PARLIAMENTARY DEBATES

HOUSE OF COMMONS
OFFICIAL REPORT
GENERAL COMMITTEES

Public Bill Committee

TELECOMMUNICATIONS (SECURITY) BILL

Fifth Sitting

Thursday 21 January 2021

(Morning)

CONTENTS

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, soon 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.

11.45 am

In order to understand the diversification of the supply chain and how effectively, or not, it is proceeding, it is important that we consider the components of the supply chain, particularly identifying where they are a threat to our national security. Up until now, we have allowed our telecoms infrastructure to lack both security and resilience. Going forward, it is critical that we address both the lack of resilience and the lack of security, and that that assessment is made by those qualified to make it. That is not the Department as things stand, but our security services and the National Cyber Security Centre, in particular.

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.

[Mr Kevan Jones]

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 stifle 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.

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 in BEIS: it is in the Cabinet Office, which seems to have 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? That the Executive should 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

[Mr Kevan Jones]

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 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.

Christian Matheson: Perhaps my right hon. Friend will reflect on a third issue. The Committee cannot ask for information if it does not know that it exists. If there is no obligation to report orders to the Committee there is no way for it to know that they have been made, and that it needs to scrutinise them.

Mr Jones: There is, but to give a bit of background, we are quite tenacious on the Committee and if we do not get what we ask for we usually keep on and get it eventually. Some of the agencies are better than others, but overall the working relationship with GCHQ has always been a very good one. The amendment would help the Bill, but I think we will to and fro on this.

12.30 pm

At this stage, I am not minded to press the amendment to a vote, but as I said on Third Reading of the National Security and Investment Bill yesterday, and as the Minister admitted afterwards when I spoke to him privately, it is quite clear that if an amendment is tabled in the other place, the Government will accept it. That approach irritates me, although as I said in the House yesterday, it is not just this Government that do it; we did it when we were in government, too. It is seen as a sign of weakness if a Bill is amended in this House, but it is somehow a virtue if it is amended in the other place—suddenly the lights shine and we get a revelation of something that should really have put in by the Bill Committee.

If the Minister will not accept the amendment in Committee, I urge him to table his own on Report. There are two ways of doing this: either he puts it in the Bill or he gets the Prime Minister and the Government, across the piece, to amend the explanatory memorandum to give responsibility, which would have the same effect as the amendment. I plead with him to act. This issue will not go away.

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 of interest 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?

[James Sunderland]

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 said 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 Donà 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 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."—[*Official Report, Telecommunications (Security) Public Bill Committee,* 14 January 2021; c. 13-14, Q10.]

Dr Bennett said:

"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."—[*Official Report, Telecommunications (Security) Public Bill Committee,* 14 January 2021; c. 49, Q62.]

Dr Bennett later said:

"I have said that audit is needed of the assets in the network. The costs of being audited and of dealing with audits are very high, and they are costs that small companies may not have the

resources to meet."—[*Official Report, Telecommunications (Security) Public Bill Committee,* 14 January 2021; c. 52, Q67.]

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.