HOUSE OF COMMONS

Defence Sub-Committee

Oral evidence: The Security of 5G, HC 201

Tuesday 30 June 2020

Ordered by the House of Commons to be published on 30 June 2020.

Watch the meeting

Members present: Mr Tobias Ellwood (Chair); Stuart Anderson; Sarah Atherton; Martin Docherty-Hughes; Richard Drax; Mr Mark Francois; Mr Kevan Jones; Mrs Emma Lewell-Buck; Gavin Robinson; Bob Seely; Derek Twigg.

Questions 184 - 260

Witnesses

I: The Rt Hon. Ben Wallace MP, Secretary of State for Defence, The Rt Hon. Oliver Dowden CBE MP, Secretary of State for Digital, Culture, Media and Sport, and Ciaran Martin, Chief Executive Officer, National Cyber Security Centre.

Written evidence from witnesses:

- The Department for Digital, Culture, Media and Sport and the Ministry of Defence

Examination of witnesses

Witnesses: Ben Wallace MP, Oliver Dowden MP and Ciaran Martin.

Q184 **Chair:** Welcome to the fourth oral evidence session of our investigation into the study of 5G security in the UK. I am delighted to welcome to this hybrid session the right hon. Ben Wallace MP, Secretary of State for Defence, the right hon. Oliver Dowden, Secretary of State for Digital, Culture, Media and Sport, and Ciaran Martin, chief executive of the National Cyber Security Centre. I am pleased that we have two Cabinet members in the room—I think that is a first—although they are at the other end of what is a huge room. You are very welcome indeed. Thank you very much for your time. Ciaran, you are joining us down the line, so hopefully you can hear us as well.

We are very conscious that the Government are conducting their own study into the relationship with high-risk vendors, and that that will therefore frame some of your replies today, but I hope you will be as candid as possible, allowing us to explore the wider picture of our security and the development of 5G from a UK perspective.

Before we jump into the meat of the issue, I would like to ask the Secretary of State for Defence a couple of questions. Thank you for being here, Secretary of State. On these rare occasions that we have you in front of us, it would be remiss of us not to thank all those who serve and have served in the Armed Forces, in recognition of what they do and have done, bearing in mind that it was Armed Forces Day over the weekend. We are sorry to see that the events in Scarborough were slightly curtailed because of covid-19. Please pass on our best wishes to all those in uniform and to all those who have served, and indeed to their families and the wider community.

I have two very short questions, because I know that the Committee is keen to get on to the 5G issues. The first relates to reports that Russia is actively encouraging the Taliban to kill UK soldiers in Afghanistan by placing a bounty on their heads. I know that you cannot comment on intelligence reports themselves, but are you aware that soldiers are in any further danger because of the Russians placing any form of bounty or working with the Taliban to cause harm to those in uniform?

Ben Wallace: On behalf of the Armed Forces, it is their privilege and their duty, which they enjoy, to help protect and provide resilience to this nation, which is what they are doing. Today we hit a high; I think we have over 4,000 deployed today, delivering covid services and support. One of the highest amounts is at the mobile testing units. As we have seen in the news, for example with Leicester locking down, that mobile testing unit is so important. We will be able to move to where—I was about to say "threat"—the pressure is and deal with it. They are out there right now and we are all truly grateful. It shows that defence is not just about pointy things; it is also about command and control, moving at pace and understanding data and resilience. Thank you for your earlier comments, Chair.

On the reports, which I think were in the *New York Times*, all I can say is that I am aware of the intelligence. I cannot comment on intelligence matters, other than to say that we take lots of measures to defend our soldiers—the men and women of our Armed Forces—and to ensure that they are kept safe when they are deployed. We take a range of measures to mitigate the threat. Where that threat comes from is, I am afraid, broad; it can be terrorists, hostile state activity or any number of adversaries. We tailor make our defensive measures to meet that threat. I do not think there is any greater danger than the danger they face everyday from IS, al-Qaeda or, indeed, other forces in Afghanistan.

