in the process of being tested with the industry, and those technical measures have been refined and improved over the last two years. The NCSC will continue to update the measures to reflect any changes in the landscape of threats, as the right hon. Member for North Durham described, and the relationship between the work of the DCMS and that of the NCSC means that such changes would be reflected in the code of practice. Alongside the DCMS and Ofcom, the NCSC will play a key role in advising public telecoms providers on how to implement detailed codes of practice.

Mr Jones: I agree with the Minister, in the sense that I think he and the Secretary of State at the DCMS are committed to there being very close working, but as I said, he ain’t gonna last forever. An issue will come up —in fact, it came up last night on the National Security and Investment Bill—when operators and others say, “Actually, from a commercial point of view, this is more paramount,” or, “This is what we should be doing.” The Secretary of State will come under a lot of pressure to perhaps look at prosperity issues rather than security issues. I just wonder whether, without the relevant provision in this Bill, a future Secretary of State could say, “Well, I’m going to ignore that issue, because I want to pander to”—well, not pander to—“accept the commercial and prosperity arguments.”

Matt Warman: The right hon. Gentleman keeps going on about ministerial impermanence, but I will not take it personally.

Mr Jones: I talked about promotion.

Matt Warman: Too kind! The key part to this is that, obviously, Ofcom remains an independent regulator and will be working closely with others. The right hon. Gentleman makes a fair point about the inevitable balance between national security and a whole host of other issues, but ultimately that independence is absolutely essential. In the light of our long-standing and established working relationships across the DCMS, NCSC and Ofcom, it seems reasonable to say that there is a track record demonstrating what he has asked for. But given the Committee’s interest in the role of the NCSC in this regime, I will just make one last point. Its role is not explicitly described in the Bill, as the NCSC already has a statutory remit, as part of GCHQ, to provide technical security advice and to receive information on telecoms security for the purpose of exercising that function.

The NCSC and Ofcom will very soon publish a statement setting out how they will work together. I think that addresses some of what the hon. Member for Newcastle upon Tyne Central mentioned; I believe she has some familiarity with Ofcom. I think it is right, because they are independent, that that statement comes from them, as well as the Government expressing a view on this. The statement will include information on their respective roles and their approach to sharing information on telecoms security, and it should provide greater clarity, which hon. Members are entirely legitimately asking for, about the NCSC’s role, including how it will support Ofcom’s monitoring, assessment and enforcement of the new security framework.

I hope that the sorts of matters that I have talked about provide the kind of reassurance that Members have asked for.

Mr Jones: A statement is a welcome step forward, but—the Minister can write to me on this; he need not respond to me today—what is its legal weight? Again, I am not wanting to consider the Minister’s demise, but I would like to know that future Secretaries of State and Ministers will use it as the template and will not be able to say, “Well, we are going to ignore that statement.” That would be very welcome, because it would bind the two organisations together, which is important, and ensure that the security aspects were taken into consideration, but will the Minister just write to me, saying what weight the statement would have? I have to say that I sympathise; I do not like Christmas tree Bills that start having things added on. If it could be done in a complete way, I would be quite happy with that. The only thing that I want to know is, basically, what its status will be in future. I beg to ask leave to withdraw the amendment.

Amendment, by leave, withdrawn.

Question proposed, That the clause stand part of the Bill.

3 pm

Matt Warman: The Committee has already heard me talk about some of this, but I think it important to provide a little more detail. The code of practice, which we have discussed, is a fundamental building block of the regime and will contain more specific information on how telecoms providers can meet their legal duties. It will provide guidance on how, and to what timescale, certain public telecoms providers should comply with their legal obligations, and will be based on technical analysis by the NCSC. Individual measures will therefore reflect the best protections against the most pressing threats to network security. The code will, for example, set out the detailed technical measures that should be taken to segregate and control access to the areas of networks that process and manage customers’ data.

We recognise of course that different companies have different ways of setting up and running their networks, and because our telecoms market is dynamic and competitive, providers range in scale from multinational giants such as Vodafone down to innovative local start-ups. We want therefore to ensure that the code of practice is proportionate, and that public telecoms providers take appropriate security measures.

I will touch as briefly as I can on how we intend to achieve that proportionality through a tiered system. Tier 1 will contain the largest national-scale public telecoms providers. Should any of those providers have a significant security incident, it could bring down services to people and business across the UK. Those operators will have the greatest level of oversight and monitoring from Ofcom. Tier 2 will contain medium-sized public telecoms providers. Those providers may not be as large, but in many cases they are critical to regions and to business connectivity. They are expected to have more time to implement the security measures set out in the code of practice.
Tier 3 will contain the smallest public telecoms providers, including small businesses and micro-enterprises, which, of course, must also comply with the law. They are not anticipated to be subject to the measures in the code of practice, but will need to comply with their legal duties as set out in new sections 105A and 105C, and in any regulations. Our expectation is that Ofcom would regulate those providers more reactively.

New section 105F describes the process for issuing a code of practice. When the Government publish a draft code of practice, we will consult with industry, Ofcom and any other appropriate persons. Specifically, publishing the first code of practice will include consulting on the thresholds of each of the tiers that I have described and on the timings for their implementation. Following the consultation period, and once the code is finalised, it will be published and a copy will be laid before Parliament.

New section 105G gives the Secretary of State the power to withdraw a code of practice. Again, that will follow consultation with industry and Ofcom. A notice of withdrawal will be laid before Parliament. The legal effects of the code of practice are described in new section 105H. To be clear, the code of practice is guidance only; it is an important tool that operators should use to comply with their legal duties.

Mr Jones: Is the Minister saying that the code of practice is the standard that providers are expected to meet? Is it the legal bare minimum or do we expect them to do more than what is set out in the code of practice? What is the direction of travel?

Matt Warman: The legislation places a duty on providers. Meeting the strictures of the code of practice would be the way of demonstrating that they were meeting that duty as an initial step, but of course, we see individual companies making decisions, for a host of reasons, to exceed codes of practice in every area of regulated life, and I would expect that to continue in the area in question as well.

Where relevant, provisions in a code could be taken into account in legal proceedings before courts or tribunals, which I think gives some sense of their status. That would include any appeals against Ofcom’s regulatory decisions heard by the Competition Appeal Tribunal. Ofcom will take account of the code of practice when carrying out its functions as required in new section 105H(3) in relation to telecoms security, as I have just described.

Under new section 105I, if Ofcom has reasonable grounds for suspecting that a telecoms provider is failing, or has failed, to act in accordance with a code, it can ask public telecoms providers to explain either how they meet the code of practice or, if they do not meet it, why. For example, if the network set-up of a particular telecoms provider meant that it could achieve a level of security equivalent to that in the code by other means, it could explain that in its statement responding to Ofcom. In such a case Ofcom might be satisfied that the provider was complying with its security details, but hon. Members will see that we are again trying to ensure a proportionate approach to the relevant part of the framework.

We believe that the code of practice will provide an appropriately flexible framework, which will be able to change as new security threats evolve, providing clarity for telecoms operators on what is required of them by this new telecoms security framework.

Chi Onwurah: I will not detain the Committee very long either, as we agree about the importance of codes of practice. I will not say that I am entirely reassured to hear of the statement being issued by Ofcom and the NCSC on how they will work together, but I certainly think that it is a positive development, and I hope we will be able to see it before the Bill progresses to the House.

On the codes of practice, as my right hon. Friend the Member for North Durham set out, it is important that the sector should understand the standard to which it will be held. I have some concerns about the tiering system, because, as was made clear by a number of witnesses during the evidence sittings, all networks are joined up and we are only as secure as the weakest link. At the same time, it is important to have a proportional burden on new entrants as we indeed hope to diversify the supply chain.

I understand, although perhaps the Minister can clarify the point, that the codes of practice will not refer to the diversification of the supply chain, despite the fact that having a secure network—we shall debate this in more detail—is dependent on having a diverse supply chain. I have made the point a number of times, and will make it repeatedly, that the lack of linkage between the diversification strategy, implementation and the security of our networks is an ongoing cause for concern. However, having made those comments, I do not object to the clause.

Question put and agreed to.
Clause 3 accordingly ordered to stand part of the Bill.

Clause 4

Informed others of security compromises

Question proposed, That the clause stand part of the Bill.

Matt Warman: As with clause 3, I have already spoken to clause 4, addressing an amendment on this issue. It will be crucial that we ensure that the Government, Ofcom, public telecoms providers and their customers have the information that they need to understand when security compromises have occurred, and then use the knowledge to prevent compromises in the future. New section 105J requires that providers inform their users of significant risks of security compromises and actions that they can take to avoid or mitigate any adverse consequences.

We want to ensure that this is done in a transparent and open way, so the clause specifies that telecoms users should be notified in clear and plain language, and given a named contact they can get in touch with if they have any further questions. Giving users that information will help to ensure that, where possible, they can take swift action to protect themselves and raise broader awareness.

New section 105K requires security compromises to be reported to Ofcom. That information will provide Ofcom with insight into the security of individual telecoms providers and security risks across the landscape, enabling us to target its regulatory action more effectively. The Bill also requires that providers report pre-positioning attacks on the network. These are attacks that do not affect the network or service at the time but allow access
that could result in further security compromises. These attacks pose real risks but too often remain invisible to a regulator.

Finally, under new section 105L, Ofcom is required to share information about serious security compromises with the Government. It may also share information on less serious compromises if, for example, it would help the Government with developing telecoms policy and future regulation.

The clause explains how Ofcom can share information about security compromise with other groups and organisations, and the Bill allows information sharing at Ofcom’s discretion with overseas regulators, other providers, telecoms users and, where appropriate, the wider public. It allows Ofcom to advise network and service users of the measures that they should take to prevent, remedy or mitigate the effects of the security compromises, to direct providers to give such advice themselves.

The clause ensures that the regulator has access to the information that it needs, and will help to ensure that the entire industry is aware of new and evolving risks and can respond accordingly—be that a customer changing their password or an operator tightening its defences against a new attacker.

Chi Onwurah rose—

Matt Warman: I will pretend I have not finished, and give way to the hon. Lady.

Chi Onwurah: I thank the Minister, as always, for graciously giving way. I will make this point later, but I want to give the Minister the opportunity to consider how the requirement for Ofcom to notify users might work with the Information Commissioner’s requirement on data controllers to also notify users when there is a data hack.

Matt Warman: Obviously, there could be an overlap in those notification requirements, but our expectation would not be that anyone would receive multiple notifications. That is why there is an emphasis on the nature of communications being clear and obvious to laypeople.

Mr Jones: Speaking gives me an opportunity to take my face mask off. I will make a few points about clause 4, which is broadly welcome because it clarifies for operators what their responsibilities are, not just from a national security point of view but from a consumer point of view. I think there is an issue, though, which my hon. Friend the Member for Newcastle upon Tyne Central raised.

Again, I do not want the Minister to respond now, but I think the crossover with the Information Commissioner might be one area that we need some clarity on. Is there an example of this? Yes—the TalkTalk case. People might look at this Bill and think national security is about the Russians or the Chinese hacking, but that was a criminal act that led to a lot of people’s data being compromised. From a constituency point of view, as any Member of the House at that time will know, trying to get TalkTalk to do anything about that, in terms of the losses that people incurred, was virtually impossible. That is why these clauses are so important.

Chi Onwurah: Is my right hon. Friend aware that the hack used by the young person had been around for longer than that young person had been alive? That is an indication of the low level of security TalkTalk had in their network; they had not been able to address a known hack that had existed for at least 16 years. The Bill aims, in part, to address that and the consequences of that lack of security for our constituents.

3.15 pm

Mr Jones: My hon. Friend is correct. A lot of the debate has been about hardware, but the biggest threat to our national security, in terms of telecoms, is from hacking and cyber-attacks. The changing nature of the threat is interesting. There are state actors and there is organised crime, acting on behalf of states, but there is also, as referred to by my hon. Friend, some poor teenager who thought it was a good idea. The TalkTalk case showed the emphasis they put on the security of their network. Not just clause 4, but the whole Bill, puts the onus on the operators, which is why it is so welcome. Never again could they be accused of not knowing their responsibilities.

New section 105J requires providers to take “reasonable” steps to inform users about the risk, the nature of the security compromise, the steps the user could take in response, and the name and details of the person to contact. That is fine, but how to respond might be a matter for Ofcom. That is important, because people might then quickly take steps to stop compromises to their security.

The Bill lays out penalties for telecoms operators, but what about the consumer and people who have lost money because of data breaches? Do I assume that the Bill does not change that? It begets it up, but I assume that any mitigation or compensation that should be paid to individuals who have been compromised would be an issue for Ofcom. When we had the TalkTalk compromise, getting TalkTalk to do anything was like trying to get blood out of a stone. That is important from the point of view of consumers.

It is important that the Secretary of State is informed, but how will that be done? I presume GCHQ and others would do that. Would that lead to lessons learned or to a notice being given to other operators that that has happened? Would that be done by Ofcom, the National Cyber Security Centre or GCHQ, or would it be a combination of all of them? It comes back to the point made by my hon. Friend the Member for Newcastle upon Tyne Central: this is a risk and this clause puts the onus initially with the operators, where it should be.

Chi Onwurah: We are cracking on at such a pace that I lost my place somewhat. I had forgotten that we are now discussing clause 4. My apologies, Mr McCabe.

My right hon. Friend the Member for North Durham has already addressed some of the points that I wanted to make, but let me say that we welcome the duty being placed on providers to report security incidents. I have long campaigned, in relation to cases such as the TalkTalk incident, to make that duty clearer and more comprehensive regarding the information that needs to be shared with users and those who are affected, and for them to have some kind of right of redress, which is effectively part of the Bill.
I welcome the requirement in clause 4 to inform others of security compromises, but will the Minister provide more clarity? There is some indication of the range of actors that the providers and Ofcom must inform, but I do not feel that there is an understanding of the level of information that will be shared with different actors. For example, if the public are to be informed of a security breach, compared with the requirement from the Information Commissioner’s Office, which, as I said, actually goes far enough, what level of information might be shared with other actors, such as other networks? My right hon. Friend talked about who else might be informed. It is also clear that the sharing of information will probably need to evolve over time, as the nature of compromises and their potential reach changes. I wonder how these requirements might be adapted to reflect that.

I will just say a little about the sharing of information with overseas regulators. If that is clearly set out in the Bill, I am unable to find it. Presumably, such data sharing will still have to conform with the requirements of our data protection legislation. Will it also reflect international data-sharing gateways for criminal prosecution purposes?

Those are just some general comments. We welcome the clause.

Matt Warman: I will reply briefly. On the point about compensation, essentially new section 105W of the Communications Act 2003, which is inserted by clause 8, covers the civil liability point, which I think opens the door that the right hon. Member for North Durham seeks to open. Then there are the notifications to industry of what is essentially best practice and recent threats. Of course, as he implied, there is a balance to be struck with the existing work of all those involved, but ultimately it would feed into the codes of practice, so there is both an informal and a formal mechanism, if I can put it like that.

On the hon. Lady’s final point about the international sharing of information, it would depend on the nature of the information, as she implied. Some of it would pertain to national security, and some of it would pertain to the kind of criminality that she has spoken about, where there are existing provisions as well. In that sense, of course, it is all covered by our own data protection regime, which has the sorts of carve-outs I have just described but operates in that holistic framework.

Mr Jones: Will the Minister write to us on the issue of data and the link to the Information Commissioner?

Matt Warman: I am not sure I fully understand the right hon. Gentleman’s point.

Mr Jones: I raised the point, as did my hon. Friend the Member for Newcastle upon Tyne Central, that we are asking operators to inform individuals about data compromises. That is welcome, but as my hon. Friend said, there might also be a breach of the Information Commissioner’s regulations, and we just wanted to get some idea of how the two would mesh together. I do not expect the Minister to know now, but could he write to us to say how the two would interact?

Matt Warman: As I said in response to the hon. Lady, there is obviously a potential overlap. The focus of this Bill is on clarity of communication to the consumer, but I am very happy to write to the right hon. Gentleman or the Committee with further details of that potential overlap.

Chi Onwurah: The Minister is being incredibly generous with his time. To clarify what we are hoping to receive, as he has indicated, we would not want the ICO to be sending out notifications to 2 million people who had been affected by a hack, and Ofcom to be doing that as well. We would expect there to be co-ordination in that regard, and we would just like to see that set out.

Matt Warman: I am very happy to do so. I think it is obvious that clarity of communication would be incompatible with duplication.

Question put and agreed to.
Clause 4 accordingly ordered to stand part of the Bill.

Clause 5
GENERAL DUTY OF OFCOM TO ENSURE COMPLIANCE WITH SECURITY DUTIES

Christian Matheson: I beg to move amendment 11, in clause 5, page 9, line 41, at end insert—

“(2) Providers of public electronic communications networks and public electronic communications services must notify Ofcom of any planned or actual changes to their network or service which might compromise their ability to comply with the duties imposed on them by or under sections 105A to 105D, 105J and 105K.”

This amendment would require providers of public electronic communications networks or services to notify Ofcom of any changes to their network or service which might compromise their ability to comply with their security duties.

It is a great pleasure to serve under your chairmanship, Mr McCabe. Since this is my first substantive contribution to the Committee, I pay tribute to the Front Benchers. It is nice to have a Minister who, I believe, was formerly a tech journalist specialising in telecoms, and who knows the subject well. Of course, the shadow Minister, my hon. Friend the Member for Newcastle upon Tyne Central, was a telecoms engineer and an Ofcom regulator for many years, and I pay tribute to her and her staff. The Committee should know that in addition to running this Bill Committee from the Opposition’s side, she has also been working in the main Chamber this week on the National Security and Infrastructure Bill Committee. Juggling two Bills at once is no mean feat.

I have also greatly enjoyed the interplay between my right hon. Friend the Member for North Durham and the hon. and gallant Member for Bracknell, both of whom have considerable national security experience. I was intrigued by my right hon. Friend’s estimation of Gentleman’s intervention as Schrödinger’s intervention—one that managed to be simultaneously right and wrong. He has set a new standard there.

From listening to the debates on previous clauses, it is clear that a common thread passes through the Bill, which we in the Opposition have been hoping to link up. Partly, it is to do with the question we raised earlier about the assumption that everybody understands exactly what the intention in the Bill is, and that everything will be all right in the long term. My right hon. Friend the Member for North Durham has talked about the importance of making things as clear as possible when it comes to responsibilities, because a future Minister
might not be as adept in this subject as the hon. Member for Boston and Skegness, who currently occupies that position. In a sense, that is the heart of amendment 11.

3.30 pm

Clause 5 asserts a general duty on Ofcom to assure compliance with security details. Much of the detail required under this clause is specified in the next one, clause 6. Obviously, we welcome the clause, which lies at the heart of the purpose of the Bill and underpins the powers and responsibilities given to the regulator. The amendment shares some responsibility with the network providers, which must surely also have a duty to maintain a running assessment of security—something that I am sure that they must try to do already, but which still requires scrutiny. The historical context is clear because, as my hon. Friend the Member for North Durham has hinted at, some of those pressures when in the previous clause he mentioned the TalkTalk hack and some of the commercial and reliability of their asset registers when it comes to equipment and software that drives it. The impression was clear that, at the top level, work had already been undertaken on making an assessment of what assets would need to be replaced before the 2027 deadline, and where the operators were on that. We welcome that.

Some later witnesses, however, while not entirely contradicting that certainty, suggested that the task would not be so easy. We heard about overlapping 2G, 3G, 4G and 5G networks, with different equipment of different ages. My hon. Friend the shadow Minister gave a shocking statistic in relation to the age of the equipment that was responsible for the insecurity that led to the TalkTalk hack. I describe that overlapping network as sounding to non-experts—such as me, I hasten to add—like a bowl of spaghetti.

We therefore accept that any assessment is a complicated task, and we recognise the work that providers have undertaken and will continue to undertake to make good the security of the networks, but several problems remain. First and foremost, any audit or asset register is simply a snapshot at the moment. When national security is at stake, an accurate, up-to-date and rolling picture is at stake, an accurate, up-to-date and rolling picture must be available. It is better to know in advance where problems might occur.

Any business faces commercial pressures, and although I have confidence that no British provider will ever take risks with our nation’s security, the obligations outlined in the amendment will provide clarity and certainty as to which side of the line they should fall in any situation where doubt occurs about whether they ought to discuss potential issues with Ofcom. I think my right hon. Friend the Member for North Durham was hinting at some of those pressures when in the previous clause he mentioned the TalkTalk hack and some of the commercial pressures that companies are under.

Another issue is the relationship between Ofcom and the companies that are being regulated—the network and service providers—because Ofcom it at once a regulator, necessarily with a stick in hand, and a partner agency that is hoping to support the service providers to meet their obligations. We hope that the amendment will provide a little bit of clarity in order to make that partnership more even.

The amendment encourages a rolling conversation with Ofcom, with those matters at the forefront. I assume and hope that that will be happening anyway but, as I have said already, assumption is no basis on which to proceed in legislation. The amendment therefore provides clarity on a sense of obligation. It would also help providers to address problems at the outset and to have the knowledge, as far as possible, but they are likely to be complying on security under the regulations, rather than finding themselves in a situation where they have to comply with the duty under the sections mentioned in the amendment only after the fact and only after work has been done.

Finally, clause 5 puts an obligation on Ofcom, but Ofcom cannot be blamed for not knowing something that it does not know and so failing in its duties under clause 5. The amendment, by sharing the responsibility with the network providers, would assist Ofcom in its duties of overseeing the networks and, I hope, foster more of a partnership when addressing the problems, in the interests of the nation.

We have to avoid providers doing first and telling Ofcom later, because the avoidance of problems is greatly to be preferred to enforcement action further down the line. We have to make things easy for Ofcom. The regulator is growing in scope and complexity, as my hon. Friend the shadow Minister has said, and national security responsibilities are still fairly novel for Ofcom. That load has to be shared, and the amendment provides a focus for providers to assist.

I was a little concerned by suggestions during the evidence sessions that it gets harder to verify security and compliance the further we go down the supply chain. The focus on national security has to be baked in. With a chip here or a piece of software code there which might have been carried forward from a previous or separate piece of equipment, as my right hon. Friend the Member for North Durham has said, it has to be the responsibility of the suppliers and ultimately the network providers not to make any assumptions, but to query every aspect of their asset register and propose changes to it to maintain their duty of security and compliance under sections mentioned in this amendment.

We heard expert testimony during the evidence sessions. Dr Drew said:

“On having providers be more proactively involved, I think it would make complete sense for these actors to be made to inform Ofcom, or whichever regulator is chosen, of significant changes to their supply chains.”—[Official Report, Telecommunications (Security) Public Bill Committee, 19 January 2021; c. 83, Q101.]

