PARLIAMENTARY DEBATES

HOUSE OF COMMONS
OFFICIAL REPORT
GENERAL COMMITTEES

Public Bill Committee

TELECOMMUNICATIONS (SECURITY) BILL

Eighth Sitting

Tuesday 26 January 2021

(Afternoon)

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

Saturday 30 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

Tuesday 26 January 2021

(Afternoon)

[Steve McCabe *in the Chair*]

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

Laying before Parliament

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 which relates to a direction or notice that 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

FURTHER AMENDMENT CONCERNING PENALTIES

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

The Chair: 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) section24, so far as it relates to section18;".

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));".—*(Matt Warman.)*

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 overstretch 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 x, 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,

[Mr Kevan Jones]

and national security. I fall 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, 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 opaquely, 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 that 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.

[Matt Warman]

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	Onwurah, Chi
Matheson, Christian	

NOES

Britcliffe, Sara	Richardson, Angela
Cates, Miriam	Russell, Dean
Caulfield, Maria	Sunderland, James
Johnston, David	Warman, Matt
Lamont, John	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	Onwurah, Chi
Matheson, Christian	

NOES

Britcliffe, Sara	Richardson, Angela
Cates, Miriam	Russell, Dean
Caulfield, Maria	Sunderland, James
Johnston, David	Warman, Matt
Lamont, John	Wild, James

Question accordingly negatived.

New Clause 6

NETWORK DIVERSIFICATION (NO. 2)

'(1) The Communications Act 2003 is amended as follows.

(2) After section 105Z29 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 of—

(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

[Chi Onwurah]

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 telcoms 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 north of Watford—or discipline, having 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,* 19 January 2021; c. 73, Q87.]

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 quantum, medical and centres markets. Most recently, that has been expanded to include graphene-based devices.

Despite covid-19, in 2020 INEX grew by 50%, having recruited six highly qualified and experienced people. To address and grow the telecommunications market, those businesses in the north-east will have to extend their reach to partners in tier 1 telecommunications companies and their labs, and demonstrate that they have the skills and resources to scale the delivery of 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 inter-operable 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 Brake 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 D10, which the Defence Committee has talked about—a Five Eyes-type of collaboration among our allies. That idea has been kicking around for some time, yet we are yet to see it progress to anything concrete. Bringing together allies to work internationally and collaboratively on reinvigorating our telecoms sector is a laudable aim, but why is the Minister so afraid of monitoring its success?

A decade of neglect of our telecoms infrastructure has left us vulnerable and created the need for this Bill. We support the Bill, but it is clear that to protect our 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 forced to choose between technological progress and national security.

Matt Warman: The hon. Lady raised an important issue. Fundamentally, however, the issue of diversification is twofold. The Government want to see greater diversification within our telecoms supply chain. 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 the minimum, rather than one, for a telecoms network. That gives you an indication of what we will be monitoring and looking at, potentially, in codes of practice in the future. The hon. Lady is right to focus on this important issue, but it is wrong to pretend, important though Secretaries of State are, that any Secretary of State could legislate in the way she describes for the greater diversification that we all seek.

The focus of the Bill is on setting clear and robust security standards for our networks that telecoms providers must adhere to, and they must be met regardless of the diversity within any of those networks. To be fair, the diversity within a provider's supply chain, in and of itself, does not offer the guarantee of network security. A provider using a diverse supply chain needs to be held to the standards set out in this Bill, so that the provider is able to offer the security standards that we need, regardless 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. I do not think it is necessary to specify the need to collect information relating to diversification, as that is just one set of information that Ofcom may collect; it is just as important as several others in monitoring and reporting the security and resilience of networks. It is also 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 we 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	Onwurah, Chi
Matheson, Christian	

NOES

Britcliffe, Sara	Richardson, Angela
Cates, Miriam	Russell, Dean
Caulfield, Maria	Sunderland, James
Johnston, David	Warman, Matt
Lamont, John	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.