Q185 **Chair:** I will make it very clear that, if it is deemed to be true, it is unacceptable for a permanent member of the United Nations Security Council to be acting in this way. The second question relates to the National Security Adviser. We now have a new one coming online, Mr David Frost, but he also happens currently to be the chief Brexit negotiator. Whatever your views of Brexit, it is unlikely that is going to end any time soon. Can you give us assurances that he will be able to focus 100% on the issues of national security for the UK, specifically in relation to the delayed integrated review?

Ben Wallace: Chair, you said at the beginning "if these intelligences are true". I would leave it that we do not comment on the intelligence itself; we just take the steps. It is absolutely the case that we have seen countries such as Russia, and Russia in itself, taking lots of malign activity against us. Salisbury is the most recent obvious example, but as a state it is involved in a whole range of activities against its adversaries that we deem to be unacceptable and that we take steps against.

On the National Security Adviser, first I would like to pay tribute to Sir Mark Sedwill. I was a Security Minister for over three years, and now I have done this job for a year. I was with him, literally side by side, throughout the whole of the 2017 terrorist attacks, and indeed during Salisbury. He was the permanent secretary in the Home Office when I was there. He is a fantastic civil servant and an extremely competent individual. As NSA, he brought a lot of skill and fusion to bringing Government together to make sure they delivered right across the horizon when they faced a threat.

The response to the Salisbury poisoning was a very good example of the type of response he delivered. He helped co-ordinate the Foreign Office to deliver the expulsion of 163 Russian intelligence agents around the world. He helped me, as Security Minister, when we needed Ministry of Defence support to deal with Salisbury. He helped the intelligence services and the police deliver the investigation. Lastly, he helped the local authorities, through the NSS in the Cabinet Office and the NSC, deliver a message. He is a hugely talented person. He will make a fantastic Secretary-General of NATO if he is successful in getting that appointment.

David Frost is a respected diplomat. The qualities that I have seen in NSAs in the past are not purely about their background in security; they

are about their ability to work across Whitehall, fuse together a response and deliver a timely response to some of the threats. I should think that negotiating with the EU sets you up pretty well to tackle an octopus, which the national security construct can sometimes be in making sure you get a response, so I should think he will do a very good job as well.

Chair: We look forward to inviting David Frost to appear before this Committee in due course. We will now turn to 5G network security.

Q186 **Stuart Anderson:** I thank all the witnesses for coming along and taking the time to help us with our report. Secretary of State for Defence, we first want to establish, before we look at network security, how dependent the MoD is on 4G and 5G.

Ben Wallace: The MoD has a range of communications. The ones you always think about with the military are radio communications, satellite communications and, indeed, normal LAN desktop fibre communications that we deal with. It is a huge landscape, depending on what type of communications you are dealing with—top secret, secret, official sensitive, unofficial and so on. Deliberately, as I said earlier, the MoD's watchword is "resilience." We are not dependent on any one mode of communications. To do that would leave us desperately exposed to an adversary in a time of war, or even in a time of peace.

Q187 **Stuart Anderson:** Could you expand a bit on that? You said that you are not dependent on one mode of communication. Those are networks. If there was no 4G or 5G, where would the MoD be?

Ben Wallace: We would be able to use the landline network. If we are not dependent on 4G or 5G, we would be able to use our radio and secure radios. We would be able to use the other networks, because we are not reliant on a single type of network to communicate. As we have made clear, for example with 5G and Huawei, there is no Huawei in our very sensitive intelligence network. If 5G Huawei went down, that would not matter because we could still use our very high-level intelligence networks, which are removed of any high-risk vendor, to carry on communicating.

Q188 **Richard Drax:** Good afternoon, gentlemen. What steps are you taking to protect the entire 5G network?

Oliver Dowden: There are two elements to this. First, it is worth bearing in mind how we got to this point. The previous regime that we had in place was under the Communications Act. Under the Communications Act, the burden was on telecoms providers to determine their own security; they had that obligation. We have carried out a review of telecoms security, with the NCSC providing the underpinning analysis. Out of that, we have produced these proposals, which will form the core of the telecoms security Bill, which we will be bringing forward shortly. That will place a range of obligations on telecoms companies, so shifting the burden, so essentially it is now the Government saying what they need to do to ensure it is secure. That is the main focus of the legislation.