Andrea Donà said:

“We need a clear understanding between Ofcom and us as providers before the legislation is enforced, so that we understand exactly the boundaries and the scope, and we all work together, having done the audits, to close any vulnerabilities that we might have. That is a clear aspect of our working together: ensuring that the assets in the telecoms network infrastructure that are in scope are very well defined.”—[Official Report, Telecommunications (Security) Public Bill Committee, 14 January 2021; c. 16, Q14.]
The amendment is simple and straightforward, sharing the obligation on security and allowing for a forward-looking assessment by Ofcom and network providers to give the assurance that we need and to head off problems before they arise. It is about being forward-looking and not always being reactive. I commend it to the Committee.

Chi Onwurah: I rise simply to support the excellent speech made by my hon. Friend the Member for City of Chester. I thank him for his very kind words. In the amendment, he makes an important contribution in ensuring that Ofcom knows what it needs to know and in putting the onus more firmly on the network providers. I simply ask the Minister to respond to the points that my hon. Friend made in his concluding remarks about being forward-looking.

A challenge for us as a nation in securing our networks during such fast-paced technological change is looking backwards to the problems we have had rather than forwards to the evolving and new threats. During the evidence sessions, we were accused of fetishising 5G as if that was the only security challenge, because of the visible problem with Huawei, and that we were not looking more broadly. I admired Ofcom during my time there because it was set up to be a forward-looking regulator. To achieve that aim, when it comes to the sweeping new requirements around security that are placed on it under the Bill, it needs to be able to see what changes are happening and are likely to influence future evolving threats. To do that effectively, amendment 11 requires the network providers to notify Ofcom of planned or actual changes.

It is worth remembering that—I made this point earlier—if BT had been required to notify Ofcom or another body of changes to its network as Huawei moved to a greater and more dominant position in its network, that might have rung alarm bells more generally. We have also already mentioned the shift that we are seeing on the importance of software and software configuration and services in controlling the network. Requiring providers to notify Ofcom of planned or actual changes to the network would make that evolution more easily visible and therefore provide Ofcom with greater visibility of how all our networks are evolving and what new threats may arise as a consequence.

Matt Warman: The amendment would add to the general duty in clause 5 that places on Ofcom the duty to ensure that providers comply with their security duties. The duty as written in the Bill makes clear Ofcom’s increasing role. The duties imposed on public telecoms providers in the Bill are legally binding, so as the Bill is written providers should not be taking decisions that would prevent them from complying with those duties in the future. If they were not to comply, they would be in breach of their legal duties and liable for enforcement action, including the imposition of the significant penalties set out in the Bill.

The underlying purpose of the amendment—that Ofcom should take a proactive role in regulating the regime—is already core to what is in the Bill and the Government absolutely agree with the principle that the hon. Member for City of Chester set out. We need to ensure that Ofcom has the tools to be forward-looking so that, in a world of fast-changing technologies and threats, it can understand where operators are taking their networks and how that will affect their security. That is an absolutely essential part of the Bill.

James Sunderland: Does the Minister agree that the Bill in its current form is prescriptive enough already?

Matt Warman: I think the Bill is perfectly drafted down to every comma and punctuation mark. To be slightly more serious, what we have sought to do in the drafting is to strike the balance between proportionate regulations and the overarching requirements for national security. That is the balance that we have struck and it is exactly for that reason that we already do in the Bill what the hon. Member for City of Chester and the shadow Minister seek with the amendment.

In section 135 of the Communications Act 2003, as amended by clause 12, Ofcom is already allowed to require information from providers about the future development of networks and services that could have an impact on the security of the network or service they are providing. That would enable Ofcom, for instance, to assess the security risks arising from the deployment of a new technology or from the proposed deployment of a new technology. For those reasons, I hope that the hon. Members are reassured not just that the Bill does what they seek, but that previous drafts of the Communications Act already did so.

Chi Onwurah: I thank the Minister for giving way; in doing so, he shortens what I will say later. I think the Minister is saying that Ofcom has the power to require information, which is true, but the amendment is about providers proactively giving that information. Ofcom cannot request information about a change to the networks that it does not know is happening. I am hoping that perhaps what the Minister is implying is that he would expect Ofcom regularly to review what was changing in the networks and therefore make those requests for further information. Could he clarify that point?

Matt Warman: The sort of horizon scanning that the hon. Lady describes is core to all essential regulation, and the relationship that Ofcom has with those whom it regulates promotes the ability to have such conversations. But as I said, the key point is that an operator that proposes knowingly to introduce a risk into its network would clearly not be complying with the statutory provisions of the Bill. That is the essential nub of the issue.

3.45 pm

Christian Matheson: I am most grateful for the debate on the amendment. My hon. Friend the shadow Minister made the key point that Ofcom cannot be blamed for not enforcing something that it does not know anything about. The amendment’s intent was to encourage a sense of shared responsibility in what my right hon. Friend the Member for North Durham reminded us is still a competitive industry in which businesses might want to maintain a level of confidentiality about technological changes or the deals they are doing with suppliers. However, if the Minister is satisfied that that is covered in other parts of the legislation, I beg to leave to withdraw the amendment.

Amendment, by leave, withdrawn.
Clause 5 ordered to stand part of the Bill.
Clause 6

POWERS OF OFCOM TO ASSESS COMPLIANCE WITH SECURITY DUTIES

Christian Matheson: I beg to move amendment 12, in clause 6, page 10, line 12, at end insert—

“(3) In this section “another person” means a UK government agency or a person from a UK government agency.

(4) OFCOM may not incur costs exceeding £50,000 in carrying out, or arranging or another person to carry out, an assessment under this section.”.

This amendment restricts those who Ofcom may arrange to carry out an assessment under this section to a UK government agency or person from such an agency. It also caps the cost of an individual security assessment at £50,000 for Ofcom.

The desire of the Committee is to crack on, so I will not detain us for too long. The clause, which covers more than three pages of the Bill, is extensive in outlining the powers of Ofcom to assess compliance with security duties and will amend sections of the Communications Act 2003 to that end. The Opposition’s probing amendment intends to bring clarity in two areas in particular.

The clause will insert proposed new section 105N into the Communications Act to give authority to Ofcom or “another person” to undertake an assessment of whether a network or service provider is carrying out its duties—an inspection, spot check or audit, whatever you will, Mr McCabe. That is all fine, but the appointment of “another person” is far too vague and needs clarity. Since this is a matter of national security, we believe such an authority can be vested only in an agency or arm of the UK Government. It would be wholly inappropriate to outsource it to a telecoms, IT or other consultancy in part because of the need for full cooperation in part because of the need for full cooperation.

Christian Matheson: I am really grateful for that intervention—not just for the context that my hon. Friend gave, but for prompting me to think that having such a tight-knit sector, and the character of the sector, works both ways. Ofcom might appoint as an inspector to undertake one of the audits somebody who is on very good terms with the business or the provider. They will perhaps take their foot off the pedal and not do quite as thorough an investigation, because they know the business and trust them. As a result, the inspection would not be as thorough.

Mr Jones: My concern is also that the Government do not have a good track record on applying the standards that have been developed over many years to ensure proprieties in public appointments. No doubt somebody who would fit the bill for the role would be Dido Harding, who was responsible for TalkTalk and is now having huge success, as we have been told by the Prime Minister, with Test and Trace. She seems to have a common thread, but success does not seem to be part of that.

Christian Matheson: Who am I to disagree with my right hon. Friend and his years of experience? So far, we have been fairly consensual in this Committee, because we want the Bill to pass. My right hon. Friend is absolutely right: we have seen a certain level of—

Mr Jones: Chumocracy.

Christian Matheson: I was going to say cronyism, but chumocracy is a far nicer way to put it, and we have seen it in the way consultancy contracts have been dished out during the current crisis. My right hon. Friend is absolutely right to say that there can be as little scope as possible for people who are perhaps not quite as qualified as they should be to be given such jobs.

Chi Onwurah: My right hon. Friend the Member for North Durham raised the Test and Trace programme. I do not want you to dwell on that, as it is not within the scope of the Bill, but it is important to understand the extent to which the programme has been used as a vehicle to privatise parts of the NHS by building up private sector skills as opposed to public sector skills. There must be some concern that the huge new powers for and requirements on Ofcom might effectively be used to privatise some of its duties.

Christian Matheson: My hon. Friend says that it is not in the scope of the Bill, but so wide is the definition of “another person” that, quite frankly, anything or anyone could be in the scope of the Bill. Again, the possibility is there, and it would not be down to the Minister. I know him—he is a friend and a man of integrity. As my right hon. Friend the Member for North Durham said, however, the next Minister to come along, in this Government, at least, might not be. Who knows? In four years’ time, we might not have that problem.

This is an important aspect of national security, so I ask the Minister for clarity. It goes to the heart of the question of accountability—where responsibilities for inspections should lie. Similarly, in the second part of the amendment, we are seeking clarity on a limit on the amount that can be spent on inspection. We certainly
do not want Ofcom to be swayed into decisions about whether inspections can go ahead based solely on fears that it might wrack up big costs. Nor can those costs be allowed to spiral if the first part of the amendment is not adopted and private contractors are brought in but abuse the system. I refer the Committee to the comments made by my right hon. Friend the Member for North Durham a while ago—such abuse does happen.

It is often not helpful to put a financial cost limit on the face of the Bill, if only because it can become outdated over time. To be honest with you, Mr McCabe, the truth is that the £50,000 limit specified in the amendment is arbitrary. We plucked it out of thin air to illustrate a point.

Mr Jones: I thought that was the case was when I looked at it. Frankly, for anyone to do that job in telecoms for £50,000 would be very unusual.

Christian Matheson: Fortunately, we will not push the amendment to a vote, so we will not have to put that point to the test. It is an arbitrary figure and I hope the Minister will not fixate on it. It simply illustrates the point that there is a question of open-ended costs. We will not push the amendment to a vote, but we think there is a vagueness and a lack of clarity that needs addressing. I urge the Minister to consider these issues and whether Ofcom would be assisted by the greater clarity that these probing amendments would bring.

Chi Onwurah: Again, I rise mainly to support the excellent contributions made by my hon. Friend the Member for City of Chester in moving this amendment. I will raise a couple of points from my experience in this area.

As I said to my hon. Friend, having worked in telecoms for 20 years, when I joined Ofcom in 2004, I had worked with, or worked with someone who had worked with, just about every operator and network provider in the business. Those personal relationships can be helpful in ensuring quick, effective collaboration, but they can also bring about conflicts of interest. Ofcom, as a public body, has processes and procedures to address those conflicts of interest. However, the Bill makes no provision for that to be applied to whoever is “another person”.

It is also the case that, unfortunately, as a regulator, one can be subject to regulatory capture by those who are regulated. The large operators often have tens or, in some cases, hundreds of lawyers and public affairs spokespeople. However, the smaller operators, unfortunately, cannot afford to dedicate so much time and resource to engaging with the regulator. It is critical that this huge increase in new powers and work for Ofcom is carried out in the right way.

As my hon. Friend said, the £50,000 figure has not been calculated on the basis of the likely costs to Ofcom, because the impact assessment does not indicate what they could be. However, it is merely the cost of five consultants at £1,000 a day for 10 days. We know that hundreds of consultants have been hired as part of the Test and Trace programme at those sorts of prices. That likely cost is within scope of any programme that is to be carried out by bringing in large private sector organisations. I hope the Minister will reassure us that he is taking these considerations into account.

Finally—I think we will discuss this point in more detail—this is a huge additional requirement on Ofcom. In the evidence session, Ofcom said that it thought it would need to hire 50 or 60 people to address the requirements of the Bill. There is always going to be an inclination to reduce internal resources, especially if they are in short supply, such as those to do with network engineering resources and the current skill set. So it is really important that the Bill should have a better definition than it currently does of who may carry out the work.

4 pm

Matt Warman: I enjoyed the semantic gymnastics by the hon. Member for City of Chester as he tried to expand the scope of the Bill, but I shall try to stick to what is in it. There is a lot of consensus across parties, so I shall resist the temptation of saying that £50,000 is a demonstration that Labour is willing to put a price on national security, which this party will never do, but I understand the points that he makes on both fronts.

The clause provides Ofcom with strengthened powers, including powers to give assessment notices to a provider, that are vital to enable it to fulfil its expanded and more active role. Assessment notices are an important new power in the regime that will give Ofcom tools to assess fully a provider’s security and the extent to which it complies with its security duties. It is Ofcom’s intention that when assessing a provider’s compliance, its first port of call would be to use its information-gathering powers under section 135 of the Communications Act 2003. Ofcom would then use its power to give an assessment notice if it wanted to check the veracity of the information or to follow up a security concern. While Ofcom will therefore use its powers in a targeted and proportionate way, it is also the case that a provider with good security practices would expect to be subject to a lighter-touch assessment. Providers’ duty to bear the costs of assessments will therefore have an incentivising effect.

The amendment would insert a new subsection into new section 105N, limiting the costs that Ofcom could incur in carrying out an assessment. Fundamentally, a hard cap of any sort will always be an arbitrary number which will potentially put an additional hurdle in place. It might be necessary for some of those tests to require genuinely extensive assessment—penetration testing, or red teaming, as exercises are sometimes called, where penetration tests mimic the action that an attacker might take to access the network. Those attacking actions may of course be from sophisticated sources, and the costs of mimicking them in an entirely legitimate way could be substantial; but it is right, in the interest of national security, that Ofcom does not reduce the quality of its testing. We would not seek to limit that either, notwithstanding its independence.

I can offer the Committee some reassurance, however, that Ofcom’s assessment costs will not be excessive. It has a general duty to act proportionately and to follow other principles representing regulatory best practice. Finally, a provider’s duty is to pay only such costs as are reasonably incurred by Ofcom in an assessment, so there is a balance there.

As to the proposed new subsection that would limit those able to carry out assessments to Ofcom or a UK Government agency, the assessments, as the hon. Member for City of Chester knows, may be complex and need
specialist skills. Methods such as penetration testing might need specific technical skills and we should not limit Ofcom in that way. However, we should also bear in mind, as the hon. Member for Newcastle upon Tyne Central mentioned, that the independence and expertise of Ofcom is the greatest bulwark against such entirely unfounded but legitimate concerns as those raised by the hon. Member for City of Chester, about who might be appointed by this or any Government to carry out a task in the national interest. None of us would want—and I do not suggest that the hon. Gentleman is doing this—to get into the business of questioning Ofcom’s role in the national interest. None of us would want—and we would perhaps like to admit, but the reason that this is inevitable given that we have private networks—and the skills to ensure compliance. I agree that there are specialised skills. Penetration testing, for example, is a specialised skill, but I would argue that it is a skill that Ofcom should take on as part of this new remit. I say again to the Minister that the skills needed to ensure compliance should be within Ofcom’s remit, or should be better defined.

Matt Warman: Ofcom itself is best placed to exercise discretion as to whether it should carry out those assessments in-house, or whether it should have the flexible capacity to have the capability brought in as necessary. Ultimately, I do not think that anyone would wish to prevent Ofcom from having the ability to do what it thinks necessary by forcing it to use in-house staff only, because we cannot predict the future, as Members on both sides of the Committee have highlighted. Although the cause that the hon. Member for City of Chester is pursuing is a noble one, its unintended consequence would be to constrain Ofcom in both the expertise that it has at its fingertips and the costs that it might incur. We would not want to limit Ofcom’s discretion to make those decisions as an independent organisation.

Chi Onwurah: Actually, the amendment would not limit Ofcom’s discretion to bring in additional resources or skills. It would limit Ofcom’s discretion to Government agencies or organisations within the public sector, which, on matters of national security, we should be able to do.

Matt Warman: If the hon. Lady were right, the only people from whom we would have heard evidence over the last few days would have been public sector employees. She knows just as well as I do that the cyber-security sector is a vast mesh of public and private expertise, which is inevitable given that we have private networks offering communications services. Although I understand her point, and I am all for Ofcom having as much expertise as it needs to do its job properly in-house, I simply do not think that we should constrain what it can access in the way that the amendment would.

On this, I think we probably agree on far more than we would perhaps like to admit, but the reason that this is a probing amendment, as the hon. Member for City of Chester said, is because imposing artificial constraints would not be beneficial to Ofcom’s work. We understand what he said, however, and in broad terms, the Government agree.

Christian Matheson: I am grateful for the debate and for the Minister’s response, but I do not intend to press the amendment any further. I beg to ask leave to withdraw the amendment.

Amendment, by leave, withdrawn.

Chi Onwurah: I beg to move amendment 13, in clause 6, page 10, line 20, at end insert—

“(aa) provide a report on the diversity of their network’s supply chains;”

This amendment gives Ofcom the power to request a report from a network provider on the diversity of their supply chains for the purpose of assessing whether they are complying with the security duties placed on them by earlier sections of the Act.

It is a great pleasure to speak to this amendment, which goes to the absolute heart of one of our key concerns about the Bill—the lack of any reference to the diversification of our supply chain. That is absolutely critical and should be integral to our national security. Our amendment 13 affects clause 6, which we have already discussed. The objective of the amendment is to give Ofcom the power to “request a report from a network provider on the diversity of their supply chains for the purpose of assessing whether they are complying with the security duties placed on them by earlier sections of the Act.”

As we have heard, clause 6 amends the Communications Act 2003 to insert section 105N, which gives Ofcom powers to assess compliance with the security duties set out in earlier sections, and section 105O, which gives Ofcom the power to impose on providers the duty to do any of a significant list of things, from (a) to (k)—

“carry out specified tests or tests of a specified description...make arrangements of a specified description...direct an authorised person to documents on the premises...” or

“assist an authorised person to view information”.

As I have said, this is an integral part of the Bill and requires some considerable debate, so it may detain the Committee for some time, but this debate can be continued at a later time if necessary. There is a long list of requirements that Ofcom might place on network providers, but nowhere is there a requirement for those providers to give a report on the diversity of their supply chains, yet the diversity of a network provider’s supply chains is absolutely integral to the security and resilience of that network provider.

We heard that very clearly during our evidence sessions. In particular, I asked Dr Drew:

“Is it possible for the UK to have secure networks without a diverse supply chain for them?”

Her answer was:

“That is a great question that comes with a very simple answer: no. The worst-case scenario for creating a risk in this sense is when monopoly meets supply chain—in secure supply chain in this case. Arguably, the reason why SolarWinds was so successful is that it provided the same service to so many different organisations and departments in the United States. Therefore, if you access one—SolarWinds—you access almost all. That is the risk.”—[Official Report, Telecommunications (Security) Public Bill Committee, 19 January 2021; c. 87, Q110]
The reason I have highlighted that particular quote—there were a number of quotations supporting the diversification of supply chains—is that it sets out really well what might happen if a network provider has only one possible supplier. If every aspect of its network is supplied by, let us say, Ericsson, and Ericsson then has supply issues itself or is bought or acquired by another operator from a different country that we might not be so close to, or—I do not mean to imply that this is a possibility—should fail in some way, that network provider no longer has any support for their network and no longer has the ability to maintain it securely.

The dependence of our telecoms security on diversifying the supply chain was set out in the 2019 telecoms supply chain report; yet the Bill fails to mention it at all. The objective of the clause is really for Ofcom to assess how successful a network provider is in meeting our nation’s security requirements. My argument is that it is not possible to do that without understanding the diversity of that network provider’s supply chain; yet the clause as it stands makes no reference to that.

4.15 pm

Our clause would enable Ofcom to request a report on the diversity of the network’s supply chain. Alongside network provider diversity more generally, that provides a double layer of network diversification measurements because it enables Ofcom to see what each network provider is doing, as well as generally how our network supply chain is being diversified. During the evidence sessions, we heard a lot about open RAN. Indeed, the telecoms diversification taskforce and the telecoms diversification strategy put a lot of emphasis on open RAN. Open RAN is a development in standards, and so on, which will enable interfaces in networks to be open so that there can be a multiplicity of suppliers at different points in the network.

The evidence that we heard suggested that open RAN was at least six to eight years’ away from maturity and from playing a significant role in our networks. What we seem unable to do in the Bill as it stands is collect the information to enable us to see how different operators are diversifying their supply chain, through the use of open RAN for example. We heard from Vodafone that it is undertaking trials of open RAN, particularly in rural areas, and we would expect, over time, that similar trials may be taken up by other network providers in the UK. How will we see that flowing through network providers’ supply chains if we do not have a requirement or amendment of this type?

In Committee, we heard from Julius Robson, who said:

“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.”—[Official Report, Telecommunications (Security) Public Bill Committee, Thursday 14 January 2021; c. 48, Q60.]

My question for the Minister is: how will we know that we are getting there? How will we know how diverse network providers’ supply chains are? How will we know how resilient they are, and what the impact and security threat of a vendor being acquired by a hostile actor will be, for example?

We also heard from Doug Brace about the problems of regarding open RAN as a silver bullet that we can make a quick transition to.

He said to us:

“I honestly worry that it is too late for open RAN to be incorporated into 5G, at least on a broad scale. For greenfield networks, it is a different story and it might make sense to go with these open and modular systems from the get-go.”—[Official Report, Telecommunications (Security) Public Bill Committee, 19 January 2021; c. 125, Q166.]

My question to the Minister is this: how will we know the extent to which particular vendors are taking up more diverse solutions and more resilient solutions without an amendment to the Bill of this type?

When it comes to understanding the diversity of vendors’ supply chains, we have heard—I have spoken about this a few times, so I apologise for repeating myself—that there is an evolution of the network, from hardware into software services. We also heard during the evidence sessions that more and more of those software services and controls would be on cloud services.

However, in terms of understanding how resilient the new network architectures are, currently the Bill does not make any requirement for reporting on the evolution of network providers’ networks with regard to who their different suppliers are and how many of them there are. So I have real concerns that the Bill is short-changing us on our network security, with the lack of any requirement on network providers to share with Ofcom information about the diversity of their supply chains. We have discussed the importance of supply chains and, to a certain extent, the complexity of supply chains, but we have not seen anything that will enable us to follow how the diversity of particular network operators’ supply chains evolves over time.

I will finish on this point. We have seen significant consolidation in this industry, including in the number of network vendors, over the years. With the removal of Huawei, we are down to two equipment vendors, Ericsson and Nokia. However, we have also had a significant consolidation in terms of the management of networks and particularly in the underlying network architectures, so that many different network operators are effectively operating by perhaps using the same radio access network, or they may have very similar management layers.

The amendment is also designed to enable Ofcom to see how those technological changes are bringing new threats into our telecoms networks by bringing in new areas of potential consolidation. A number of times, I have used the example of Amazon Web Services. The future of networks that was suggested in our evidence sessions would ideally be a radio access network, manufactured by a number of different manufacturers but with quite simple boxes and antennae. And then the control, the services—everything—would be in a layer that would be running over equipment, or servers, from Amazon Web Services or any cloud computing service. It in itself is a different form of potential monopoly consolidation and potentially a different single point of failure. Yet I see no requirement on Ofcom to assess how each vendor, each network provider, is evolving in terms of its network architectures and the threat to diversification of the supply chain that comes as a consequence of that.

When it comes to understanding the supply chains of the network providers as they are today, understanding how successfully they are evolving to become more
diverse, which is a hope that we all have—a shared desire—and understanding how technological changes may be bringing in new potential areas of consolidation, monopoly provision, and single points of failure, this amendment is designed to ensure that we have greater understanding of how things are today and advance warning of the implications of changes, and I do hope that the Minister will be able to accept it.

Matt Warman: I will go very briefly over the diversification strategy, which is essentially a £250-million initial tranche of investment to diversify the UK network, with a focus, to a certain extent, on open RAN, as the hon. Lady said. On the information that she would require, I agree with her so comprehensively that the provision is already in the Bill. Section 135 of the Communications Act 2003, as amended by clause 12—she is right that the provision is not in this clause—provides Ofcom with the power to gather information on diversification where Ofcom considers the information necessary for the purpose of carrying out its functions. Clause 12 specifically provides that such information can include information concerning future developments of a public electronic communications network or public electronic communications service that could impact on security. As I said, I agree with her so comprehensively that we had already foreseen the issue and the provision is already in clause 12. The addition of it to this clause would not change that fact. I hope that that provides—

Chi Onwurah: I thank the Minister for those comments. He says that the provision is already in clause 12. This is obviously down to my lack of studying, and I thought that I had studied every line of the Bill, but where specifically does clause 12 refer to diversification of supply chains?

Matt Warman: The approach that we have adopted across the Bill is that powers such as those in clause 12 are more than wide enough to cover exactly what is needed. What I am essentially saying, I suppose, is that the legal interpretation of clause 12 absolutely does what the hon. Lady seeks, because it is an absolutely essential part of one of the purposes of the Bill. That is why I hope she can take the necessary comfort to withdraw her amendment.

Chi Onwurah: I thank the Minister for that, but I am still puzzled as to where clause 12 says that Ofcom will collect data with regard to diversification of the networks. Ofcom is given the power to collect data with regard to the duties under the Bill, but there is not a duty under the Bill to diversify networks. I am trying to speed-read clauses and subsections; perhaps the Minister can direct me to a part of the clause that specifically requires information concerning. Clause 12 mentions “information concerning future developments of a public electronic communications network or public electronic communications service that could have an impact on the security of the network or service.”

I agree that that could be liable to an interpretation that included diversification of the network, but given that the Bill does not anywhere mention diversification of the supply chain as being part of the security of the network, I am afraid I do not feel reassured.

4.30 pm

Matt Warman: I am very happy to write to the hon. Lady to clarify why it is our belief that the Bill does that. What I would say is that the kind of specificity that she seeks would have the unintended consequence of narrowing what we do, rather than retaining the broad powers that we have in the Bill. As has been the case so often today, we do not disagree on the intent that she is seeking to obtain, and that is why the Bill is drafted as it is. As I say, I am very happy to write to her to try to clarify some of that.

Chi Onwurah: We all agree that the Minister is someone whom we like and who has the best intentions. On that basis, and on the basis that we can table further amendments at this stage or on Report if his letter of reassurance should not be sufficiently reassuring, I beg to ask leave to withdraw the amendment.

Amendment, by leave, withdrawn.

Ordered, That further consideration be now adjourned.

—[Maria Caulfield.]

4.32 pm

Adjourned till Tuesday 26 January at twenty-five minutes past Nine o’clock.
Written evidence reported to the House
TSB 09 Heba Bevan OBE, CEO and Founder, Utterberry Ltd.

TSB 10 Photonics Leadership Group and UK optical communication community
Public Bill Committee

TELECOMMUNICATIONS (SECURITY) BILL

Seventh Sitting
Tuesday 26 January 2021
(Morning)

CONTENTS

Clauses 6 to 16 agreed to.
Clause 17 under consideration when the Committee adjourned till this day at Two o’clock.
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

Saturday 30 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 *(Hyndburn)* (Con)
† Cates, Miriam *(Penistone and Stocksbridge)* (Con)
† Caulfield, Maria *(Lewes)* (Con)
Clark, Feryal *(Enfield North)* (Lab)
Crawley, Angela *(Lanark and Hamilton East)* (SNP)
† Johnston, David *(Wantage)* (Con)
† Jones, Mr Kevan *(North Durham)* (Lab)
† Lamont, John *(Berwickshire, Roxburgh and Selkirk)* (Con)
† Matheson, Christian *(City of Chester)* (Lab)
† Onwurah, Chi *(Newcastle upon Tyne Central)* (Lab)
† Richardson, Angela *(Guildford)* (Con)
† Russell, Dean *(Watford)* (Con)
† Sunderland, James *(Bracknell)* (Con)
Thomson, Richard *(Gordon)* (SNP)
† Warman, Matt *(Parliamentary Under-Secretary of State for Digital, Culture, Media and Sport)*
West, Catherine *(Hornsey and Wood Green)* (Lab)
† Wild, James *(North West Norfolk)* (Con)

Sarah Thatcher, Huw Yardley, *Committee Clerks*

† attended the Committee
Public Bill Committee

Tuesday 26 January 2021

(Morning)

[Mr Philip Hollobone in the Chair]

Telecommunications (Security) Bill

9.25 am

The Chair: Before we begin, I have a few preliminary points. Please switch electronic devices to silent. Tea and coffee are not allowed during sittings. I remind Members about the importance of social distancing. Spaces for Members are clearly marked. I also remind Members that Mr Speaker has stated that masks should be worn in Committee. The Hansard reporters would be grateful if Members could email any electronic copies of their speaking notes to hansardnotes@parliament.uk.

Today we continue line-by-line consideration of the Bill. The selection list for today’s sitting is available in the room. It shows how the selected amendments have been grouped for debate. Amendments grouped together are generally on the same or a similar issue. Please note that decisions on amendments do not take place in the order they are debated, but in the order they appear on the amendment paper. The selection and grouping list shows the order of debates. Decisions on each amendment are taken when we come to the clause to which the amendment relates.

Clause 6

Powers of Ofcom to assess compliance with security duties

Question proposed, That the clause stand part of the Bill.

The Parliamentary Under-Secretary of State for Digital, Culture, Media and Sport (Matt Warman): It is a pleasure to be back under your chairmanship, Mr Hollobone. As we discussed during the debate on amendments to this clause in our previous sitting, clause 6 inserts proposed new sections 105N to R, providing Ofcom with strengthened powers to assess whether providers of public electronic communications networks and services are complying with their security duty. These powers are vital to enable Ofcom to fulfil its expanded and more active role, giving it the tools to monitor and assess providers’ compliance with the new telecoms security framework and providing the basis for commencing any enforcement action.

Proposed new section 105O provides the power to give assessment notices to a provider. Assessment notices may impose a duty on a provider to do a number of different things, which I will briefly summarise. First, providers can be required to carry out, or arrange for another person to carry out, technical testing in relation to their network or service. Secondly, they can be required to make staff available to be interviewed, enabling Ofcom to gain insights into how a provider’s security practices and policies are implemented.

Thirdly, providers can be required to allow an Ofcom employee or an assessor authorised by Ofcom to enter their premises to view documents or equipment. I recognise that that is a significant power, but it is necessary. It is subject to certain restrictions to protect legally privileged information and to limit entry to non-domestic premises only. To provide clarity for telecoms providers, Ofcom will also publish guidance setting out how and when it will use the power. Importantly, providers have a right of appeal.

The powers of assessment set out in the clause are key to enabling Ofcom to carry out the effective and extensive monitoring and assessment of providers’ security practices that is necessary.

Chi Onwurah (Newcastle upon Tyne Central) (Lab): It is a pleasure to serve under your chairmanship, Mr Hollobone, and to come back to this important Bill. I thank the Minister for writing to me and reassuring me on certain matters relevant to the clause. We accept the need for Ofcom to have powers to require information from vendors, but we would like a specific requirement whereby Ofcom can ask vendors for information on the diversity of their supply chains. I will leave further discussion on that for our new clauses. I will support this clause.

Question put and agreed to.

Clause 6 accordingly ordered to stand part of the Bill.

Clause 7

Powers of Ofcom to enforce compliance with security duties

Question proposed, That the clause stand part of the Bill.

The Chair: With this it will be convenient to discuss the following:

Clause 8 stand part.
Clause 9 stand part.
Clause 10 stand part.

Matt Warman: I will seek to move relatively rapidly through these four clauses.

Clause 7 provides Ofcom with enforcement powers in relation to providers’ security duties. The Bill gives Ofcom new powers to impose tough financial penalties on providers who breach their security duties. The penalties range to a maximum fine of 10% of a provider’s annual turnover, which is in line with the maximum fines available for breaching other regulatory requirements. For continuing contraventions, Ofcom can levy a daily penalty of up to £100,000. Penalties that are generally lower than that but still significant will also apply for contravening information requirements, which are subject to a maximum penalty of £10 million or, for a continuing contravention, a penalty of up to £50,000 per day. These penalties ensure that there will be a real financial deterrent to poor security practices. I should also say that, in the most serious cases, or in cases where a provider repeatedly contravenes its security duties, Ofcom would be able to use existing powers to suspend or restrict the provider’s entitlements to provide a network or service. Clearly, that is a step that we hope the regulator will never need to take.
The clause also gives Ofcom an important new power to take action where security is being compromised or is at imminent risk of being compromised. Proposed new sections 105U and 105V of the Communications Act 2003 would enable Ofcom to direct a provider to take interim steps to secure its network or service while Ofcom investigates or pursues further action. This power recognises that contravention of a security duty could result in a security compromise that causes real damage to users of that network or service. Where Ofcom uses that power, it will be required to commence and complete the enforcement process as soon as is reasonably practicable. The clause gives Ofcom the tools it needs to effectively enforce compliance with the new security framework.

Clause 8 sets out the position for bringing civil claims against providers who breach their security duties, which is a matter we touched on in earlier debates. It enables providers to be held accountable not just by Ofcom but by service users, such as members of the public, in cases where loss or damage is sustained by those users as the result of a breach of a duty. Providers owe a duty to any person who may be affected by a contravention of their security duties to take security measures, to comply with specific security duties in any regulations and to inform users of security compromises.

This clause allows any affected person to take legal action should providers breach those security duties. However, any affected person can bring legal proceedings against a provider only with the consent of Ofcom, which may be subject to conditions relating to the conduct of the legal action. This reflects the existing position in the Communications Act 2003 and ensures that providers face legal action only in appropriate circumstances. The clause also makes providers responsible to their users, providing another source of accountability. It allows users to bring legal claims for any losses they have suffered, which is only fair and reasonable.

Clause 9 addresses the interaction between provisions in the Bill and other legislation, specifically national security, law enforcement and prisons legislation. The security duties created by the Bill do not conflict with duties imposed on communications providers by other legislation via these clauses. Equally, we do not want the Bill to affect adversely the important work carried out by our law enforcement agencies, criminal justice authorities and intelligence agencies. The clause gives that clarity to providers about their responsibilities.

Finally, clause 10 requires that Ofcom publish a statement of policy about how it will fulfil its general duty and use specific powers to ensure that providers comply with their security duties. This will provide welcome clarity to industry about the expected use of important new powers. I beg to move that these clauses stand part of the Bill.

Chi Onwurah: I will not detain the Committee long, as we are cracking on through the clauses. I will only emphasise that these clauses give Ofcom broad powers — very broad powers — and measures of enforcement, as well as placing duties on the network operators to all users of their network services. We support these broad powers, but it is incumbent on the Minister and indeed on the Committee to consider whether those powers will receive sufficient scrutiny, and sufficient oversight and input from our security services. We anticipate debating those particular questions in more detail later today. In the meantime, we will not stand in the way of these clauses standing part of the Bill.

Question put and agreed to.

Clause 7 accordingly ordered to stand part of the Bill.

Clauses 8 to 10 ordered to stand part of the Bill.

Clause 11
REPORTING ON MATTERS RELATED TO SECURITY

Chi Onwurah: I beg to move amendment 14, in clause 11, page 18, line 26, at end insert—

“(aa) an assessment of the impact on security of changes to the diversity of the supply chain for network equipment;”

This amendment requires that network supply chain diversification is included in Ofcom reports on security.

The Chair: With this it will be convenient to discuss the following:

Clause 8 stand part.

Clause 12 stand part.

Clause 13 stand part.

Chi Onwurah: We start this debate where we ended our sitting on Thursday, on the diversity of the supply chain. But this is not groundhog day; this is a very different aspect of the diversity of the supply chain. I hope the Minister has noticed that there are three themes to our amendment: national security, diversity of the supply chain and appropriate scrutiny. Those are our key concerns about the Bill as it stands.

We wish to see the Bill debated as speedily as possible. For the record, I reiterate my concern that, in the midst of a pandemic lockdown, where the advice is to stay at home, the Leader of the House requires that Members of Parliament should congregate in one room for several hours. With that in mind, we are cracking on as quickly as possible, and we have made significant progress only this morning. However, we feel strongly that, given the speed at which we are providing the appropriate scrutiny, more time should be devoted to debating the Bill on the Floor of the House. We are cracking on in order to protect, as far as we can, the public health of Members of Parliament, staff, House officials and Clerks, who are doing an amazing job in the midst of a pandemic.

Clause 11 makes provision for reporting by Ofcom on security matters. That includes a duty to provide an annual security report to the Secretary of State. Amendment 14, in my name and those of my right hon. and hon. Friends, requires that network supply chain diversification is included in Ofcom’s report on security. As I said, we anticipate having a broader debate this afternoon on the importance of the diversification of the supply chain to security, as part of the debates on our new clauses, so I will only summarise our key points and concerns now.

This amendment follows amendment 13, which sought to give Ofcom the power to request reports from operators on their supply and the progress of their supply chain diversification. We support steps to remove high-risk vendors from the UK networks, but they must go hand
in hand with credible measures to diversify the supply chain. I am afraid it remains the fact that we have no reference to the diversification of the supply chain in the Bill, despite the fact that, as I will briefly outline, both the Secretary of State and experts during our evidence sessions emphasised that we could not have network security without effective diversification.

We cannot have a robust and secure network with only two service providers. Supply chain diversification is absolutely vital to protecting our national security. If a vulnerability exists in one vendor or service provider, that intrusion may be limited to that one vendor or service provider alone. A diversity of suppliers in the supply chain limits the exposure of vital information. This amendment ensures that network supply chain diversification is addressed in Ofcom’s report on security. My key question to the Minister is, how can Ofcom report on security if it is not reporting on supply chain diversification?

The Minister may well say that Ofcom has the power to report on supply chain diversification and to request information on supply chain diversification. As I have said on a number of occasions, the powers in the Bill are broad. That is why effective scrutiny requires some specification of what will be reported upon.

The security report to the Secretary of State should be made as “soon as practicable after the end of each reporting period” and “must contain... information and advice... to assist the Secretary of State in the formulation of policy”. It must also include the extent to which providers have complied with security duties. That is as an example of some of what may be included in the security report. Given that the Secretary of State has said on a number of occasions that supply chain diversification goes hand in hand with the security of the network, it is essential that supply chain diversification is specifically mentioned in the Bill, so that we can have accurate and detailed reports from Ofcom on key aspects of network security.

The amendment will help provide the Secretary of State with the information to update Parliament on the progress of the Government’s diversification strategy, depending on Ofcom’s findings. The Secretary of State has promised to give Parliament such updates, so this is an enabling amendment to ensure that the Secretary of State has the information he needs to provide the reporting that he has committed to.

In support of the amendment, I would like to cite one of the witnesses in our evidence sessions. Dr Alexi Drew, from Kings College, London, was asked whether it was possible to have a secure network without a diverse supply chain, and answered:

“That is a great question that comes with a very simple answer: no. The worst-case scenario for creating a risk in this sense is when monopoly meets supply chain—insecure supply chain in this case. Arguably, the reason why SolarWinds was so successful is that it provided the same service to so many different organisations in the United States. Therefore, if you access one—SolarWinds—you access almost all. That is the risk.”—[Official Report, Telecommunications (Security) Public Bill Committee, 19 January 2021: c. 87, Q110]

That is a risk that, I am sorry to say, the Bill currently does not sufficiently address. I hope that, by accepting this amendment, the Minister will recognise that we are, as always, seeking to improve the Bill and to ensure that it provides a credible and effective means to secure our networks.

With regard to clauses 11, 12 and 13 stand part, we recognise the importance of providing Ofcom with the appropriate powers to request information, but also to share information related to security. In that respect, these provisions are ones that we can support.

9.45 am

Matt Warman: I welcome the spirit of the amendment. I think that the hon. Lady and I share the same ambition. I know that she wants to have the proper debate later, so we look forward to that.

Clause 11 inserts into the Communications Act 2003 proposed new section 105Z, which deals with Ofcom’s reports on security. It requires Ofcom to produce such reports within two years of the Bill receiving Royal Assent and every 12 months thereafter. As the hon. Lady said, amendment 14 is similar to the amendment to clause 6 that we discussed previously. Ultimately, when considering Ofcom’s role and specifically its reporting function, we should note that proposed new section 105Z(2) requires Ofcom security reports to include such information and advice as Ofcom considers may best assist the Secretary of State in the formulation of policy on telecoms security. That could go beyond the list in proposed new subsection (4) to include other relevant information, such as that related to diversification. The Secretary of State can also direct Ofcom to include information that goes beyond that list.

As the Committee and, indeed, Ofcom will be well aware, the Government have recently published a targeted diversification strategy, which will deliver lasting and meaningful change in the 5G supply chain and pave the way for a vibrant, innovative and dynamic supply market. We heard widespread support for the strategy from witnesses during the oral evidence sessions. The strategy demonstrates our commitment to building a healthy supply market and is backed by a £250 million initial investment.

We have publicly announced that the Government will be funding the creation of a UK telecoms lab to research and test new ways of increasing security and interoperability, and we are already partnering with Ofcom and Digital Catapult to fund the industry-facing test facility SONIC—the SmartRAN Open Network Interoperability Centre. Both of those will play a key part in our investment in diversification and demonstrate Ofcom’s existing part in it.

As already mentioned, amendment 14 would require Ofcom to include in its security reports “an assessment of the impact on security of” any “changes to the diversity of the supply chain for network equipment”. As that requirement is already essentially covered by Ofcom’s existing powers, the amendment is not necessary. The inclusion of any such information is already within Ofcom’s discretion, but I am sure that we will discuss it more later on, as the hon. Lady said.

Clause 12 expands Ofcom’s information-gathering powers for the purposes of its security functions and enhances its ability to share the information with the Government. It enables Ofcom to require a provider to produce, generate, collect or retain security information,
and then to analyse that information. Any information sought using this power must always be proportionate to how Ofcom will use it.

Clause 13 makes provision in connection with the standard of review applied by the Competition Appeal Tribunal in appeals against certain of Ofcom’s security-related decisions. Ofcom’s regulatory decisions are subject to a right of appeal to the tribunal, and that will also be the case for most of Ofcom’s decisions relating to the exercise of its regulatory powers conferred by the Bill. This clause makes provision to ensure that the tribunal is not required to modify its approach in appeals against relevant security decisions, and should instead apply ordinary judicial review principles.

I hope that I have sufficiently explained to the Committee why amendment 14 is unnecessary and why clauses 11 to 13 as drafted should stand part of the Bill.

Chi Onwurah: I thank the Minister for his comments. Although we agree on many things in many areas, I think that in this case he is trying to have his cake and eat it, inasmuch as he is saying that amendment 14 is not necessary because Ofcom already has the powers, but he is reluctant or is refusing to specify that those powers will be used for the objective of reporting on the progress of diversification of the supply chain. It was good to hear the Minister reiterate the importance of diversification of the supply chain, but I remain confused about whether he agrees with the evidence and, indeed, with his own Secretary of State that diversification of the supply chain is a prerequisite of the security of our networks and, indeed, our national security—that is what we are discussing with regard to our telecoms networks. If diversification is a prerequisite, why is the Minister so reluctant to refer to it? If he is so confident in the plan to diversify our supply chains, why is he so reluctant to insert any requirements to report on the progress of that diversification?

I listened intently; the Minister said that Ofcom has the powers to report on whatever it considers to be relevant to security. During the evidence session, we heard from Ofcom itself, very clearly and repeatedly, that it is not for Ofcom to make decisions on national security. It will not make national security decisions. That is not within its remit and responsibilities; the witnesses from Ofcom stated that repeatedly and clearly. I would be happy to read from Hansard if that point is in question. Given that Ofcom will not make security decisions and that the diversification of the supply chain is essential for security, I am at a loss to understand why the Minister will not accept a reference to reporting on the progress of diversification. Although, unfortunately, the pandemic means that we are not at full strength on the Opposition side of the Committee, I wish to test the will of the Committee on the amendment.

Question put, That the amendment be made.

The Committee divided: Ayes 3, Noes 10.

Division No. 1]

AYES

Jones, rh Mr Kevan
Matheson, Christian
Onwurah, Chi

NOES

Britcliffe, Sara
Cates, Miriam
Gaulfield, Maria
Johnston, David
Lamont, John
Richardson, Angela
Russell, Dean
Sunderland, James
Warman, Matt
Wild, James

Question accordingly negatived.

Clause 11 ordered to stand part of the Bill.

Clauses 12 and 13 ordered to stand part of the Bill.

Clause 14

Reviews of sections 1 to 13

Chi Onwurah: I beg to move amendment 15, in clause 14, page 21, line 28, leave out from beginning to end of line 30 and insert—

“(3) The reports must be published not more than 12 months apart for the first 5 years, then not more than 5 years apart.

(4) The first report must be published within the period of 12 months beginning with the day on which this Act is passed.”.

This amendment requires the Secretary of State to report on the impact and effectiveness of clauses 1 to 13 every year for the first five years after the Act is passed, and then every five years following.

The amendment reflects another of our key concerns about the Bill, which is the level and extent of appropriate scrutiny for such broad and sweeping powers. It seeks to ensure appropriate scrutiny. Clause 14 requires the Secretary of State to review the impact and effectiveness of clauses 1 to 13 at least every five years. Our amendment would require the report to be published every year for the first five years after the legislation is passed, and then up to every five years after that.

As we have said, the Bill gives the Secretary of State and Ofcom sweeping powers. We want to ensure both that they are proportionate and that there is accountability. As we have previously emphasised, we are sure that the Minister and the Secretary of State are inclined to exercise the powers in a proportionate and accountable way, but they will not be in their posts forever, and perhaps not for the entire first five years of the legislation’s operation, so it is important that the Bill requires that Parliament be able to scrutinise its effectiveness, as that is so important to our national security. In that sense, this amendment follows amendments 5, 9 and 10 with respect to the requirement for appropriate oversight and accountability.