Within that, we have had to determine the approach we take towards high-risk vendors, of which Huawei is the most significant. That is why we have imposed the provisions that the Committee will be familiar with, so the cap and the exclusion from both the core and the sensitive sites. In addition to that, since the middle of May we have had the US sanctions in respect of Huawei. Given that those sanctions are targeted at 5G and are extensive, they are likely to have an impact on the viability of Huawei as a provider for the 5G network. That is why the NCSC is undertaking an analysis of the extent of that impact. It is pretty much finished with that. We are going through the final stages of it. Off the back of that, we will determine what policy measures, if necessary, need to be taken in response.

Q189 **Richard Drax:** The next part of the question is about how this differs from the Government's approach to protecting other networks. I think what you said was that with 5G it will be the Government who impose rules and regulations, rather than the provider.

Oliver Dowden: This will apply to all telecoms networks, so it will apply to 2G, 3G, 4G and 5G. This is a different approach. We have examined the potential vulnerabilities of the telecoms network as a whole and come up with guidance on how that should be addressed. That is currently in the form of guidance, which companies are not obliged to follow. The purpose of putting it on a statutory footing is to ensure that they then are required to follow it. That will not differentiate between the different levels of telecommunications network, whether 3G, 4G or 5G.

Q190 **Richard Drax:** Can you comment on Huawei itself? As you know, the Government have said that Huawei would be allowed to take 30% or 35%, or you will keep it to 30% or 35%, as I understand it. How can you trust Huawei? We have heard about this in different evidence sessions. Some people say there is not a threat, others say there is a threat, and some are in between. What is your view of allowing Huawei 30% or 35% access, so far as the future security of this country is concerned, with a company that is linked to the Chinese state, which, as you know, has a pretty appalling record?

Oliver Dowden: The first thing to be clear about is that the No. 1 requirement for us is to protect national security. In doing that, we asked the NCSC to carry out an evaluation of how we protect the telecoms network and, within that, what we do in respect of high-risk vendors. In respect of Huawei, which is the main high-risk vendor, I am absolutely clear eyed—and the advice from the NCSC was clear eyed—about the potential risk with Huawei, given that it is a Chinese company and we know the extent to which the Chinese state has influence over its companies, particularly through its intelligence laws. As a consequence of that, among other factors, including its resilience, we deemed it a high-risk vendor and put those restrictions on it.

It is because of our concerns about high-risk vendors and that we have excluded Huawei from any sensitive parts of the country geographically,

for example around nuclear bases and so on, or the guidance will set that out. Secondly, that is why we are excluding it from the core and capping it at 35% on the edge. The assessment of the NCSC, which was analysed and accepted by the National Security Council and formed Government policy from January, was that that was an acceptable balance of risk and that we were not unnecessarily exposed through doing that.

It is worth bearing in mind that all telecoms networks are potentially at risk. We have seen that our own telecoms networks have been compromised or attacked by hostile foreign states, such as the activities of the Russian state—that is in the public domain. There are always going to be risks, so one needs to mitigate those risks. The analysis from the NCSC was that that was a correct level of risk, particularly given the other risk we have on this, which is resilience and diversity. You get greater resilience by having more operators in the network.

I should layer all of this by saying there is now a further specific issue with Huawei. Given that the US Government have imposed sanctions on Huawei, and given that those are focused on 5G, we need to fully understand those and understand how that impacts on how much we can rely on Huawei equipment in the system, given that it is subject to those restraints from the sanctions.

Q191 **Chair:** It sounds like the pressure from the Americans is having an impact on your decision making.

Oliver Dowden: It is a fact that the Americans have imposed these sanctions. It is a fact that those sanctions are targeted at 5G. It is a fact that, given that they are targeting, for example, US patents, upon which Huawei relies, that will, in turn, have an impact on the reliability of Huawei. The reason we have given it back to the NCSC for consideration is to understand the full extent of that. If policy changes are necessary as a result of that, the process would be that, off the back of the report, I will work with the Prime Minister and then it will go to the National Security Council, and clearly I would make a statement to the House if it necessitated a policy change.