I emphasise—I am sure that you will understand, Mr Hollobone—that in some ways we are here because of a lack of effective parliamentary scrutiny of the presence and growth of high-risk vendors in our networks. It was only when Parliament became aware of and was able to give its full-throated input on concerns about the dominance of high-risk vendors in our telecommunications market that the Government took action. We do not want to be in the position of finding again that there has been a dramatic change in the security of our networks without appropriate scrutiny.

Clause 14 states that the Secretary of State must “carry out reviews of...impact and effectiveness” and that the report must be laid before Parliament for parliamentary scrutiny. However, we are to wait up to five years before it will be made possible to give
parliamentary scrutiny to a Bill that is so important to national security, as both the Minister and the Secretary of State, and indeed the security services, have emphasised. We are not to review its effectiveness for five years.

Sara Britcliffe (Hyndburn) (Con): Does not the clause state that the period is up to five years? The review could be done during that period; it would not have to be at the five-year mark every time.

Chi Onwurah: The hon. Lady is absolutely right. The clause enables the Minister or Secretary of State to choose to lay a report more frequently. Again, I do not want to impute anything against the Minister or the Secretary of State, but given the importance of the subject and parliamentary review, why not ensure that it is more frequent?

I am sure that the hon. Lady will agree that Parliament has many things to consider, and so does the Secretary of State. There is competition for parliamentary time, particularly in a pandemic and in view of the challenges that we shall face in the next few years. How can I put this? We have concerns that the priority may slip in the face of, for example, economic challenges, investment challenges and recovery challenges. We want to be sure what is happening. We are the party of national security and we want to ensure that, in this context, national security is brought to Parliament to be debated, discussed and reviewed at least every year.

10 am

I have outlined the importance of parliamentary scrutiny as part of our wish to do that, but we should also consider what might happen in the next five years, before the first review mandated by the Bill. We have seen vast technical, technological and geopolitical shifts in the last five years. We face security challenges from China and Russia, and terrorist threats in a complex security environment. I am sure the Minister does not anticipate that those hostile actors against whom the measures in the Bill securing our networks are primarily directed will not respond; they will do so. We cannot imagine that we will take these measures to secure our networks against those who seek to attack or undermine our telecommunications capability in their own interests and they will not respond in some way. As it stands, the first review of that response could be five years after it has happened.

In addition, specifically with regard to the hope on which the Government might be placing an unjustified amount of assurance in diversifying our supply chains using open radio access network technology, we heard from witnesses that the next five years are key. The next five years will be the period in which we will see—or not see—the maturity of open RAN technology. There was a discussion about whether open RAN will be a viable and credible alternative in the next year, two years, three years or four years. While there are technological changes and the maturity of open RAN is in question, spending the next five years without having a review of its effectiveness seems to me to lack appropriate oversight.

There is support for increased review measures. We heard from Derek McManus, the chief operating officer of O2, about the evolution of open RAN. He said:

“There are trials in the UK...it will be at least a couple of years before you have a viable technical and commercial product, focused initially on rural.”—[Official Report, Telecommunications (Security) Public Bill Committee, 14 January 2021; c. 11, Q5.]

As things stand, that period could pass without any review or report. We also heard from Emily Taylor, the chief executive of Oxford Information Labs, who said:

Imagine if we were sitting here, in five or 10 years’ time, lamenting the fact that the equipment market is now dominated by Microsoft and Google. I am just making that up as a hypothetical example—I have no knowledge to back that up—but those are the companies that have the sufficient scale and skills, and as Chi Onwurah said in her question we are moving to a more hybrid network, where skills in cloud computing and software are going to define the success of the player.”—[Official Report, Telecommunications (Security) Public Bill Committee, 19 January 2021; c. 77, Q92.]

I am quoting someone quoting me, who says that “skills in cloud computing and software are going to define...success” but we are going to wait five years to review, when, as I am sure the Minister is well aware, given his background, five years could be five technological generations in this area.

The next five years will be key to the maturation of the technologies about which the Minister has so many hopes to help with the diversification of our supply chain and in terms of the global security and geopolitical environment and landscape, yet we have no requirement for reporting or accountability during that time. That is what the amendment is designed to change.

Matt Warman: I listen with interest to the points that the hon. Lady makes, and to the assertion that she is a member of the party of national security. I welcome her to this side of the House, if that is the case. [Interruption.] Thank you, but no.

As the hon. Lady says, clause 14 is a review clause requiring the impact and effectiveness of clauses 1 to 13 to be reviewed at least every five years by the Secretary of State. The review report must be published and laid before Parliament, but it is by no means the only source of parliamentary scrutiny, as she knows. Her amendment would increase the frequency of these reports to every year for the first five years after the Bill is passed and then every five years thereafter.

Increasing the frequency of the reports would bring its own challenges for a number of reasons. First, the framework is considerably different from the previous security regime in the Communications Act 2003. It seems to me that we will not be able fully to assess the impact and effectiveness of the new security regime instituted by clauses 1 to 13 until all parts of the framework, including secondary legislation, codes of practice and other things, have been in place for a reasonable period of time. The code of practice that will provide guidance on the detailed security measures that telecoms could take is intended to set clear implementation timelines. Some measures may require significant operational change, as we heard in the evidence sessions for telecoms providers, and we are aware that that may be costly. For that reason, we cannot reasonably expect all changes to be implemented instantly or, indeed, all necessarily at the same time.

There is a further practical difficulty with the amendment. If the first report is to be produced 12 months after Royal Assent, it will require the review to be undertaken...
well in advance of that deadline. That means that the report will represent an incomplete picture of the Bill’s impact, even at its very first production. Some measures will not even have been implemented by telecoms providers.

My hon. Friend the Member for Hyndburn was exactly right that the current requirement for publishing reports is at least—rather than at most—every five years. We have been deliberate in our choice of this timeframe because five years is the reasonable point by which we expect the majority of telecoms providers to have implemented most, if not all, changes. It is therefore considered appropriate to require a report on the impact and effectiveness of the framework by that time. I recognise that five years is a long time. That does not mean that the framework will be free from scrutiny in the intervening period. As clause 11(3) sets out, the Bill amends section 134B of the Communications Act so that Ofcom’s regular infrastructure reports will include information on public telecoms providers’ compliance with the new security framework. Ofcom publishes the reports annually, rendering the amendment unnecessary.

**Chi Onwurah:** On a point of clarification, I have the impression that the Minister anticipates that the first report under the Bill would only happen once all the requirements had been implemented. I think that that implies that it would only happen once a high-risk vendor, specifically Huawei, had been removed from the network.

**Matt Warman:** No is the short answer, because while this is a progress report, five years from 2021 is 2026—the deadline is 2027, even at the most extreme end, which is not where we anticipate it will end up—and it would be before the point that she identifies.

The infrastructure reports from Ofcom will help to provide Parliament and the public with a view on how telecoms providers are progressing with compliance with the new framework. As I alluded to earlier, they are not the only means of parliamentary scrutiny. We have the Intelligence and Security Committee and we have Select Committees. I suspect that there might be one or two debates on this matter over the next five years as well. To pretend that this is the only method of parliamentary scrutiny is not accurate.

**Chi Onwurah:** If the Minister will give way briefly, he may find it saves time. To clarify: for the first report we have implemented most, if not all, changes. It is therefore reasonable to require that the framework will be free from scrutiny in the intervening period. As he has indicated that the reports would do well to include reference to everything that appertains to security, including the diversification of supply chain, I beg to ask leave to withdraw the amendment.

**Clause 15**

**Designated vendor directions**

The Chair: With this it will be convenient to discuss the following:

Amendment 17, in clause 16, page 27, line 8, at end insert—

“(3A) When considering whether a designated vendor direction is necessary in the interests of national security, the Secretary of State must take account of the advice provided by the intelligence services.”

This amendment would require the Secretary of State to give due priority to advice provided by the Intelligence Services (including the National Cyber Security Centre as part of GCHQ) when considering whether to issue a designated vendor direction.

The Chair: With this it will be convenient to discuss the following:

Amendment 18, in clause 16, page 28, line 3, at end insert—

“(m) the person’s control of data flows”

This amendment requires the Secretary of State to consider a person’s potential control of data flows when issuing a designation notice.

Clause 16 stand part.

Amendment 19, in clause 17, page 29, line 19, at end insert

“, together with an assessment of the impact the designation notice will have on supply chain diversity;”.

This amendment requires the Secretary of State to lay before Parliament a report on the impact a designation notice will have on telecoms market supply chain diversity, enabling parliamentary scrutiny.
Mr Jones: I thought I would bring some light relief to the Committee’s proceedings. Amendments 16 and 17 are both probing amendments. I might sound like a broken record, but they are really just to ensure that we get a situation where the necessary advice is taken. Amendment 16 states:

“When considering whether a designated vendor direction is necessary in the interests of national security, the Secretary of State must take account of the advice provided by the intelligence services.”

I accept that the entire purpose of the Bill is to have national security at its heart, but I still have a nagging doubt about whether Ofcom will be able to put national security at the heart of its considerations.

Amendment 17 states:

“When considering whether a designation notice is necessary in the interests of national security, the Secretary of State must take account of the advice provided by the intelligence services.”

This is an attempt to future-proof the Bill. As I mentioned the other day, when we pass legislation in this place it is important that it outlives present Ministers, and us all. Unfortunately, there is form on this—look at the Intelligence and Security Committee’s 2013 report on critical national infrastructure. I accept it was then the Cabinet Office, not Ofcom, that dealt with this, but when BT negotiated its contract with Huawei, the Cabinet Office was told about it but did not feel it necessary to tell Ministers for another three years, until 2006. I am concerned that national security will not be at the forefront when people look at such matters. The amendment is really just to ensure that that takes place, and codifies it into law.

I do not wish to criticise civil servants in any way, but having been a Minister myself, I know they sometimes have a tendency not to put forward things that might have a political dimension that they do not recognise. That is why it is important for national security that the Secretary of State has first-hand knowledge and information directly from the security services. We have very effective security services in this country—I pay tribute to them—but we also have the Cabinet Office. I know the Minister might think I am a bit obsessive, but I am sure he has come up against the buffer of the Cabinet Office, which seems to want to intervene in everything and anything that does not really concern it.

10.15 am

The Secretary of State should have access directly to the security information and should not have to go through the filter of the Cabinet Office or Ofcom. I accept the assurances that the Minister gave about Ofcom’s ability to give advice and work closely with the security services, and these are probing amendments. I am interested in what he says about how we can ensure that when the Secretary of State takes a decision, national security is at its heart, and that he or she got it straight from the horse’s mouth—in other words, from the security services—rather than its being filtered through the membrane that sometimes exists in Whitehall.

Matt Warman: I thank the right hon. Gentleman for his contribution to the debate. He has talked so much about my impermanence that I felt lucky to come back today, never mind any time in the future. He makes a reasonable point, with which I broadly sympathise. As this is a broad grouping that covers clauses 15 and 16 and the amendments to clauses 15, 16 and 17, I will discuss the policy intention behind the clauses in sequence, and address the amendments.

As the right hon. Gentleman said, it is obviously an opportune moment to pay tribute to the heroic work of our national security services. The Bill emphasises the importance of their advice, and it empowers the Government to manage the presence of high-risk vendors in our networks. The report to which he refers is important, but it is also important to say that it was published, as he said, in 2013. It related almost entirely to events that took place under Labour, and it predates the existence of the National Cyber Security Centre, so we are dealing to some extent with a different world. I will go into a bit of detail on that.

As the right hon. Gentleman knows, the Government announced in January last year that new restrictions should be placed on the use of high-risk vendors in the UK’s 5G and full-fibre networks. In July 2020, the Government worked with the NCSC to update the guidance following action taken by the US Government in relation to Huawei. Clauses 15 to 17 provide the principal powers that the Government need to manage the risks posed by high-risk vendors. Without such powers, the guidance issued to industry will remain unenforceable and therefore present a risk to national security.

Mr Jones: I accept what the Minister says about the report, but its key point was that civil servants basically decided not to tell Ministers. On his explanation and the way forward, or what has changed since, how can we avoid a situation whereby Cabinet Office civil servants take the decision not to tell Ministers? How can we ensure that that will not happen again?

Matt Warman: In short, the right hon. Gentleman is challenging the fundamental effectiveness of Government and the judgments that were made by officials at the time. I simply say that it is the duty of Government to ensure that such errors are not made in future. That cannot be done solely by legislative means; it must be done by custom and practice. The right hon. Gentleman understands, through his work on the ISC, that the role of those close working relationships is in some ways far more important in the day-to-day security issues that we are dealing with. Perhaps we can return to that point later.

The Bill will allow the Secretary of State to issue designated vendor directions, imposing controls on the use of goods, services or facilities that are supplied, provided or made available by designated vendors. The Secretary of State may issue such directions only where it is necessary to do so in the interests of national security and proportionate to the aims sought to be achieved.

Amendment 16, which would amend clause 15, seeks to place a statutory requirement on the Secretary of State to take into account advice from our intelligence services when considering whether to issue a designated vendor direction. Amendment 17, which would amend clause 16, seeks to place a similar requirement when considering a designation notice.

I should reassure hon. Members that the Secretary of State, as the right hon. Member for North Durham knows, has every intention of seeking the advice of our
security and intelligence services, as would any Secretary of State, in particular the NCSC, when considering whether to issue a designated vendor direction or designation notice.

It is also worth saying, from a scrutiny point of view, that the Department for Digital, Culture, Media and Sport maintains an excellent relationship with the NCSC. We are scrutinised by the Select Committee on Digital, Culture, Media and Sport and I have appeared before the Intelligence and Security Committee, as the right hon. Gentleman knows. There are many examples in the Bill where the NCSC’s expert advice has been taken into account.

The UK telecoms supply chain review, on which the Bill is based, was the product of the close working relationship between the Department for Digital, Culture, Media and Sport and the NCSC. In a sense, that close working relationship demonstrates that matters have moved on substantively since 2013.

I draw hon. Members’ attention to the illustrative notices that we published in November last year. The NCSC was closely involved in the drafting of those illustrative notices. It will also be involved in the drafting of direction and designation notices once the Bill has been enacted. Given the demonstrable success of our collaboration with the NCSC thus far, I hope that the right hon. Gentleman will be satisfied with that explanation, although I appreciate that he introduced a probing amendment.

Clause 15 would create the new power for the Secretary of State to issue designated vendor directions to public communications providers, in the interests of national security. Although clauses 15 and 16 are distinct, they are complementary. Directions cannot be issued without identification of a designated vendor and designations have no effect unless directions are given to public communications providers. Clause 15 inserts new sections 105Z1 to 105Z7 into the Communications Act 2003 and amends section 151 for that purpose.

The clause will enable the Government’s announcements in 2020 on the use of high-risk vendors to be given legal effect. Those announcements include advice that require a public telecoms provider to exclude Huawei from their 5G networks by 2027, and stop installing new Huawei goods, services or facilities in 5G networks from September 2021. It will also enable the Government to address risks that might be posed by future high-risk vendors, helping to ensure our telecoms networks are safe and secure.

Proposed new section 105Z1 sets out the direction power. It would allow the Secretary of State to give a designated vendor direction to a provider, imposing requirements on their use of goods, services or facilities supplied by a specified designated vendor. Proposed new section 105Z2 provides further details on the types of requirements that may be imposed in a designated vendor direction. Proposed new section 105Z3 sets out the consultation requirements and expectations for public communications providers. Proposed new section 105Z4 sets out a requirement for the Secretary of State to provide a copy of a direction to the designated vendor or vendors, specified in a direction and, hence, affected by it. Proposed new sections 105Z5 and 105Z6 set out when and how the Secretary of State may vary or revoke a direction. Lastly, 105Z7 enables the Secretary of State to require a public communications provider to provide a plan setting out the steps that it intends to take to comply with any requirements set out in a direction and the timings of those steps.

Although the Government have made specific announcements on Huawei, the high-risk vendor policy has not been designed around one company, country or threat. The designated vendor direction power, as set out in these provisions, is intended to be an enduring and flexible power, enabling the Government to manage the risks posed to telecoms networks both now and in the future.

Clause 16 includes a non-exhaustive list of matters to which the Secretary of State may have regard when considering whether to issue a designation notice. Amendment 18 seeks to amend that clause by adding a person’s control of data flows to the list of matters to which the Secretary of State may have regard. However, nothing in the clause prevents the Secretary of State from considering control of data flows before issuing a designation notice already, if the matter were deemed relevant to the assessment of national security. It is already covered and so is not required as a stand-alone measure.

The clause creates a power for the Secretary of State to issue a designation notice, which designates a vendor for the purposes of issuing a designated vendor direction. Proposed new section 105Z8 is the principal measure of the clause, and sets out the power for the Secretary of State to designate specific vendors where necessary in the interests of national security. A designation notice must specify the reasons for designation unless the Secretary of State considers that doing so would be contrary to the interests of national security. The proposed new section also lists the primary factors that may be taken into account by the Secretary of State when considering whether to designate a vendor on national security grounds.

Finally in this group, amendment 19 would require the Secretary of State, when laying a designation notice before Parliament, also to lay before Parliament a report detailing the impact that the designation notice might have on the diversity of the UK’s telecoms supply chain. The effect of the amendment would be to require the Secretary of State to lay a report purely on the impact of the designation notice, but a designation notice simply notifies vendors that the Government consider them a risk to national security.

Only when the designation notice is issued alongside a designated vendor direction are controls placed on the use of a designated vendor’s goods, services and facilities by public communication providers, so it is those controls that might have an impact on the diversity of the supply chain. I can reassure the Committee that the Government will consider the diversity of the supply chain before issuing designation notices and designated vendor directions. A lack of diversity is in itself a risk to the security of a network. I hope that answers the question that the hon. Member for Newcastle upon Tyne Central asked in regard to amendment 18. Her amendment is right that the Government consider that risk before deciding whether to issue designation notices and designated vendor directions.

To conclude, clauses 15 and 16 provide us with the ability to improve the security of our telecommunications networks and to manage the risks relating to high-risk vendors, both now and in the future.
Mr Jones: I thank the Minister for his reply. I do not question his commitment to ensuring that we have security at the heart of the Bill, and I do not intend to press my amendments to a vote.

Chi Onwurah: I will speak to amendments 18 and 19, standing in my name and those of my hon. Friends, and to clauses 15 to 17. As the Minister set out, the clauses are about key powers in the Bill that seek to secure our networks and to regularise requirements already in place, albeit informally or not legally, to remove Huawei as a specific high-risk vendor from our networks. The clauses give Government the powers to do what they have said they will do.

On the clauses, I will not repeat what the Minister said, and I congratulate him on clearly setting out their powers, which the Opposition believe are necessary. I also join the Minister and my right hon. Friend the Member for North Durham in paying tribute to our security services, which do such great work to keep us secure across a wide range of threats and challenges—both present and evolving—and on whose continued work and effectiveness the Bill is highly dependent. As my right hon. Friend set out, we want to ensure that national security is absolutely at the heart of the Bill.

10.30 am

As the Minister set out, the clauses are rightly not specific to Huawei or any vendor or country of origin. It is also important, as the Minister clarified to me in a letter, that they sit in addition to the current process for identifying and designating high-risk vendors and then issuing designated vendor directions, which set out how a designated vendor is to be treated and are critical to ensuring that we do not again find ourselves in a position where we have a high-risk vendor dominant in our telecommunications networks.

Although I accept that the clauses were not designed for Huawei, as is right, the Minister and the Committee must recognise that their impact will be different for Huawei and for future vendors. Parliament—and the sector have spent some years considering the level of risk posed by Huawei specifically, and we have spent some time in this Committee discussing the impact of removing Huawei on the diversity of our supply chain. We have agreement from the Secretary of State, the sector and experts that that leaves us in a position where we have only two vendors, effectively, which is not, as the Minister set out, an acceptable position.

Any further designated vendor notices after the one to deal with Huawei will have a considerable impact and will require considerable consultation. We are in a position now where our telecommunications networks supply chains are not diverse or resilient; that is the general consensus. A further designated vendor notice will therefore have a significant impact on the progress of the diversification of our supply chains, which I do not feel is adequately reflected in the Bill or the debate around it. That is partially what our amendments seek to probe.

We are quite focused on Huawei and the process that got us into the mess that we are in at the moment, having to rip a vendor out of our existing networks. I am not sure that we are sufficiently focused on what will happen in the future should there be a need to designate another vendor, perhaps from a hostile state or perhaps not, because of the impact on security. Our amendments probe whether there is sufficient understanding there.

Amendment 18 amends the list of concerns in clause 16 to which the Secretary of State must pay attention when issuing a designation notice, by adding,

“the person’s control of data flows.”

The list is already quite long, at about 40 lines, and includes,

“the nature of the goods… the reliability of the supply of those goods… the extent to which and the manner in which goods, services or facilities supplied, provided or made available by the person are or might be used in the United Kingdom”.

Our concern, which we are highlighting, is whether those are sufficiently forward-looking, whether we are—as was suggested in evidence sessions—fixated on Huawei, the current architecture and current major security threats, and whether we are looking forward to the evolving security threats. That is because—as we have said and I will repeat—the Labour party puts national security at the heart of our scrutiny of this Bill, as the party of national security, a priority which is above the economic considerations that have too often been prioritised above our national security.

Our concern is that failings in the Bill show that the Government may take risks with the security critical network infrastructure and, as part of that, with our long-term economic security. Data is absolutely central to the information economy, which is the economy. Almost all digital services gather personal data and use it for commercial purposes. Data is often described as the new oil. I prefer to call it the engine of our economy. The international and national flows of data are critical to our security, as well as to our economy. We would like the Minister to explain that the protection for UK data flows is recognised as a threat, which is taken into account by the Secretary of State when considering designation notices.

One reason behind the amendment is what we heard from the Committee’s expert witnesses. In response to my question about different aspects of network security that might not be fully addressed by the Bill as it stands, Dr Louise Bennett, the director of the Digital Policy Alliance, said:

“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.”—[Official Report, Telecommunications (Security) Public Bill Committee, 14 January 2021; c. 52, Q68.]

Dr Bennett suggested that control of data flows was a threat that needed to be specifically addressed by the Bill. Howard Watson, the chief technology officer of BT Group, also said:

“We also faced logical threats, such as malware implants, DDoS attacks and what are called advanced persistent threats, which is an actor embedding themselves into parts of the environment, staying hidden for a while and potentially collecting credentials—think of the SolarWinds hack that is in the news at the moment.”—[Official Report, Telecommunications (Security) Public Bill Committee, 14 January 2021; c. 17, Q16.]

Emily Taylor, chief executive of Oxford Information Labs, said

“It is also the case that consolidation of infrastructure providers, like the cloud providers, is a security risk, because they become too big to fail. There was a brief outage of Google just before Christmas, and people just cannot work. When Cloudflare or Dyn go down, they introduce massive outages, particularly at a
point where we are all so reliant on technology to do our work. These are security risks, and that highlights the need for a flexible approach. You have to be looking across all sectors.

The witness evidence testimonies show that this is not only about the ability to control our signalling systems and protocols in the 5G network as it stands, but as the network evolves more and more of the network control will be both in the centre and on different infrastructure, such as Amazon Web Services in the cloud.

What I particularly want the Minister to respond to the question of how he anticipates the threat from consolidation as the network evolves—this consolidation at cloud level—will be addressed by designation notices? He said that the amendment talks about having regard to designation notices rather than the directions, which would specify the steps that operators have to take. When it comes to making decisions when issuing a designation notice, this requirement fits in with paragraphs (a) to (l), which are already included.

Amendment 19 to clause 17 requires the Secretary of State to lay before Parliament a report on the impact a designation notice will have on telecoms market supply chain diversity to enable parliamentary scrutiny. The amendment seeks to provide greater scrutiny of the diversification of the telecoms market supply chain, which, as we have all agreed, is a prerequisite for the Bill to be effective. It follows amendments 13 and 14, which we have already discussed, in addressing supply chain diversity.

I have mentioned a number of times that the Bill does not refer to the diversification strategy. We heard during the evidence sessions that it was a strategy and not yet a plan. The security of our networks depends on an effective plan to diversify the supply chain, which should also include support for UK capability. The amendment would require that a report be laid before Parliament to set out the impact that the designation notice will have on supply chain diversity. The Minister commented on whether it should be the designation notice or the direction. The objective of the amendment is to ensure discussion and understanding of the impact on the diversification strategy. It is particularly important because, as I have said, any future designation notice will be in the context of a telecoms supply chain that has been significantly reduced as a consequence of Huawei’s removal. It is important that the further impact be understood.

10.45 am

To be clear, we recognise that a designation notice is an appropriate response where there are risks to our national security and to the security of our telecommunication networks, regardless of the impact on diversification. However, we feel strongly that it is important to understand the impact, because of the reduced state of diversification in our supply chain. We cannot have a robust and secure network with only two vendors, and the Government’s emphasis on open RAN technology is yet to be shown to be sufficient to ensure the diversification of our networks in a reasonable timeframe.

I want us to imagine that the Government chose, for whatever reason, to issue a designation notice against one of the remaining vendors—Ericsson or Nokia. It would be critical for the impact on the progress of the diversification strategy to be set out, as well as for discussions to be had with industry and so on. A designated vendor notice could remove a vendor from the supply chain, further reducing resilience and security. I am sure the Minister will agree that it would be important to fully understand the implications, even as we put in place a designation notice. I think we all agree that we are aiming to have a rich diversity of suppliers, but it is also essential to understand the impact of designation notices on that.

We want to encourage the network operators to diversify their supply chains, as we discussed in the evidence sessions. The Bill contains a lot of stick and not very much carrot. A designation notice is absolutely a stick. A requirement to report on the impact on supply chain diversity would encourage the Government to put in place appropriate carrots to increase the incentives for diversification with one hand, as they take away potential vendor diversity in the supply chain with the other.

I support the clauses standing part of the Bill.

The Chair: Order. The hon. Lady has done really well, but we are not debating clause 17 stand part. She can refer to the other clause if she wishes.

Chi Onwurah: Thank you for the clarification, Mr Hollobone. I see that we are discussing whether clauses 15 and 16 stand part. I support those clauses and look forward to the Minister’s response to the amendment.

Matt Warman: I pre-emptively covered a lot of the hon. Lady’s questions, but I will say two brief things. She talked about consolidation in the cloud sector. While the Bill is very much a national security Bill, the National Security and Investment Bill would cover consolidation in that sort of sector, rather than this one. Obviously they do work together.

Chi Onwurah: The point I am making—clearly, I did not make it effectively—is that that sector is becoming this sector. The cloud sector is becoming the telecoms sector. The reason we need this Bill in addition to the National Security and Investment Bill is to address the security concerns of the telecoms sector specifically. The cloud sector is becoming part of the telecoms sector, yet the Bill does not address those concerns.

Matt Warman: The hon. Lady is not wrong, obviously, in the sense that there is a potential conversation to be had about when a cloud provider is a telecoms provider and vice versa, if I can put it like that, although it is not the most elegant way of doing so. However, the point is that the reason we have comprehensive coverage of the landscape is because we have both the National Security and Investment Bill, which she debated recently, and this Bill. The broad powers that she described are intended to provide precisely that sort of coverage.

Similarly, the hon. Lady referred to the length of the list in clause 16 of matters that can be taken into consideration. That relates to the point I made previously, namely that the sorts of issues that she is talking about, such as data flows, are already covered in the long list.

The list is as long as it is because it is intended to look to the future. Therefore, being prescriptive in the way that she describes is fundamentally unnecessary. We are not excluding what she wants to be on the list. A matter is
already very much there if it is pertinent to national security. For that reason, I do not think there is a compelling case to add that single topic to the list, both because it is already there and because if we start going down that route, we could make the case for adding a host of other things that are already covered but that people might want to be mentioned specifically.

As I said earlier on the convergence of the two sectors, the point is that we have comprehensive coverage through both Bills. It will be for the NCSC, Ofcom and the Government to make a judgment as to whether any consolidation in a sector poses a national security risk.

Mr Jones: I beg to ask leave to withdraw the amendment.

Amendment, by leave, withdrawn.

Clauses 15 and 16 ordered to stand part of the Bill.

Mr Jones: I beg to ask leave to withdraw the amendment.

Amendment, by leave, withdrawn.

Clauses 15 and 16 ordered to stand part of the Bill.

Clause 17

Laying Before Parliament

The Chair: We now come to amendment 20 to clause 17. This is Christian Matheson’s big moment. I call him to move the amendment.

Christian Matheson (City of Chester) (Lab): I beg to move amendment 20, in clause 17, page 29, line 31, at end insert—

“(4) Where the Secretary of State considers that laying a copy of the direction or notice (as the case may be) before Parliament would, under subsection (2), be contrary to the interests of national security, a copy of the direction or notice must be provided to the Intelligence and Security Committee of Parliament as soon as reasonably practicable.

(5) Any information excluded from what is laid before Parliament under the provision in subsection (3)(b) must be provided to the Intelligence and Security Committee of Parliament as soon as reasonably practicable.

This amendment would ensure that the Intelligence and Security Committee of Parliament is provided with any information relating to a designated vendor direction or designation notice which on grounds of national security is not laid before Parliament, thereby enabling parliamentary oversight of all directions and notices.

The Chair: With this, it will be convenient to discuss the following: amendment 22, in clause 20, page 35, line 30, at end insert—

“(9) The Secretary of State must provide the Intelligence and Security Committee of Parliament with a copy of any notification under this section relating to a designated vendor direction, designation notice, a notice of a variation or revocation of a designated vendor direction or a notice of a variation or revocation of a designation notice to which subsection (2) or (3)(b) of section 105Z11 applies.”

This amendment would require the Secretary of State to provide the Intelligence and Security Committee of Parliament with a copy of any confirmation decision which relates to a direction or notice that has not been laid before Parliament on grounds of national security.

Amendment 24, in clause 21, page 39, line 9, at end insert—

“(6) The Secretary of State must provide the Intelligence and Security Committee of Parliament with a copy of any urgent enforcement direction relating to a designated vendor direction to which subsection (2) or (3)(b) of section 105Z11 applies.”

This amendment would require the Secretary of State to provide the Intelligence and Security Committee of Parliament with a copy of any urgent enforcement direction which relates to a direction that has not been laid before Parliament on grounds of national security.

Amendment 25, in clause 21, page 40, line 6, at end insert—

“(8) The Secretary of State must provide the Intelligence and Security Committee of Parliament with a copy of any confirmation of an urgent enforcement notification relating to a designated vendor direction to which subsection (2) or (3)(b) of section 105Z11 applies.”

This amendment would require the Secretary of State to provide the Intelligence and Security Committee of Parliament with a copy of any confirmation of an urgent enforcement notification which relates to a direction that has not been laid before Parliament on grounds of national security.

Christian Matheson: I am sure the Committee has been waiting with bated breath for my big moment all morning, Mr Hollobone. May I say what a great pleasure it is to serve under your chairmanship?

I had prepared some notes to help me present the amendments, but I need not have bothered: I could simply have taken the Hansard report from last week and quoted my right hon. Friend the Member for North Durham. He talked about being a stuck record, but he is not; he is being consistent. I like to think that Labour has been consistent throughout the detailed consideration of the Bill. My hon. Friend the Member for Newcastle upon Tyne Central talked about the three areas that we consistently think would improve the Bill, and the amendment falls into one of those areas: scrutiny and the role of the Intelligence and Security Committee.

I refer to my right hon. Friend’s speech last week on amendment 9, when he talked about the desire to help the Bill. He also laid down a challenge. He commented on the fact that I thought that some parts of his speech were inspirational. They were, because they made me think quite a lot. There was one lightbulb moment when he used his experience of, I believe, 20 years in the House this year—on which I congratulate him—and said that the chances are that a similar amendment will be proposed in their lordships’ House and the Government may well agree to it.

My right hon. Friend also said that it is not necessarily a good thing for the Minister—not in this case, mind you—to be a tough guy who wants to get through the Bill without any amendments, when there is a genuine desire among the Opposition to get the Bill through. I remind the Minister and Government Members that we support the Bill. There have been occasions when an Opposition have tried to scupper, delay or make mischief with a Bill. I assure Government Members—I hope it is obvious to them—that there is no such skullduggery on this side of the House, not with this Bill and not ever, and certainly not when my hon. Friend the Member for Newcastle upon Tyne Central, my right hon. Friend the Member for North Durham and I on the Bill Committee. We are genuinely keen to improve the Bill during its passage.
The amendment again falls into one of the three areas my hon. Friend the Member for Newcastle upon Tyne Central has identified as necessary. As the Minister may have guessed, the chances are that we will not put it to the vote, but we do ask that he gives it careful consideration. I refer the Committee to the speech by my right hon. Friend the Member for North Durham last week about the role of the Intelligence and Security Committee. Amendments 20 to 25 relate to different clauses, but have the common aim of ensuring that there is correct parliamentary oversight of the process outlined in the Bill, specifically by referring all orders made under proposed new section 105Z11 of the Communications Act 2003 to the Intelligence and Security Committee.

It would normally be the Digital, Culture, Media and Sport Committee that would take on telecommunications matters. Additionally, the Secretary of State may lay orders before Parliament for general consideration and scrutiny. However, the Bill has our national security at its heart, and, as a proud former member of the Culture, Media and Sport Committee, I am the first to admit that it would not be at all an appropriate forum for the consideration of such reporting to take place, nor would it be the normal procedure for laying orders before this House or the other place, either in general or on the specifics of the order.

As we touched on last week, the temptation is therefore the default position that no reporting at all would take place, which is clearly not desirable. I hope the Minister will confirm that that is not the Government’s intention. To be fair, I think he touched on that point last week, but it would be helpful if he could touch on it again.

The use of the ISC is therefore an elegant and obvious solution. The Committee, of which my right hon. Friend the Member for North Durham is such a distinguished member, has worked well and has the confidence of the House. It provides a secure and trusted forum for decisions of the Secretary of State that may have far-reaching commercial and technical implications, as well as security implications, to be scrutinised and considered by hon. Members who are able to receive the full facts and make a judgment based on them, while giving nothing away to those who wish us ill and would exploit our open democracy in doing so. I see no reason why our determination to protect our communications infrastructure should be used against us by our adversaries, but nor should that determination be traded off with a reduction in parliamentary scrutiny of the Executive and agencies that act on behalf of us all.

The ISC is there for a reason: it is precisely to cover situations such as this. If the Minister can propose an alternative solution that balances security with scrutiny, we would be pleased to hear it. I suspect this solution would also make commercial UK businesses more open to scrutiny themselves by offering a level of confidentiality, although I accept that that is not the primary role of the ISC.

It should also not be option for the Secretary of State to report. Such a chaotic patchwork would undermine the integrity of the Bill and the processes that we are setting up. Failing any alternative being proposed, we believe that these amendments, which involve the ISC acting on behalf of the whole House—indeed, the whole of Parliament—would fill a glaring hole and enhance the Bill. I commend them to the Committee.

Mr Jones: My hon. Friend the Member for City of Chester said that we were going over old ground, and to a certain extent we are because some of the amendments reflect those that I moved last week.

May I say at the outset, Mr Hollobone, that the Minister has been an exemplar in engaging with and briefing the ISC? He has set something of a precedent; usually we have only Cabinet Ministers or Prime Ministers before us to give evidence. He is one of the few junior Ministers to have appeared before us, so I congratulate him. He did it because he wanted to engage with the issues. He must therefore be commended on his commitment to ensure that there is scrutiny. However—this is not to wish his demise, but to argue for his promotion—he will not be there forever. I think he does not quite understand why the Government are not at least moving on this.

The ISC’s remit is defined in the Justice and Security Act 2013. It sets out which Departments we cover, and the Department for Digital, Culture, Media and Sport is not one of them. However, as I said last week, security is increasingly being covered by other Departments, and this Bill is a good example. The National Security and Investment Bill is another one, where security decisions will be taken by the Secretary of State for Business, Energy and Industrial Strategy. Parliament must be able to scrutinise that.

If a high-risk vendor is designated as banned from the network by the Secretary of State for Digital, Culture, Media and Sport, there are perfectly good reasons why the intelligence behind that cannot be put into the public domain. The methods by which such information is acquired are of a highly sensitive nature, so it would not only expose our security services’ techniques, but in some cases would make vulnerable the individuals who have been the source of that information. I think most people would accept that that is a very good reason.

This sort of thing is happening increasingly. We have the two Bills that I have referred to, but we also have the Covert Human Intelligence Sources (Criminal Conduct) Bill, which will come back to the House tomorrow. Covert human intelligence and the ability to collect intelligence on behalf of our security services is very important. Most of that is covered by the Home Office, and covert human intelligence sources are covered by the ISC’s remit and can be scrutinised. However, there is a long list of other organisations that will be covered by tomorrow’s Bill, including—we never quite got to the bottom of this—the Food Standards Agency, for example. Again, how do we ensure that there is scrutiny of the decisions?

We also have—this has come out of the pandemic—the new biosecurity unit in the Department of Health. Again, there is no parliamentary scrutiny, because the Health and Social Care Committee will not be able to look at the intelligence that supports so much of that. An easy way out of this is in the Justice and Security Act 2013: the memorandum of understanding, which just means that, were our remit extended to look at this and other matters, the ISC could oversee and ask for the intelligence.

Having spoken to the Business Secretary and the Minister, who sympathises with us, I am not sure where the logjam is in Government. The point is that an amendment will be tabled in the Lords. Whether the
[Mr Kevan Jones] provision is in the Bill or just in the memorandum of understanding between the Prime Minister and the ISC, it is easily done and would give confidence that the process at least had parliamentary oversight.

On many of these decisions, frankly, the oversight would not be onerous; we are asking only that we are informed of them. On some occasions, we might not even want to look at the intelligence. It might be so straightforward that, frankly, it is not necessary, so I do not think that it is an administrative burden. I cannot understand what the problem is. To reiterate what I said last week in Committee, it is not about the ISC wanting to have a veto or block over such things. It is, rightly, for the Government and the Secretary of State to make and defend those decisions.

It is also not about the ISC embarrassing the Government, because we cannot talk in public about a lot of the information that we receive. It is not as though we would publish a publicly available report, because of the highly classified nature of the information. However, the ISC can scrutinise decisions and, if it has concerns, write to the Prime Minister or produce a report for the Prime Minister raising them. That gives parliamentary scrutiny of the Executive’s decisions.

As I say, the report might not be made public. People might ask, “Would that be a new thing?” No—it happens all the time. For example, on the well-publicised Russia report this year, there was a public report with redactions in it and quite an extensive annex, which raised some issues that we were concerned about. That annex was seen only by individuals in Government, including the Prime Minister.

There is already a mechanism, so I fail to understand why the Government want to oppose this. From talking to Ministers privately, I think that there is a lot of sympathy with the position and I think that we will get there eventually. How we get there and in what format, I am not sure—whether the method is to put it in the Bill or to do it through the mechanism in the 2013 Act. That might be a way forward.

Chi Onwurah: I rise to support the excellent comments made by my hon. Friend the Member for City of Chester and my right hon. Friend the Member for North Durham. I did well to delay my remarks till after my right hon. Friend had spoken, because he has set out very effectively, based on his considerable experience as a long-standing member of the Intelligence and Security Committee, both why it is important that that Committee should be consulted and receive the reports, and why it is hard to understand the Minister’s reluctance both in this Bill and in the National Security and Investment Bill to involve a source of such credible security expertise and, importantly, security clearance in key issues of national security.

I want to add two points to those made by my right hon. and hon. Friends. The first is to reiterate a point made previously: our security threats are changing, evolving and, unfortunately, diversifying. We see that in changes to our defence spending, in changes in the national review of our defence capabilities, and in changes in the evolution of the geopolitical landscape—the potential source of threats. However, the Minister does not seem able to support reflecting that by ensuring that, rather than keeping to our existing modes of parliamentary scrutiny, we enable parliamentary scrutiny of issues of national security by those who are best placed to carry out such scrutiny—undoubtedly members of the Intelligence and Security Committee.

I want to point briefly to a discussion in the evidence sessions. Ofcom made it clear that it does not consider itself in a position to make national security decisions, which is understandable, and that some of the decisions and considerations about national security with regards to telecommunications networks would require people who have STRAP clearance. Ofcom’s group director for networks and communications pointed to the fact that she had had STRAP clearance previously, and she said that if the NCSC “feels that that is needed for the type of information that we may need to handle, we would make sure that happened.”—[Official Report, Telecommunications (Security) Public Bill Committee, 14 January 2021; c. 90, Q115.]

To my knowledge, Digital, Culture, Media and Sport Committee members do not have STRAP clearance. I would like the Minister to comment specifically on the level of security clearance required for members of the Committee that he has identified as being the location for scrutiny of important issues of national security. What level of security clearance do its members have? Would that enable the scrutiny that we all agree is in the best interests of the Bill?

I would like the Minister to respond to a specific example. Amendments 20, 22, 23, 24 and 25 are designed to require that the Intelligence and Security Committee has access to the appropriate information. There is a requirement for the Secretary of State to lay before Parliament a copy of a designated vendor direction, as set out in clause 15, which inserts new section 105Z11 into the Communications Act 2003. The new section states:

“The Secretary of State must lay before Parliament a copy of—

(a) a designated vendor direction;
(b) a designation notice;
(c) a notice of a variation or revocation of a designated vendor direction; and
(d) a notice of a variation or revocation of a designation notice.”

So far, so good—we have that scrutiny. However, the new section also says:

“The requirement in subsection (1) does not apply if the Secretary of State considers that laying a copy of the direction or notice (as the case may be) before Parliament would be contrary to the interests of national security.”

11.15 am

My right hon. Friend the Member for North Durham alluded to occasions when, we can see, that would be the case. I should like the Minister to respond specifically. Imagine, for example, that through the work of our excellent security services we became aware that a telecoms start-up in this country or abroad was under the undue influence of someone hostile to our national interest, and its integrity was compromised, and that those who had come by the information did not want to share with the wider world how they had done so. Indeed, as my right hon. Friend said, sharing that information might compromise the means by which it was acquired. It might also have a significant impact on the stock market price of the company, and perhaps of other companies
or British institutions that were invested in it. That information could not be shared publicly. Yet there could not be an understanding of the reason for the designation notice or effective scrutiny of it by Parliament unless the information was shared in some secure way. Surely that secure way would be sharing it with the ISC.

To take another example, what would happen if the security services became aware that the billionaire owner of one of our major suppliers for, say, cloud services was compromised in some way or that it was going to be bought by a hostile actor? I have previously suggested that I want to understand how the Bill would address the potential for, say, Amazon Web Services to be bought by a hostile actor, and the influence that that would have on our security.

That information would be incredibly security-sensitive, but it would also be market-sensitive. My hon. Friend the Member for City of Chester said that market sensitivity is not the primary reason for the amendments. We prioritise national security. However, let us recognise that questions of national security have a huge impact on our markets as well, and our markets are influential on national security.

Under the clause the Secretary of State would not need to lay a copy of the direction or notice before Parliament if it would be contrary to the interests of national security. Revealing the way we obtain security information through our excellent security services would clearly be contrary to the interests of national security. How would the Minister ensure that there would be an appropriate level of scrutiny for a notice of that kind, which would not be laid before Parliament for reasons of national security? How would scrutiny be maintained?

I look forward to the Minister’s response. I emphasise that we support clause 18—[Interruption.] I am sorry. We are discussing clause 17.

The Chair: We are.

Chi Onwurah: We support clause 17 and our amendments are intended to make it more accountable to Parliament and therefore more successful and effective in securing our national security.

The Chair: Order. I misled the hon. Lady. We are now discussing amendments 20 and 22 to 25. When we finish the debate on those amendments, we will debate clause 17 stand part. The hon. Lady may want to save this part of her remarks until the next debate.

Chi Onwurah: Thank you, Mr Hollobone. It is sometimes confusing to know exactly what is being discussed at what point. With that, I ask the Minister to respond to our concerns about the scrutiny of the powers in the clause.

Matt Warman: I welcome the second salvo in the campaign to address this matter by the right hon. Member for North Durham. He said it would be an ongoing campaign.

This group of amendments would require the Secretary of State to provide information relating to a designated vendor direction or designation notice to the ISC. The amendments would require the Secretary of State to do this only where directions and designation notices had not been laid before Parliament, whether in full or in part, as a result of the national security exemptions in clause 17. It will not surprise the right hon. Member for North Durham or other Opposition Members that some of these short remarks will overlap with the conversation that we had earlier on a similar matter.

Amendment 20 would require designated vendor directions or designation notices to be provided to the ISC. Amendments 22 to 25 would require the Secretary of State also to provide the ISC with copies of any notifications of contraventions, confirmation decisions and so on. Although I recognise some Members’ desire for the ISC to play a greater role in the oversight of national security decision making across government, including in relation to this Bill, the amendments would, as the right hon. Member for North Durham knows, extend the ISC’s role in an unprecedented way. None the less, I thank his welcome for my unprecedented appearance.

As I said in the debate on amendment 9, the ISC’s primary focus is to oversee the work of the security and intelligence agencies. Its remit is clearly defined in the Justice and Security Act 2013, and the accompanying statutory memorandum of understanding, to which the right hon. Gentleman referred. I do not think he thinks it is my place to take a view on that role, and I do not think this Bill is the place to have that debate.

Mr Jones: Yes, but I would ask the Minister’s civil servants to read the Act before they write this stuff for him. The Act refers to “intelligence”. Our remit is not fixed by a Department. I know the Minister sympathises with this and that we will get there eventually, but I say to his civil servants, please read the Act.

Matt Warman: I will come on to that. Accepting any of these unilateral amendments to this Bill is not the appropriate place to achieve an overall enhanced role for the ISC—

Mr Jones: I am sorry to say to the Minister that it is not looking for an enhanced role at all. It is actually doing what it says in the Justice and Security Act 2013. It is about scrutinising intelligence. A lot of the information, which will be used by him and others in these orders, will be derived from the same decisions that we oversee.

Matt Warman: Absolutely. Members of the Committee should note that in exercising the powers created by this Bill, the Secretary of State will be advised by the NCSC on relevant technical and national security matters. The NCSC’s work already falls within the Intelligence and Security Committee’s remit, so the right hon. Gentleman has found his own salvation.

In that context, the amendment seems to duplicate that existing power, while also seeking to do something that is better done in reform of a different Act, if that is what the right hon. Gentleman seeks. I am sorry to disappoint him again. I think he knew already that I would do that, but I look forward to his third, fourth and fifth salvos in his ongoing campaign.

Christian Matheson: I hear the Minister’s explanation, which we have been over before when considering other amendments. He talks about other salvos by my right hon. Friend the Member for North Durham. I go back to the statement that my right hon. Friend made last week, which is that he expects that at some point something will happen and we will move forward.
The Chair: Order. If the hon. Gentleman would like to chair this afternoon’s sitting, I am sure we could arrange for him to do that. I know Members will be disappointed, but I am instructed to say that as it is 11.25 am, the Committee is now adjourned.

11.25 am
The Chair adjourned the Committee without Question put (Standing Order No. 88).

Adjourned till this day at Two o’clock.
PARLIAMENTARY DEBATES
HOUSE OF COMMONS
OFFICIAL REPORT
GENERAL COMMITTEES

Public Bill Committee

TELECOMMUNICATIONS (SECURITY) BILL

Eighth Sitting
Tuesday 26 January 2021
(Afternoon)

CONTENTS
Clauses 17 to 29 agreed to, one with amendments.
New clauses considered.
Bill, as amended, to be reported.
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

Saturday 30 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 *(Hyndburn)* (Con)
† Cates, Miriam *(Penistone and Stocksbridge)* (Con)
† Caulfield, Maria *(Lewes)* (Con)
Clark, Feryal *(Enfield North)* (Lab)
Crawley, Angela *(Lanark and Hamilton East)* (SNP)
† Johnston, David *(Wantage)* (Con)
† Jones, Mr Kevan *(North Durham)* (Lab)
† Lamont, John *(Berwickshire, Roxburgh and Selkirk)* (Con)
† Matheson, Christian *(City of Chester)* (Lab)
† Onurah, Chi *(Newcastle upon Tyne Central)* (Lab)
† Richardson, Angela *(Guildford)* (Con)
† Russell, Dean *(Watford)* (Con)
† Sunderland, James *(Bracknell)* (Con)
Thomson, Richard *(Gordon)* (SNP)
† Warman, Matt *(Parliamentary Under-Secretary of State for Digital, Culture, Media and Sport)*
West, Catherine *(Hornsey and Wood Green)* (Lab)
† Wild, James *(North West Norfolk)* (Con)

Sarah Thatcher, Huw Yardley, Committee Clerks

† attended the Committee
Telecommunications (Security) Bill

2 pm

The Chair: Before we begin, I know this is difficult and people forget, but Mr Speaker is clear: we should be wearing our masks if we are not speaking. I ask you to do your best to comply with that, because it is sensitive. The rules under which the House is allowed to operate have been agreed with health and safety, meaning that if we are not complying, not only are you putting everyone at risk, but unfortunately all the work that has been done could be invalidated. I urge people to do their best to remember.

Clause 17

Amendment proposed (this day): 20, in clause 17, page 29, line 31, at end insert—

“(4) Where the Secretary of State considers that laying a copy of the direction or notice (as the case may be) before Parliament would, under subsection (2), be contrary to the interests of national security, a copy of the direction or notice must be provided to the Intelligence and Security Committee of Parliament as soon as reasonably practicable.

(5) Any information excluded from what is laid before Parliament under the provision in subsection (3)(b) must be provided to the Intelligence and Security Committee of Parliament as soon as reasonably practicable.”—(Christian Matheson.)

This amendment would ensure that the Intelligence and Security Committee of Parliament is provided with any information relating to a designated vendor direction or designation notice which on grounds of national security is not laid before Parliament, thereby enabling Parliamentary oversight of all directions and notices.

Question again proposed. That the amendment be made.

The Chair: I remind the Committee that with this we are discussing the following:

Amendment 22, in clause 20, page 35, line 30, at end insert—

“(9) The Secretary of State must provide the Intelligence and Security Committee of Parliament with a copy of any notification under this section relating to a designated vendor direction, designation notice, a notice of a variation or revocation of a designated vendor direction or a notice of a variation or revocation of a designation notice to which subsection (2) or (3)(b) of section 105Z11 applies.”

This amendment would require the Secretary of State to provide the Intelligence and Security Committee of Parliament with a copy of any notification under this section relating to a designated vendor direction or a designation notice which has not been laid before Parliament on grounds of national security.

Amendment 23, in clause 20, page 37, line 41, at end insert—

“(10) The Secretary of State must provide the Intelligence and Security Committee of Parliament with a copy of any confirmation decision relating to a designated vendor direction, designation notice, a notice of a variation or revocation of a designated vendor direction or a notice of a variation or revocation of a designation notice to which subsection (2) or (3)(b) of section 105Z11 applies.”

This amendment would require the Secretary of State to provide the Intelligence and Security Committee of Parliament with a copy of any confirmation decision which relates to a direction or notice that has not been laid before Parliament on grounds of national security.

Amendment 24, in clause 21, page 39, line 9, at end insert—

“(6) The Secretary of State must provide the Intelligence and Security Committee of Parliament with a copy of any urgent enforcement direction relating to a designated vendor direction to which subsection (2) or (3)(b) of section 105Z11 applies.”

This amendment would require the Secretary of State to provide the Intelligence and Security Committee of Parliament with a copy of any urgent enforcement direction which relates to a direction that has not been laid before Parliament on grounds of national security.

Amendment 25, in clause 21, page 40, line 6, at end insert—

“(8) The Secretary of State must provide the Intelligence and Security Committee of Parliament with a copy of any confirmation of an urgent enforcement notification relating to a designated vendor direction to which subsection (2) or (3)(b) of section 105Z11 applies.”

This amendment would require the Secretary of State to provide the Intelligence and Security Committee of Parliament with a copy of any confirmation of an urgent enforcement notification which relates to a direction that has not been laid before Parliament on grounds of national security.

I need to understand, Mr Matheson, what your intention is.

Christian Matheson (City of Chester) (Lab): As you correctly say, Mr McCabe, I need to announce my intention, but just as I was about to, the Committee was halted. I am reminded of the occasion involving that notorious football referee Clive Thomas. The 1978 World Cup blew up against Brazil because, as the ball was heading towards the goal, he disallowed the goal. That was rather how I felt this morning.

That said, I do not wish to press the matter further, despite the fact that I had devastating remarks that would have swayed the Minister. I will not put my amendments to the vote. I beg to ask leave to withdraw the amendment.

Amendment, by leave, withdrawn.

Clause 17 ordered to stand part of the Bill.

Clause 18

Monitoring of designated vendor directions

Question proposed, That the clause stand part of the Bill.

The Chair: With this it will be convenient to discuss clauses 19 to 23 stand part.

The Parliamentary Under-Secretary of State for Digital, Culture, Media and Sport (Matt Warman): It is a pleasure to be back under your chairmanship, Mr McCabe.

I will try to rattle through these as quickly as I can. Clauses 18 to 23 cover monitoring and enforcement, and further provisions relating to non-disclosure and information requirements. Clause 18 gives the Secretary of State the power to give Ofcom a monitoring direction, requiring the regulator to obtain information relating to a public telecoms provider’s compliance with a designated vendor direction and to provide that information in a report to the Secretary of State.

The clause also includes requirements about the form of such reports and the procedures around their provision, but it does not create any new powers for Ofcom, which already has them under section 135 of the Communications
Act 2003. The provisions in the clause are an integral part of the compliance regime. The power to give a monitoring direction to Ofcom is necessary to ensure that the Secretary of State has the ability to require it to provide the information needed to assess compliance with designated vendor directions.

Clause 19 provides Ofcom with the power to give inspection notices to public communications providers. The provisions will apply only where the Secretary of State has given Ofcom a monitoring direction. Inspection notices enable Ofcom to gather information from communications providers in relation to their compliance with a direction. The notices are a tool for Ofcom to give effect to its obligations under a monitoring direction.

Clause 19 also sets out the new duties that inspection notices can impose, the types of information that they can be used to obtain and how the duties in an inspection notice will be enforced. Ofcom may only give inspection notices in order to obtain information relating to whether a provider has complied or is complying with a direction. The notice power cannot be used to obtain information relating to whether a provider has complied or is complying with a direction. The notice power cannot be used to obtain information relating to how a provider is preparing to comply with a direction. Ofcom can instead use its other information-gathering powers under section 135 of the Communications Act 2003 to obtain such information.

Clause 20 provides the Secretary of State with the powers necessary to enforce compliance with designated vendor directions, as well as with any requirement for a public communications provider to prepare a plan setting out the steps it intends to take to comply. It is the Secretary of State’s responsibility to issue directions where necessary in the interest of national security. Clause 20 is essential to ensure that the Secretary of State can carry out this role effectively and enforce compliance with any directions issued. New sections 105Z18 to 105Z21 will be inserted into the Communications Act 2003 for this purpose. The provisions set out the process that the Secretary of State will follow in instances where an assessment is made that a public communications provider is not acting in compliance with the direction or with the requirement to provide a plan. The process encompasses giving a contravention notice, enforcing it and imposing penalties for non-compliance. The clause is essential in ensuring that the Secretary of State can carry out the role effectively and deters and penalises instances of non-compliance.

Clause 21 provides the Secretary of State with the power to give urgent enforcement directions. Provisions to enable urgent enforcement are needed in cases where the Secretary of State considers that urgent action is necessary to protect national security or to prevent significant harm to the security of a public electronic communications network, service or facility.

Clause 22 creates a power for the Secretary of State to impose a requirement on public communications providers or vendors not to disclose certain types of information without permission. The provisions are necessary to prevent the unauthorised disclosure of information, which would be contrary to the interest of national security.

Finally, clause 23 creates a power for the Secretary of State to require information from a public communications provider or any other person who may have information relevant to the exercise of the Secretary of State’s functions under clauses 18 to 21. For example, the Secretary of State can require information on a provider’s planned use of such goods or information relating to how a network is provided. It can also include information about the proposed supply of goods or services. The ability to gather such information would ensure that the Secretary of State is able to make well-informed decisions when considering whether to issue designation notices and designated vendor directions. Information obtained through the use of this power can also be used to support the monitoring of compliance, with directions supplementing information gathered by Ofcom through its information-gathering and inspection notice powers.

To summarise, new sections 105Z18 to 105Z21 together establish the power and processes that outline how the designated vendor regime will be monitored and enforced. The provisions in clause 22 are needed to manage the disclosure of information, the unauthorised disclosure of which may be contrary to national security, and clause 23 will ensure that the Secretary of State is able to obtain the information necessary to make assessments to determine whether to give a notice or direction and to assess compliance.

Chi Onwurah (Newcastle upon Tyne Central) (Lab): It is a pleasure to serve under your chairmanship once again, Mr McCabe. I will not detain the Committee long with a consideration of the clauses, and I thank the Minister for so ably setting out what the clauses aim to achieve. Indeed, we on this side recognise the importance and the necessity of clauses 18 to 23 in establishing the process and ensuring the powers to obtain information and enforce direction as part of that process.

We only reiterate a small number of important points to draw attention once again to the breadth of the powers, which enable the Secretary of State to require information to an almost unlimited extent. Given the breadth of the powers, the information and progress on the telecommunications diversification strategy is, once again, notable by its absence. Given the breadth of the requirements, it is notable that there is nothing on progress on the diversification strategy. Nor, if my memory serves me correctly, does the impact assessment reflect the potential costs to either the network operators or Ofcom in exercising these powers. The clauses do not set out the impact and they emphasise once again the importance of Ofcom having the appropriate resources to enable it to carry out the requirements effectively. I hope that the Minister will bear those limitations in mind in his ongoing review of the Bill.

Question put and agreed to.
Clause 18 accordingly ordered to stand part of the Bill.
Clauses 19 to 23 ordered to stand part of the Bill.

Clause 24

Chi Onwurah (Newcastle upon Tyne Central) (Lab): With this it will be convenient to discuss clause 25 stand part.

Matt Warman: Clause 24 enables higher penalties than those currently set out in the Communications Act 2003 to be issued by Ofcom, and clause 25 makes two necessary consequential amendments to that Act.
[Matt Warman]

The penalties under clause 24 can be imposed for contraventions of requirements to provide information to Ofcom for the purpose of its security-related functions. That includes when providers do not provide information requested by Ofcom for the purpose of providing a report to the Secretary of State.

Penalties can be set at a maximum of £10 million or, in the case of a continuing contravention, up to £50,000 a day. These maximum penalties are a marked increase on the existing ones, which are capped at £2 million, or £500 a day. This clause ensures that the maximum penalties are the same as those in clause 23. The size of these penalties is appropriate given the potential impact of the situation described. Proposed new section 139ZA(5) of the 2003 Act, inserted by this clause, gives the Secretary of State the power to change, by regulations subject to the affirmative procedure, the maximum amount of the fixed and daily penalties. That will help to future-proof the framework by ensuring that penalties can be adjusted over time—for example, because of inflation.

In summary, clause 24 enables Ofcom to issue the financial penalties necessary to ensure that providers supply it with the information that it needs. Clause 25 contains the consequential amendments to that, which are necessary because the Bill creates a number of powers to make regulations and some of those regulations will amend primary legislation.

2.15 pm

Question put and agreed to.

Clause 24 accordingly ordered to stand part of the Bill.

Clause 25 ordered to stand part of the Bill.

Clause 26

FINANCIAL PROVISION

Question proposed, That the clause stand part of the Bill.

The Chair: With this it will be convenient to discuss the following:

Clause 27 stand part.

Government amendments 1 to 4.

Clauses 28 and 29 stand part.

Matt Warman: I will be brief, but it is important to cover the Government amendments. The clause provides that any increase in expenditure attributable to the Bill is paid out by Parliament. Clause 27 covers the extent of the Bill and clause 28 provides for the commencement of the Bill’s provisions.

I turn to the small set of amendments that the Government deem necessary, given that the Bill will be carried over to the second Session. The Bill creates new national security powers for the Secretary of State to address the risks posed by high-risk vendors through the issuing and enforcement of designated vendor directions in clauses 15 to 23 and 24. Amendment 1 enables clauses 15 to 23 to come into force on the day on which the Bill receives Royal Assent. Amendment 2 ensures that the higher penalties also come into force. Amendment 3 removes the subsection of clause 28 providing for sections to come into force at the end of the two-month period. Finally, amendment 4 ensures that the provisions of clause 24 that are not commenced early come into force via commencement regulations on a day determined by the Secretary of State. Without the amendments, the provisions relating to those powers would come into force two months after the Bill receives Royal Assent, which could put at risk the timely implementation of this important policy.

Question put and agreed to.

Clause 26 accordingly ordered to stand part of the Bill.

Clause 27 ordered to stand part of the Bill.

Clause 28

COMMENCEMENT

Amendments made: 1, in clause 28, page 46, line 19, leave out “section 14” and insert “sections 14 to 23”.

This amendment would cause clauses 15 to 23 to come into force on Royal Assent.

Amendment 2, in clause 28, page 46, line 19, at end insert—

“(ca) section 24, so far as it relates to section 18;”.

This amendment is consequential upon Amendment 1. Clause 24 provides for higher penalties to be available for certain contraventions of information requirements, including contraventions associated with section 105Z12 of the Communications Act 2003, which is inserted by clause 18.

Amendment 3, in clause 28, page 46, line 25, leave out subsection (2).

This amendment is consequential upon Amendments 1 and 2.

Amendment 4, in clause 28, page 46, line 30, at end insert—

“(ba) section 24 (so far as not already in force by virtue of subsection (1))”.

This amendment is consequential upon Amendments 1 and 2.

Clause 28, as amended, ordered to stand part of the Bill.

Clause 29 ordered to stand part of the Bill.

New Clause 3

DUTY OF OFCOM TO REPORT ON ITS RESOURCES

‘(1) Ofcom must publish an annual report on the effect on its resources of fulfilling its duties under this Act.

(2) The report required by subsection (1) must include an assessment of—

(a) the adequacy of Ofcom’s budget and funding;

(b) the adequacy of staffing levels in Ofcom; and

(c) any skills shortages faced by Ofcom’.’.—(Christian Matheson.)

This new clause introduces an obligation on Ofcom to report on the adequacy of their existing budget following the implementation of new responsibilities.

Brought up, and read the First time.

Christian Matheson: I beg to move, That the clause be read a Second time.

The Chair: With this it will be convenient to discuss new clause 7— Review of Ofcom’s capacity and capability to undertake duties (No.2)—

‘(1) The Communications Act 2003 is amended as follows.

(2) After section 105Z29 insert—

“105Z30 Review of Ofcom’s capacity and capability to undertake duties

The Secretary of State must, not later than 12 months after the day on which the Telecommunications (Security) Act 2021 is passed, lay before Parliament a report on Ofcom’s capacity and capability to undertake its duties under this Act in relation to the security of public electronic communications networks and services.”.’
This new clause would require the Secretary of State to report on Ofcom’s capacity and capability to undertake the duties provided for in the Telecommunications (Security) Bill which would be inserted into the Communications Act 2003 under the cross-heading “Security of public electronic communications networks and services” (which would encompass all the clause numbers which start with 105).

Christian Matheson: I do not want to detain the Committee all that long. The basis of the new clause is to ensure that Ofcom has the staffing and financial resources, as well as the capacity and technical capability, to undertake its new responsibilities under the Bill.

I remind the Committee that we heard in the evidence sessions that this is only one of several new areas of responsibility that Ofcom has received in recent years. For example, it now has responsibilities for regulating aspects of the work of the BBC. Parliament will be presenting Ofcom with responsibilities in relation to online harms, all of which is to be welcomed, but we have to recognise that there will be an overstretched for Ofcom.

In the area that the Committee is considering, there are technical complications that require specific sets of talents and capabilities which, we have heard previously, are not always in ready supply in the sector. We heard evidence that Ofcom, in common with other public sector bodies, does not pay as highly as some high-end consultancies, suppliers, developers or software houses, and therefore there will be churn. I do not want to stand in the way of anyone’s career development, but understandably there will be churn, in terms of Ofcom’s ability to maintain its responsibilities in what we know will be a continually evolving sector that throws up new technical challenges.

New clause 3 provides a duty on Ofcom to report on its resources, including the “the adequacy of Ofcom’s budget and funding…the adequacy of staffing levels…and any skills shortages faced”. In doing so, it will concentrate the minds of senior management at Ofcom, although I have no doubt that those minds will be focused on these matters already. Perhaps they will give this priority, particularly in terms of forward planning, and they will think, “We’re okay at the moment, but are we going to require extra and additional capability in area a, y or z in the next couple of years.” It will also focus and concentrate the minds of Ministers and Parliament, ensuring that Ofcom has the resources and capability to achieve the tasks that we have given it.

We heard many lines of evidence from the expert witnesses. My hon. Friend the Member for Newcastle upon Tyne Central may refer to some of them in her contribution, and I do not want to undermine that. Professor Webb said:

“I doubt Ofcom has that capability at the moment. In principle, it could acquire it and hire people who have that expertise, but the need for secrecy in many of these areas is always going to mean that we are better off with one centre of excellence”.

Emily Taylor of Oxford Information Labs said:

“Ofcom is going to need to upskill. In reality, as Professor Webb has said, they are going to be reliant on expert advice from NCSC, at least in the medium term.”—[Official Report, Telecommunications (Security) Public Bill Committee, 19 January 2021; c. 79, Q95.]

The new clause is about assisting Ofcom to make an audit of what is available and ensuring that it is up to standard in terms of technological changes. It will also ensure that it is looking forward, in the midst of all the other responsibilities that Parliament is asking it to undertake, in order to maintain a level of skills and expertise that will enable it to undertake the snapshot reviews of current networks, as well as reviews of future provision and threats to the network. I hope that the new clause is self-explanatory and I am pleased to present it to the Committee.

Mr Kevan Jones (North Durham) (Lab): I would like to speak to new clause 7, which stands in my name. It is related to new clause 3, in the name of my hon. Friend the Member for City of Chester. As he has just said, Ofcom has had an expansion of its duties in the last few years and become a little bit like a Christmas tree with added responsibilities, but none of them will be as important for the nation’s future as this. That is not to decry any of the expertise or other duties that Ofcom has, but national security and the security of our national telecoms infrastructure, is a vital new task. I have said before that my concern about Ofcom centres on national security. That is why I have tabled amendments to the Bill. My fear is that Ofcom will not have the necessary expertise, although I am not suggesting that it cannot develop into a good regulatory body looking at security and our national telecoms infrastructure.

I tabled parliamentary questions on Ofcom’s budgets and headcounts, and I am glad to see that its budget and personnel have increased as its tasks have grown. That was not the case in 2010, when its budgets were subject to some quite savage cuts. My concern—I will call this my Robin Day approach—is that we have to future-proof Ofcom to ensure that the organisation not only has the budget but also has the personnel it needs. I do not want to suggest that the Minister would want to cut Ofcom’s budget at present, as it does important work. However, it is a regulator and perhaps does not have the clout of a Government Department, so any future Chancellor or Treasury looking for cuts disguised as efficiencies could see it as easy, low-hanging fruit.

Ensuring that the Secretary of State undertakes duties highlighting Ofcom’s efficiency puts a spotlight on the basis of considerations by future Administrations of any political persuasion. That will be important, not just in the early stages but as we continue. It may take a while for Ofcom to get up to speed, but I want to ensure that that continues. The obligation for the Secretary of State to report on Ofcom would at least give me comfort that first, it is being looked at and, secondly, that civil servants cannot in future just assume that an easy cut can be made but which might then impact on our national security.

I raised another subject with the head of Ofcom when she appeared before the Committee. I do not really want to rehearse the discussions again, but as the Bill progresses the Minister will have to give assurances on security, and try to demonstrate the close working relationship between Ofcom and the security services.

That will be important, as it will give credibility to the expectation that Ofcom can actually do the job that we have set out. If the Minister does that, it will reassure people who may not be convinced that Ofcom has the necessary expertise, and ensure that that close working relationship continues, not just now but in future, so that national security is at the centre of this.

There will always be a balance—as I said, we saw it in the National Security and Investment Bill—between wanting, quite rightly, to promote telecoms as a sector,
and national security. I fully very much on the side of national security being the important consideration, and we need to ensure that that is always the case. It is important that national security and intelligence agencies are able to influence these decisions, not just in respect of Ofcom but also in respect of Ministers in future.

Chi Onwurah: I support and second the comments and contributions of my hon. Friend the Member for the City of Chester (Christian Matheson) and of my right hon. Friend the Member for North Durham (Mr Kevan Jones), who tabled new clauses 3 and 7. I would also like to congratulate the Committee on having made it through, as it were, the thickets of the Bill as it stands to the sunlit uplands of our new clauses, which are designed to improve it in a constructive and supportive way.

New clauses 3 and 7 both address the challenge of Ofcom’s resources. As Members of the Committee know, I joined Ofcom in 2004. I know that we are not allowed to use props in debates in the Chamber, but the Communications Act 2003, which I am holding in my hand, is the Act with which the Bill is concerned. The changes that the Bill makes are mainly adding to that Act.

2.30 pm

When I joined Ofcom in 2004, the Act was about half the size it is now. I am grateful to the Vote Office for printing and binding the enlarged Act which, as I said, is about double the size it was when I joined Ofcom. That is because—my hon. Friend the Member for City of Chester alluded to this—Ofcom has acquired responsibility for critical national infrastructure, the BBC, the Post Office. What is not yet reflected in the Act is Ofcom’s soon-to-be-acquired responsibility for the entirety of our online existence, as reflected in an online safety Bill, which has yet to make its appearance but has the absolute commitment of the Minister’s Department.

This latest expansion of Ofcom’s duties will necessarily add a strain not only to its budget—I shall come on to address that briefly—but, most importantly, to its resources, as was referred to by my right hon. and hon. Friends. In January this year, a colleague of the Minister stated that Ofcom will have the resources that it needs to do its job. If that is the case, may I ask what objection the Minister has to Ofcom reporting to Parliament on the state of its resources, particularly as those resources will be very hard to come by. My right hon. and hon. Friends emphasised the fact that Ofcom lacks experience in national security measures, and that expansion of duties will require the recruitment of people with the required level of security clearance and experience.

We heard in the evidence sessions that that might be a challenge. Dr Alexi Drew said:

“I think what needs to be considered in that question is the type of resources that will be the hardest for Ofcom to acquire. I frankly believe it is not necessarily technology; I believe it is actually personnel. The edge that is given to companies that have already been mentioned in your hearings today—Google, Microsoft, Facebook et al—is not necessarily in the technology, but in those who design the technology. Those people are hard to come by at the level that we require them at. They are also very hard to keep, because once they reach that level of acumen and they have Google, Facebook or Amazon on their CV, they can pretty much choose where they go and, often, how much they ask for in the process.”—[Official Report, Telecommunications (Security) Public Bill Committee, 19 January 2021; c. 84, Q82.]

I just want to reiterate that the Bill must be forward-looking on security challenges. While we the existing architecture of our telecoms networks requires skills in certain aspects of technology—radio frequencies and so on—as the architecture moves more and more into the cloud and the software domain, those skills and CVs are going to be all the more scarce and difficult to obtain.

We also heard from Dr Drew that she was not sure whether Ofcom had the capacity to take on the sheer volume of work that was likely to be created. Finally, we heard evidence from Lindsey Fussell, Ofcom’s group director for network and communications:

“In relation to Ofcom’s costs, Ofcom is funded in two ways: first, by a levy on the sectors and companies that it regulates and, secondly, through the collection of fees, primarily from our spectrum duties. Our overall funding is obviously agreed by our board but also subject to a cap agreed with Government... We are currently in discussion with the Treasury about the exact technicalities and which of those routes will be used to fund this, but it will be in line with Ofcom’s normal funding arrangements.”—[Official Report, Telecommunications (Security) Public Bill Committee, 19 January 2021; c. 97, Q131.]

Mr Jones: This is about resources for Ofcom as a whole, but there will also be debate within Ofcom about how its resources are spent. Without any ring-fenced moneys for security, it is my hon. Friend concerned, like me, that not only the external control of the budget but that debate internally might compromise security.

Chi Onwurah: My right hon. Friend makes an excellent point. This debate is important for the Bill and important for our new clauses. It is also important that the Minister clarifies what the duties and priorities of Ofcom should be. Having worked for Ofcom at a different point in its history, I can tell hon. Members that when there is, say, a complaint about the behaviour of somebody in the “Big Brother” household that is hitting all the headlines in all the newspapers, that attracts the sudden concentration of resource—unnecessarily, one might argue. There needs to be a counterweight, if you like, to those headline-driven resourcing bottlenecks, which would be either ring-fencing or reporting on how resource is being used to support national security.

All Opposition Members are clear that national security must be the first priority of Government, and therefore the first priority of Ofcom. This is all the more relevant as I pick up the Communications Act 2003, in all its weightiness, where we find the general duties of Ofcom in section 3:

“It shall be the principal duty of OFCOM, in carrying out their functions—(a) to further the interests of citizens in relation to communications matters; and (b) to further the interests of consumers in relevant markets, where appropriate by promoting competition.”

Security is not mentioned—national security or telecommunications security. During the evidence sessions, the argument was made, although I forget by whom, that security was a necessary part of furthering the interests of citizens in relation to communication matters. That is possibly true, but I still think this important issue would be improved by clarity.

As we know, there is a significant pressure on Ofcom’s resources, which changes week by week and month by month depending on what the issues are in the many and increasing domains in which it operates. If these principal duties of Ofcom do not reflect our national security, the
concern is that having no direct reporting mechanism to Parliament could mean these resources being used opaque, with no direct requirement to prioritise national security. I hope the Minister will agree that new clauses 3 and 7 solve a problem the Bill will have in practice. I hope that if he will not agree to the clauses as they stand, he will agree to consider how Ofcom’s prioritisation of national security interests can be made clearer.

Mr Jones: As I have said before, I am not a great fan of arm’s length regulators, because it is a way of Government Departments and Ministers off-loading their responsibilities. Given how my hon. Friend has described the Bill, the way this is going means that Ofcom will be larger than DCMS in the future. Does she share my concern about accountability if things go wrong? It is a good get-out for the Government to be able to hide behind Ofcom, rather than Ministers taking direct responsibility.

Chi Onwurah: As always, my right hon. Friend raises a good point. Having worked for a quango, I had clear insight into the line between independence and dependence, and into the importance of the political will of the Government, regardless of supposed independence. Equally, I saw how any regulator or supposedly independent organisation can be used as a shield for Ministers who do not want to take responsibility.

My right hon. Friend also raises a good point about the hollowing out of capacity in Government Departments. A consequence of 10 years of austerity and cuts is that DCMS and other Departments do not have the capability, capacity or resources that they previously might have enjoyed. I will point out to the Minister the example of the Government’s misinformation unit. It has no full-time employees and is supposed to exist using resources already in the Department—for something as critical now, with the vaccine roll-out, as disinformation.

My right hon. Friend is right to emphasise that given the relationship between the Government and Ofcom, which is an independent regulator, and given the increase in responsibilities that the Bill represents at a time when other responsibilities are also being added to Ofcom, the Minister cannot have it both ways. He cannot have no visibility when it comes to Ofcom’s resources and capacity while giving it yet more responsibility. In fact, this seems to be responsibility without accountability. I hope the Minister will take on board the suggestions in new clauses 3 and 7.

Matt Warman: I thank the hon. Lady for her contributions. To address her central point, it would not be possible for Ofcom to meet the duties Government have tasked it with without addressing the foundational issue of security. It is important that we bear in mind that this is not an exhaustive list, but security will always be a foundational point.

The new clauses would require the Secretary of State to lay a report before Parliament within 12 months of Royal Assent. New clause 3 would require Ofcom to publish an annual report on the adequacy of its budget, resourcing and staffing levels in particular.

As the Committee is aware, the Bill gives Ofcom significant new responsibilities. Ofcom’s budget is approved by its independent board and must be within a limit set by the Government. Clearly, given the enhanced security role that Ofcom will undertake, it will need to increase its resources and skills to meet these new demands. As such, the budget limit set by the Government will be adjusted to allow Ofcom to carry out its new functions effectively. This is of a piece with the direction of travel we are going in. In 2012, Ofcom had 735 employees. Last year, it had 937 employees, so as its remit has expanded, so has its headcount. That will continue to be reflected in the level of resourcing that it will be given.

2.45 pm

Christian Matheson: Budget allocations can go down as well as up and there might be a future Government who are not quite as generous as past Governments have been. What guarantee can the Minister offer us that without some kind of reporting, such as that we propose, Ofcom’s budget will not be frozen or, indeed, reduced?

Matt Warman: Ultimately, a mechanism already exists by which Parliament is able to scrutinise Ofcom’s resourcing. Ofcom is required under the Office of Communications Act 2002 to publish an annual report on its financial position and other relevant matters. That report, which is published every March—I am sure the hon. Gentleman is waiting with bated breath for the next one—includes detail on Ofcom’s strategic priorities as well as its finances, and details about issues such as its hiring policies.

Mr Jones: I am intrigued. The Minister says Ofcom already has over 900 people, and it is obviously going to have to grow. How big is DCMS? We basically have a mini-Department here.

Matt Warman: The right hon. Gentleman asks me a question that I may be able to answer in a moment, depending on a number of factors. As for the thrust of his question, Ofcom is ultimately a serious regulator that has the resourcing to do a serious job. The right hon. Gentleman would be criticising us if it had fewer people, so he cannot have his cake and eat it by criticising the fact it has enough to do the job—but I think he is going to have a go.

Mr Jones: Quite the opposite. This just reinforces my point about quangos. If we reach a situation where quangos are bigger than the sponsoring Department it is perhaps best to keep things in-house rather than having arm’s length quangos and the nonsense behind which we hide in this country about so-called independence.

Matt Warman: The reality is that the relationship between Government Departments and regulators is very often incredibly close, but independence is an important part of regulation. Although the right hon. Gentleman makes a reasonable point about the optimal size for in-house expertise versus external expertise, it is getting the balance right between Ofcom, the National Cyber Security Centre and DCMS that this Government and the reporting measures we already have are fundamentally committed to providing.

The right hon. Gentleman talked about Ofcom’s resourcing. Ofcom will not be making decisions on national security matters, as we have said repeatedly, but it will to be responsible for the regulation around these issues. As the right hon. Gentleman said, the Intelligence and Security Committee has shown great interest in how Ofcom is preparing for its new role.
As for the point about disclosure and resources, I would be happy to write to the ISC to provide further details in the appropriate forum about Ofcom resourcing and security arrangements. This could include information that cannot be provided publicly, including information about staffing, IT arrangements and security clearances of the sort that we have discussed. I hope that Opposition Members understand that that is the appropriate forum to provide reassurance and to satisfy the legitimate requirements of public scrutiny on this issue.

Chi Onwurah rose—

Christian Matheson rose—

Matt Warman: How to choose?

Christian Matheson: My hon. Friend is the shadow Minister.

Matt Warman: I give way to the hon. Lady.

Chi Onwurah: I thank the Minister for giving way and for the tone of his response to the different points we made. I will leave the reassurance about writing to the ISC to my right hon. Friend the Member for North Durham. Does the Minister recognise that that does not address the issue of Ofcom’s resources and reporting more generally, particularly lower down the pipeline, when it comes to national security? We have emphasised again and again the breadth of powers. The Minister has said that Ofcom will have the discretion, for example, to require an audit of all operators’ equipment—an asset register audit. It will take significant resource to understand the audit when it comes back. There are significant resource requirements involved that do not necessarily require security clearance but are nevertheless essential to effective security, and the Minister does not really seem to be offering reassurance on those.

Matt Warman: I would say that there is a sensible place to put some of that information, which is the communication to the ISC that I have offered, and there is a sensible place to put other information, which is the annual reporting that already exists. Hopefully the hon. Lady can find some comfort in the fact that both the information that cannot be shared publicly and the information that can will be subject to an appropriate level of parliamentary and public scrutiny.

Christian Matheson: I simply want to welcome the Minister’s comments, and the fact that he has recognised that the Intelligence and Security Committee is the appropriate place to discuss these matters, which, of course, cuts across other clauses that the Committee has already considered. He might bear that in mind on Report.

Matt Warman: I thank the hon. Gentleman for that intervention. I hope that now that I have given those various reassurances, hon. Members are appropriately comforted.

Everyone is waiting for the headcount of DCMS. I am assured that it is 1,304 people, some 300 more than that of Ofcom. I do not know whether that makes the right hon. Member for North Durham happier or more sad.

Mr Jones: According to the website that I have looked at, the figure is 1,170, so it has obviously increased slightly. Still, it makes Ofcom with its new responsibilities nearly as big as, if not bigger than, the sponsoring Department.

Matt Warman: We can discuss the optimal sizes of quangos and Departments outside this room. However, the right hon. Gentleman is obviously right that Government Departments and regulators need the resources they require to do their job properly. I hope that by describing the various mechanisms I have provided hon. Members with the reassurances they need to withdraw the new clause.

Christian Matheson: First, I owe you an apology, Mr McCabe; so keen was I to crack on with the consideration of the Bill that I did not say how great a pleasure it was to serve yet again under your chairmanship. I should have done so at the outset and I apologise.

I am grateful to the Minister for his response. I am looking to the shadow Minister, my hon. Friend the Member for Newcastle upon Tyne Central, for a little guidance. It could well be that we might want to serve a little bit longer under your chairmanship, Mr McCabe, by testing the views of the Committee on new clause 3, if we may.

Question put. That the clause be read a Second time.

The Committee divided: Ayes 3, Noes 10.

Division No. 2]

AYES

Jones, rh Mr Kevan

Matheson, Christian

Onwurah, Chi

NOES

Britcliffe, Sara

Cates, Miriam

Caffield, Maria

Johnston, David

Lamont, John

Richardson, Angela

Russell, Dean

Sunderland, James

Warman, Matt

Wild, James

Question accordingly negatived.

New Clause 5

Reporting to Parliament No.2

(1) The Communications Act 2003 is amended as follows.

(2) After section 105Z29 insert—

"105Z30 Reporting to Parliament

(1) The Secretary of State must produce an annual report for the Intelligence and Security Committee of Parliament concerning—

(a) designated vendor directions made under section 105Z1; and

(b) designation notices issued under section 105Z8.

(2) The report must contain an assessment of the national security risks underpinning the directions and notices made under those sections."
(3) Ofcom must produce an annual report for the Intelligence and Security Committee of Parliament—

(a) assessing the adequacy of existing security measures within UK public electronic communication networks and services; and

(b) assessing future threats to the security of those networks and services.”—(Chi Onwurah.)

This new clause introduces a requirement for the Secretary of State to report to Parliament on the impact of vendor designation on national security risks. It also requires Ofcom to produce a forward-looking report on future threats to network security and undertake an assessment of the adequacy of existing measures.

Brought up, and read the First time.

Chi Onwurah: I beg to move, That the clause be read a Second time.

New clause 5 is similar in its intent to amendment 19, which we discussed earlier. As with all our amendments and new clauses, it is designed to improve the Bill through ensuring greater scrutiny, focus, transparency and security for the diversification of our network. It would introduce a requirement for the Secretary of State to report to Parliament on the impact of vendor designation on national security risks. It would also require Ofcom to produce a forward-looking report on future threats to network security and undertake an assessment of the adequacy of existing measures.

At the centre of the new clause is a wish to reflect the importance of national security not as a snapshot in time but as something that needs to be continually monitored, considered and assessed for future impact.

The new clause would require the Secretary of State to produce an annual report for the Intelligence and Security Committee of Parliament. That would ensure that the report can be comprehensive with regard to security issues that might not be appropriate to share with the public or the Digital, Culture, Media and Sport Committee. The new clause would require that the annual report should concern designated vendor directions made under new section 105Z1 and designation notices issued under new section 105Z8. The report must contain an assessment of the national security risks underpinning the directions and notices made under those sections. That is for the Secretary of State to report.

In addition, Ofcom would be required to produce an annual report for the Intelligence and Security Committee to assess the adequacy of existing security measures within the UK public electronic communication network and services. Critically, it should assess future threats to the security of the networks.

As we have discussed, the Bill gives major sweeping powers to the Secretary of State and Ofcom. We want to ensure that they are proportionate and accountable. Like amendments 5, 9, 10, 20 and 22 to 25, the new clause seeks to address issues of oversight, scrutiny and transparency. We have taken some heart from the Minister’s recognition in the previous debate of the unique role of the Intelligence and Security Committee in assessing security implications, in that case resourcing for Ofcom. The new clause would ensure a focused accountability to Parliament, via the Intelligence and Security Committee, of the notices, designated vendor directions and designation notices made under the provisions of the Bill, and the existing security measures and future threats.

As aspects of this have already been debated, I want to focus on assessing future threats to the security of the network and services. The Minister might say that that is part of the responsibility of the National Cyber Security Centre. What we see is a massive transformation of how the UK addresses security in telecommunication networks, for very good reasons, and a significant amount of the responsibility falls on Ofcom.

3 pm

The Minister has written to us about how Ofcom and the NCSC will be expected to work effectively together, and we welcome that, but it is also important that Ofcom demonstrates that it has the resources and skills to assess forward-looking threats to the security of our networks. If the measures in the Bill are to be effective for the next five or 10 years, there must be adequate accountability and assessment of future threats, so that we do not find ourselves once more in the position that we are in now because there has been a wholesale change to the networks and Parliament has not been able to assess the implications.

To support the concerns that we have raised, it is worth remembering that Andrea Donà, UK head of networks at Vodafone, said:

“Reviewing the legislation at regular intervals to assess its efficacy in the face of new technological challenges, and also in the light of new strategic aims by Government and that constant review involving the industry, will be very welcome.”—[Official Report, Telecommunications (Security) Public Bill Committee, 14 January 2021; c. 8, Q3.]

Dr Alexi Drew of the Centre for Science and Security Studies, talked about making it as hard as possible for attackers to get access, saying:

“…We should be making sure that there is as much oversight and understanding as is possible of where our supply chains go, the standards that they should meet, and whether those standards are being met…this Bill goes some way towards that. I would argue that it needs to be continually updated, checked and maintained. This is not a one-off: times change, and the internet changes faster. Those would pretty much be my recommendations.”—[Official Report, Telecommunications (Security) Public Bill Committee, 19 January 2021; c. 82, Q100.]

Dr Louise Bennett argued that it was incumbent on the Government to have funding in place if vendor designations affected particular suppliers, because it could have the opposite effect to the one intended as small suppliers might not have

“the resources of skills, time or money”—[Official Report, Telecommunications (Security) Public Bill Committee, 14 January 2021; c. 52, Q67.] to respond. Reporting to the Intelligence and Security Committee on the impact of vendor designation notices as well as on forward-looking threats would be provide an opportunity to take account of the impact on particular sectors and on small suppliers, for example. Furthermore, we have talked previously about issues of confidentiality in the sector and concerns about changes and evolution in network architecture or the performance and predominance of one particular supplier, and the increasing influence that a supplier might have, which might not be appropriate to be reported in a public domain but would very much gain from being reported in a secure measure.

I know that the Minister is reluctant to add to the duties of Ofcom. He will probably say that Ofcom could do this if it wanted to. I reiterate that Ofcom has a lot of things that it could or should do, and would do, but it does not have as a principal duty ensuring the forward-looking security of our networks. The new
clause will ensure that that is regularly considered by Ofcom and that Parliament can exercise adequate and effective scrutiny. It would also contribute greatly to the ability of Ofcom and the National Cyber Security Centre to work together effectively, as they would to produce such a report. I hope the Minister will support the provisions of the new clause.

Matt Warman: As the hon. Lady said, we have addressed various issues relating to the new clause in previous debates. It is important to stress that Ofcom has the resources that it needs. She talked about its ability to face the future, but in our evidence sessions, we talked to Simon Saunders, the director of emerging technology. I know she does not wish to suggest that Ofcom does not do this already, but demonstrably it is already proactively engaged in horizon scanning.

Chi Onwurah: Speaking as someone who was head of technology at Ofcom, I am aware that it engages in horizon scanning. I am sure the Minister will come on to this, but while there might be horizon scanning to understand how markets evolve and what level of competition may be seen in new markets in the future, the new clause deals specifically with horizon scanning for security and security threats. I am sure the Minister will focus on that.

Matt Warman: It is important to say that we have amended section 3 of the Communications Act 2003, to which the hon. Lady alluded, so that Ofcom must have regard to the desirability of ensuring the security and availability of networks and services, so that should be incorporated into the horizon scanning work.

Chi Onwurah: This is an important point. I do not think the 2003 Act has been amended, since I had it reprinted a week ago. We were talking about the principal duties. Under section 3, Ofcom has about two and a half pages of duties that it needs to carry out, but only two principal duties. Those principal duties do not mention security.

Matt Warman: The hon. Lady is right, but as of 31 December 2020, section 3(4) states:

“OFCOM must also have regard, in performing those duties, to such of the following as appear to them to be relevant in the circumstances... the desirability of ensuring the security and availability of public electronic communications networks and public electronic communication services”.

It is absolutely there, but I fear we are getting into a somewhat semantic argument.

Chi Onwurah: The Minister is generous in supporting this back and forth in debate. I will close by pointing out that the duty to which he refers is one of 13 duties, so it can hardly be considered a priority. To put it more fairly, to ensure that it is a principal priority, it would need to be elevated.

Matt Warman: I think an organisation of 937 people can cope with 13 priorities. On one level, however the hon. Lady makes a reasonable point, and it is not one that we disagree with. Security has to be absolutely central to the work that Ofcom will do.

I will not restate the points I have made about how seriously we take the Intelligence and Security Committee and how seriously we will continue to take it. We will continue to write to the Committee on topics of interest as they arise and we are happy to continue to co-operate in the way that I have done; however, as I said in the debate on amendment 9, the primary focus of the ISC is to oversee the work of the security and intelligence agencies, and its remit is defined in the Justice and Security Act 2013. Amending the Bill to require regular reporting to the ISC, as proposed by the new clause, would risk the statutory basis of the ISC being set out across a range of different pieces of legislation.

Mr Jones: Will the Minister give way?

Matt Warman: Earlier, the right hon. Gentleman was suggesting that it was the memorandum of understanding that he would like to see amended. Now he seems to be suggesting that we should insert the new clause, which will not change the memorandum of understanding.

Mr Jones: No, I said in an earlier contribution that if it were done by the memorandum of understanding, I would be quite happy. I know the Minister is limited in the number of civil servants he has beneath him compared with Ofcom, but will he go away and read the Justice and Security Act 2013? It talks about Departments, but it also talks about intelligence more broadly, which is covered by the memorandum of understanding. I do not know why he is pushing back on this issue; it may be because of the Cabinet Office, which has more civil servants than he has. I suggest that we will win this one eventually.

Matt Warman: That may well be the case, but the right hon. Gentleman is not going to win it here—that is the important point to make. It is right not to try to address this issue in the new clause, but the Government will continue to take very seriously the work of the ISC, as he would expect.

Additionally, the new clause is designed to require Ofcom to provide annual reports to the ISC, which would, as the right hon. Gentleman knows, be particularly unusual in the context of the work of the Committee, as Ofcom will not be making judgments about the interests of national security under the Bill, or as part of its wider function. Ofcom’s role as regulator seems not to be something that comes under the purview of the ISC, even if I understand the broader point. As I said earlier, however, the NCSC is very much under the purview of the ISC, and there are plenty of opportunities for the Committee to interrogate the work of that excellent agency. I am sure the Committee will continue to take up such opportunities with vigour, but as I have said before, it would not be right to seek to reframe the remit of the ISC through the new clause. I ask the Opposition to withdraw it.

Chi Onwurah: I thank the Minister for his comments and for engaging so readily in debate. I have to say that we feel very strongly about the new clause, both for parliamentary scrutiny and for ensuring that Ofcom is looking forward and assessing future threats. With bated breath, I wish to test the will of the Committee on the new clause.

Question put, That the clause be read a Second time.
The Committee divided: Ayes 3, Noes 10.

Division No. 3]

AYES
Jones, rh Mr Kevan
Matheson, Christian

NOES
Britcliffe, Sara
Cates, Miriam
Caulfield, Maria
Johnston, David
Lamont, John

Question accordingly negatived.

New Clause 6

NETWORK DIVERSIFICATION (NO. 2)

'(1) The Communications Act 2003 is amended as follows.
(2) After section 105Z2 insert—
 "105Z30 Network diversification
 (1) The Secretary of State must lay before Parliament an annual report on the impact of progress of the diversification of the telecommunications supply chain on the security of public electronic communications networks and services.
 (2) The report required by subsection (1) must include an assessment of the effect on the security of those networks and services—
 (a) progress in network diversification set against the most recent telecommunications diversification strategy presented to Parliament by the Secretary of State;
 (b) likely changes in ownership or trading position of existing market players;
 (c) new areas of market consolidation and diversification risk including the cloud computing sector;
 (d) measures taken to implement the most recent telecommunications diversification strategy presented to Parliament by the Secretary of State;
 (e) the public funding which is available for telecommunications diversification.

(3) A Minister of the Crown must, not later than two months after a report has been laid before Parliament under this section, make a motion in the House of Commons in relation to the report.”’ (Chi Onwurah.)

This new clause requires the Secretary of State to report on the impact of the Government’s diversification strategy as it relates to the security of telecommunications networks and services, and to allow for a debate in the House of Commons on the report.

Brought up, and read the First time.

3.15 pm

Chi Onwurah: I beg to move, that the clause be read a Second time.

It is with some sadness that I come to the last new clause we have to present—[Interruption.] I see that causes some hilarity in the Committee; I am sure that is just nervous laughter and everyone shares my dismay that the focus on telecommunications that the Committee has ably exhibited for the last few sittings will soon come to an end. Our consideration in some detail of the importance and implications of our telecoms network’s security must conclude, but I am pleased that we end on this new clause, which sums up one of the key themes we have focused on throughout our discussions: the importance of the diversification strategy.

Many amendments tabled by the Opposition reflect our concern that the Bill claims to seek the security of our telecommunications networks and yet does not mention once the diversification strategy. We are moving the new clause to put that right. We support the Bill and the Government’s aims in the Bill. We believe it is right to remove high-risk vendors from the UK’s networks and to take the measures in the Bill that will ensure that the Government will be able to designate vendors and require telecoms operators to comply with security requirements. However, those steps must go hand in hand with credible measures to diversify the supply chain, and that must be subject to parliamentary scrutiny.

As I said, the Bill as drafted fails to mention the Government’s diversification strategy and chooses to ignore the impact that the new powers afforded to the Secretary of State and Ofcom will have on supply chain diversity. The Minister recognises that they will reduce diversity, yet there is no reference to the steps that will be taken to diversify the supply chain. The new clause would require the Secretary of State to report on the Government’s diversification strategy’s impact as it relates to the security of telecommunications networks and services.

The Opposition have argued throughout our deliberations that the sweeping powers afforded to the Secretary of State and Ofcom by the Bill must be put under proportionate scrutiny, and the new clause would do that. It would bring about a debate in the House on the findings of the Secretary of State’s diversification strategy report and require a ministerial response no more than two months after the report’s publication. The new clause would therefore provide accountability for the diversification strategy’s progress and lead to real action, not just talk.

It has been said that “it is essential that we create a more diverse and competitive supply base for telecoms networks” because reliance on two providers creates “an intolerable resilience risk”. Those are not my words, but the words of the Secretary of State. Members from across the House agree that we cannot have a robust and secure network with only two service providers. That is something we were repeatedly told in the evidence sessions. The chief technology officer of BT Group, the director of emerging technology at Ofcom and the former head of cyber-security at GCHQ think so, and even the Secretary of State thinks so, yet the lack of link between the diversification strategy implementation and the security of our networks is ongoing cause for concern. Now we have the chance to take action, and I am glad to offer the Minister the opportunity to put this right.

This is not new information. The dependence of our telecoms networks on diversifying the supply chain was set out in the 2019 telecoms supply chain report. A leak from that report caused a Cabinet resignation, so important was it considered to be. Unfortunately, in the intervening year and a half, the Government have failed to act, refusing to take the necessary steps to ensure the diversification of our national supply chain, leaving us at real risk of being short-changed on national security. I emphasise, once again, that we place national security at the heart of everything that we do in this Committee.

The UK defence industry seeks to encourage, support and create markets for UK small and medium-sized enterprises, supporting the very best in innovation and
helping innovative small and medium-sized enterprises to grow. We would like to see the UK’s telecommunications industry do likewise, to ensure a sovereign security capability. We want the Bill and the diversification strategy to create significant opportunities for UK businesses, linking them to global supply chains.

I welcome the Government’s diversification strategy. After all, I have been calling for a strategy to grow and diversify our telecoms sector for a long time—even before I came to this House. Although the Government have been talking about such a strategy for some time—there was an awful lot of talk about a diversification strategy and bigging it up before it was published—as is often the case with this Government, the strategy that was published was a bit of a disappointment. It lacked the clear commitment and funding that one would expect to find in any effective strategy.

The £250 million committed by the Government over five years came with little detail on how it would be spent. I have now had assurance that the funding is focused on integration and testing facilities, which are necessary, but there is no emphasis on supporting research and development, and particularly supporting our start-ups in the telecommunications sector. In the evidence sessions, Mike Fake of Lumenisity highlighted that the first year of the £250 million diversification funding was equivalent to only 10% of BT’s annual research and development budget. This is not the bold action of a Government committed to network diversification and our telecommunications security.

The diversification strategy declares itself “a clear and ambitious plan to grow our telecoms supply chain while ensuring it is resilient to future trends and threats.” That is a bold ambition. It says it will do that by focusing on three main areas:

“Supporting incumbent suppliers to ensure their resilience and ability to supply the market in the near term, while supporting their transition into the emerging market structure; attracting new suppliers into the UK market to build resilience and competition, prioritising deployments that are in line with our longer term vision; accelerating open-interface solutions and deployment so that we are not reliant on any single vendor and begin to realise our long term vision for a more open and innovative market.”

These are all highly laudable. They are not easy. I recognise the challenge that the Government face. As we discussed in the evidence sessions, this comes after decades of neglect of sovereign capability, not only in the UK but by other countries, which is why we find ourselves with only two vendors, both from Scandinavian countries, and no UK, US or other European capability.

We have heard just how difficult this challenge will be. Will the Minister tell me how we can possibly achieve that bold ambition if we fail to monitor the impact of the strategy? We need an annual report on the progress made by the diversification strategy, so that we can apply appropriate parliamentary scrutiny. After all, the strategy commits the Government to regular reports on progress, which is what the new clause asks for, while adding a focus on the diversification strategy’s impact on our national security. That is what it is all about. The Secretary of State tells us that the Government are implementing one of the toughest telecommunications security regimes in the world, but why is there to be no scrutiny applied to this key part of the regime?

When I asked the Minister in parliamentary questions why the diversification taskforce was not diverse in terms of geography—it includes no one from either of the devolved nations, or discipline, harvesting on it no equipment supply chain expertise, I was told that geography did not matter, and that the taskforce was focusing on cyber-security skills. To be fair, the Minister did say that Ian Livingston, the chair, was Scottish, but I think he will acknowledge that he has not lived in Scotland for some time. Geography does matter. We need to build up concentrations of skills and expertise—clusters. Cyber-security is very important, but focusing on it suggests that we are not serious about developing sovereign capability in other very important areas.

We are agreed that diversification is essential, and I hope that we are agreed that that should include UK capability. We also agree that it is challenging. How do we do it? In an evidence session, Professor Webb said: “If I wanted to diversify, I would instruct the telecoms operators to diversify. I would not try and pull the levers one step removed. I would say to the telecoms operators, either with a carrot or a stick, ‘You must diversify. If you have x number of vendors in your network, I will give you £x million as a carrot.’ The stick might be some kind of licence condition that said, ‘In order to meet your licence, you have to have at least x number of vendors in your network.”’—[Official Report, Telecommunications (Security) Public Bill Committee, 14 January 2021; c. 38, Q43.]

We also heard from Chris Jackson, who said: “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.”—[Official Report, Telecommunications (Security) Public Bill Committee, 14 January 2021; c. 38, Q43.]

The Government have chosen not to do that. They have chosen to focus on big sticks for security, as set out in the Bill, such as designations, enforcements and fines of up to 10% of turnover, but they have left diversification very much to the market, providing it with a sweetener of £250 million over five years. Surely we have a right—indeed a duty—to monitor how and whether that is successful.

We heard in the evidence sessions that we have significant national promise in terms of capability. Dr Andy Sellars, the strategic development director for the Compound Semiconductor Applications Catapult, said: “In the UK we have something like 5,000 companies that design and manufacture electronic systems. Something like 600 of them are involved in telecoms. I am not suggesting that all of those 600 become equal players. That would be a crazy scenario. But there are certainly some parts of the telecom network where the UK is pre-eminent. There are some backhaul and fibre technologies that we are very good at. As we deploy 5G into rural communities, that is likely to require low Earth orbit satellites; we are very good at satellite communications.”—[Official Report, Telecommunications (Security) Public Bill Committee, Tuesday 19 January 2021; c. 109, Q142.]

3.30 pm

I will give the Minister a specific example of both the opportunity and the challenge, which I hope he will respond to equally specifically. I am very pleased to say that the example comes from my constituency of Newcastle upon Tyne Central: INEX, which is leading the UK’s drive for a sovereign radio frequency and communications gallium nitride semiconductor—an important semiconductor capability for telecommunications.
INEX is currently working with many of the organisations in the north-east communications cluster, including aXenic, Evince, VIPER RF, II-VI, Newcastle University and Durham University. Further afield, it works with companies and organisations in south Wales, Glasgow, Cambridge and Edinburgh, deploying compound semiconductors for RF and microwave applications, and working on the microfabrication of devices for telecommunications hardware. The biggest challenge will be accessing the capital investment to buy the process and manufacturing equipment to deliver at-scale commercial products. That is a fundamental barrier to entry for many small and medium-sized enterprises in the sector. I ask the Minister what specifically he is doing to redress that. He will say that the diversification strategy suggests that there will be funding for testing and integration, but we are specifically looking at the challenge regarding capital investment.

If that group of companies is to be an intrinsic part of telecommunications deployment, we must ensure that it can reach into and benefit from the competitive pull of tier 1 labs and access the global telecommunications industry. I strongly believe that although direct procurement of critical subsystems, cyber-certification and sponsoring the UK’s attendance on standards bodies is beneficial—I will talk a bit about that—for truly secure telecommunications, the UK’s sovereign businesses, both hardware and software, need to be embedded in the global supply chain from which telecoms infrastructure is built.

The Bill needs to ensure that the UK is an embedded development partner, rather than simply a taker of technology. I am afraid that right now the Bill simply tries to ensure that we are a taker of technology. During the evidence sessions, we heard repeatedly of the importance of standards from numerous sources. Emily Taylor, the chief executive officer of Oxford Information Labs, heralded the exciting opportunities presented by interoperable standards, and the impact that they could have on prevention of vendor blocking. The diversification strategy recognises that too, stating that standards “play a critical role in determining the barriers to entry for new suppliers and establishing principles such as open interfaces and interoperability”, but the Bill gives no requirement for reporting on the progress of standards, and no indication of how our involvement in standards, which is necessary for diversification, will be achieved.

Emily Taylor also said:

“The ITU is headed by a Chinese national, and of 11 working groups within the ITU’s Telecommunication Standardisation Sector ...China has a chair or vice-chair in 10, and a total of 25 positions at chair or vice-chair”—[Official Report, Telecommunications (Strategy) Public Bill Committee, Tuesday 19 January 2021; c. 71, Q82].

Clearly there is a huge challenge in increasing UK participation in the standards necessary for telecommunications security, but how are we to see the progress that I am sure the Minister envisages if we do not have a report on the progress of the diversification strategy and its implications for security?

On standards, Professor William Webb told us:

“The UK Government themselves could not really have an influence, and nor could a university or any other organisation like that, not unless they spent inordinate amounts of money and hired a lot of people to write a lot of papers. There needs to be a concerted global or western European effort, or some kind of larger scale activity that can help the larger companies with the resources and expertise and the standards bodies to step up their efforts”—[Official Report, Telecommunications (Security) Public Bill Committee, 19 January 2021; c. 72, Q83]

yet we see no reflection of that in the Bill.

The impact that standards can have on vendor supply chain diversity is reflected in the diversification taskforce and the diversification strategy, which put a lot of emphasis on open RAN. We had much discussion in the evidence sessions about the maturity or otherwise of open RAN. The Government seem to have placed open RAN technology at the centre of their strategy to diversify 5G hardware, and aim to see live 5G open RAN in the UK this year. We support utilising open RAN, but evidence suggests that the technology may not be mature for another five to eight years, and Doug Brake stated that open RAN may not even be ready to be incorporated into 5G.

I acknowledge that through open RAN, the Government are thinking about how we will build the next generation of UK networks, but the UK currently has only two vendors. Our telecoms security is desperately in need of diversification and the development of a sovereign capability as soon as possible. We need an appropriate way of measuring that success.

We have also discussed the implications of changes in the architecture of telecommunications networks, and of moving control and services to the cloud. We have discussed the importance of forward-looking assessment, but I feel that a report to Parliament would ensure that those matters were kept very much at the forefront of the minds of Ofcom and the Department. It is worth mentioning that, on diversification and strategy, Dr Bennett suggested that a commissioner could help by “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”—[Official Report, Telecommunications (Security) Public Bill Committee, 14 January 2021; c. 49, Q61].

I will make a couple more points before I bring my remarks to a close. First, we heard concerns from a number of operators that they might be left in a contractual limbo, with designated vendor notices rendering them unable to buy from a supplier but contractually obligated to. If the Government will not address that now, they should at least allow us visibility, through a report, of the impact. Secondly, as discussed, neither the Bill nor the diversification strategy include incentives to diversify, but the Government could put in place incentives to innovate, which might have the same effect—requiring improving rates of spectral efficiency, and network SIP funds, such as the rural one, for example. Is the Minister considering that?
Finally, I think we can all agree that this should involve working with our allies. We heard in evidence that the new Administration in the United States, for example—we all congratulate the new President, Joe Biden—would be inclined to do that. Doug Braide said:

“What we have seen over the last several years in the United States is a variety of different agencies doing what they can to mitigate the risks. It is less a co-ordinated whole of Government approach in the US and more a disjointed and fragmented policy response across different agencies, so I am hopeful that under a Biden Administration we will see a much more co-ordinated effort and one that is more co-operative with allies.”—[Official Report, Telecommunications (Security) Public Bill Committee, 19 January 2021; c. 123, Q163.]

We also heard from Emily Taylor about the idea of a Five Eyes-type of collaboration among our allies. That idea has been kicking around for some time, yet we are forced to choose between technological progress and national security now and in future we must have an effective network supply chain diversification strategy, plan and implementation. New clause 6 would ensure that this vital aspect of our telecoms security is regularly reviewed and scrutinised, so that the UK is never again left with suppliers that have left us vulnerable and created the need for this Bill. We support the Bill, but it is clear that to protect our telecoms security, we must have the powers to do. We can set requirements on what the minimum standards might look like. For instance, NCSC guidance already says that two vendors should be available. The £250 million allocated for the first three years of that programme to support the diversification strategy is a hugely important part of it.

As we are already seeing in the increased use of open RAN, whether with Vodafone in Wales or the NeutrORAN project with the NEC, there is already significant progress. I think that demonstrates that the industry does regard this—whether the hon. Lady wants to call it as an incentive or a carrot—as something that is making things happen to a greater extent. The Government cannot legislate for the diversification of the market; that is something that we can incentivise and work with the market to do.

We can monitor the diversity of networks, as Ofcom has the powers to do. We can set requirements on what the minimum standards might look like. For instance, NCSC guidance already says that two vendors should be available. One of the number of suppliers that they have available.

It is important to reassure hon. Members that Ofcom will have the ability to collect information relating to the diversity of suppliers’ networks under section 135 of the Communications Act 2003, as we have discussed. It is important to clarify that, although greater diversity is critical in ensuring that we reduce our national dependence on a small number of suppliers, it is part of a broader approach to building security and resilience across the global supply chain that sits outside the Bill, important though it is. Diversification is an issue broader than the make-up of supply chains for UK providers alone, as the hon. Lady knows.

3.45 pm

At this stage, there is a limited number of suppliers in the global market—a smaller number that are capable of providing equipment suitable for the UK market. It is a global challenge that requires a global solution, which is why it is an integral part of the diversification strategy that the hon. Lady mentions. Our primary objective has to be to grow the supplier base and give operators more choice about the vendors that they use.

As we heard in evidence sessions, operators are equally committed to increasing diversity in UK networks. To achieve that, the Government will take forward the programme of works that the hon. Lady mentioned, with trials and testbeds for new suppliers and open RAN technology. We will ensure that telecoms standards are set in a way that promotes security and interoperability, and we will remove barriers to entry for new suppliers.

As the hon. Lady said, all that work is being informed by an independent taskforce looking at all options to drive increased market diversification. That includes incentives in forms other than those that I have already described, and the taskforce will be making recommendations in the coming months. It is also looking forward to identify areas where market consolidation might occur in the future, what can be done to offset those risks and where the UK can establish its sovereign capability.

The hon. Lady asks why there were not suppliers on the taskforce. If there had been suppliers directly on the taskforce, they would have been conflicted, but the taskforce has worked closely with suppliers because they are obviously very important. Indeed, Manevir, NEC and others who gave evidence are among those who have spoken to and worked closely with, as we have with Nokia, Ericsson and Samsung.

As the Government deliver our strategy across all these areas, we will be making announcements and providing regular updates as required. That approach, rather than the one the hon. Lady seeks through the new clause, will enable us to provide up-to-date and timely information on progress. With that, I hope she will be content that there is plenty in the diversification strategy that will deliver what she wants, but it is not an issue for the new clause.
Chi Onwurah: I thank the Minister for his comments; having spoken for so long myself, I was reluctant to interrupt him. I am pleased that he has clarified that the £250 million is over three years, as opposed to being over five years—I had not seen that before. That is welcome, and I anticipate further funding.

However, the Minister says that the Government cannot legislate for the diversification of the network. Why not? The Government can legislate to break up consolidation in other markets, and they have legislated to do so—for example, competition law does exactly that. We heard in evidence sessions from some who felt that diversification could be achieved only through direct intervention. He implies that I am arguing that diversification delivers telecoms security on its own, but I am not arguing that. I am arguing that it is necessary though not sufficient—clearly, other methods are needed.

The Minister suggests that diversification is one of many things that Ofcom can report on, if it so chooses. That is equally important, but let us be clear that it was the diversification of a supply chain that was the critical report—a report so important that the current Secretary of State for Education was forced to resign because of its leaking, which is why we are here today. The diversification of the supply chain is absolutely critical.

The Minister says that we heard from operators that were committed to diversification, but we also heard that there were real challenges in their commitment to diversification. We would not be where we are today if they were so committed to diversification of their supply chain. That is why there is a need for incentives and intervention. On that basis, it is important to test the will of the Committee on the new clause.

Question put, That the clause be read a Second time.

The Committee divided:

Ayes 3, Noes 10.

Division No. 4]

AYES
Jones, rh Mr Kevan
Matheson, Christian

NOES
Britcliffe, Sara
Cates, Miriam
Caulfield, Maria
Johnston, David
Lamont, John

Richardson, Angela
Russell, Dean
Sunderland, James
Warman, Matt
Wild, James

Question accordingly negatived.

The Chair: Mr Jones, new clause 7 has already been debated. Do you want to put it to a Division?

Mr Jones: No, Mr McCabe, it was a probing amendment. We debated some important issues around the accountability of Ofcom. Clearly, we are getting to a point where Ofcom has more staff than DCMS—perhaps, at some future date, Ofcom could take over the role of DCMS.

The Chair: I realise that this will come as a devastating blow to all of you, but the final question I must put is that—

Chi Onwurah: On a point of order, Mr McCabe. I put on the record my gratitude, and that of my right hon. Friend the Member for North Durham and my hon. Friend the Member for City of Chester, to you and your colleague, Mr Hollobone, for the way in which you have expertly chaired proceedings in the Committee. I also sincerely thank all House staff who have supported our work here, including those representing Hansard, and particularly the Clerks, who have been absolutely invaluable in setting out our desires to improve the Bill in clear and orderly amendments and new clauses.

I also thank all members of the Committee from both sides of the House. This detailed, technical Bill is critical for our national security, coming at a time of national crisis, when we are braving—all of us: staff and Members—a pandemic in order to be here. We have had an orderly and constructive debate.

Matt Warman: Further to that point of order, Mr McCabe. What fun we have had! It is a pleasure to come to this point in the Bill’s passage. I echo the hon. Lady’s thanks to the House staff and to yourself, Mr McCabe, and Mr Hollobone. I also reiterate her point that this is a crucial Bill—one that I am glad enjoys cross-party support. I look forward to debating its further stages in the House.

Bill, as amended, to be reported.

3.54 pm

Committee rose.
Written evidence reported to the House
TSB 11 Stefano Cantarelli, Chief Marketing Officer, Mavenir.