Q192 **Richard Drax:** I have one last point. Clearly this is largely to do with the defence and security of our country. You are the Secretary of State for Defence. Are you happy that 5G could be involved to the extent it is being planned to be involved?

Ben Wallace: Am I happy that high-risk vendors are contributing to the 5G network? No, I am not, any more than the whole of Government are. The Government's ambition is to remove high-risk vendors from the network over time. No one wants high-risk vendors in the network. That is why we have started with the process of banning from the sensitive part, capping in the less sensitive and working towards diversification of supply and everything else, to make sure we improve quality and so on, and identify the alternatives and options.

I recognise that there are other ways to mitigate security vulnerabilities. As the Secretary of State for DCMS said, our own networks are vulnerable. Everybody's networks are vulnerable. You only have to look at the range of cyber-attacks that happen every week, or even every day, to see that there are adversaries out there, either organised crime or hostile states, who are seeking in every way possible to exploit vulnerabilities. Some of those vulnerabilities are in the software. Some of them are weak encryption or weak passwords that your constituents or mine get tangled with. Some of it is shoddy quality.

The thing that we should all be concerned about is that shoddy quality of hardware in itself creates a vulnerability. That could be something that is delivered to your door, a British-made piece of equipment or badly designed piece of equipment. It could be Chinese, South Korean or American; where it is made is not a guarantee of safety. You might ask the chairman of the National Cyber Security Centre to come in on some of those questions, because that might provide an important reflection from the technical expert.

Q193 **Chair:** It is also an indication of why we need an Intelligence and Security Committee to look at these matters as well, but that is another avenue that we will not explore at the moment. Can I invite Ciaran Martin to comment? We are still on our very first question so we need to make some progress.

Ciaran Martin: I will respond quickly to three points that have been raised. The first is about the security of telecoms networks in general. The two Secretaries of State have put it very well. We have a serious structural challenge with the security of telecoms networks in general. That goes to the range of possible vectors of attack and some of the weakness that our casework has shown us over recent times. In 2018 we attributed to the Russian state a very serious compromise of some of our infrastructure, which allowed the attacker to go from home routers all the way to the controlling plane. That was unconnected to the national identity of the vendor, because we do not have Russian vendors in the network. It shows you some of the wider resilience and security challenges we have.

On high-risk vendors, as the Defence Secretary has just said, there are a whole range of exclusions, which are absolute blanket exclusions. It would take far too long to read them out and they are very technical. These are privately built networks by operators. The 35% is not a target. If the legislation passes, it would be a strict, legally binding limit, consistent with our risk analysis, because there are other risks of having two vendors in the market, which I have no doubt we will come to.

To deal with Mr Anderson's question about defence, I endorse what the Secretary of State has said, and I will perhaps expand on that a little. The National Cyber Security Centre spends a lot of money and expertise supporting defence on sovereign cryptography for some things, where we do not allow any non-UK parts—never mind Chinese or Russian—into the

supply chain. That is quite expensive, but in some small parts of key strategic national assets it is necessary. That has no dependency whatsoever on public telecommunications networks of any kind. Then we go through to things that have to be highly secure but interoperable with allies, all the way through to ordinary communications and business communications through public networks. It is very layered, depending on risk.

Q194 **Mr Jones:** Can I ask you about the American sanctions? They are directed against, for example, chips, but we are already being told that Huawei and others have basically bankrolled loads of chips for the future and will develop their own, in terms of technology, to get around that. Secretary of State, do you think that we are concentrating too much on the hardware, rather than what has just been said by the Defence Secretary? The really big threat is hacking and network security.

Can I ask one direct question to the Secretary of State for Defence about MoD secure networks? One of our American witnesses tried to give the impression that MoD secure networks have Huawei equipment in them. Could you reassure us by putting the record straight that our secure networks go nowhere near Huawei equipment?

Ben Wallace: On that specific point, I can. No, we have no Huawei on our defence estate or in our defence networks. We have been very clear with that, to make sure that happens. As I renew or place contracts with vendors, I now ask, even on the outside, "Have we got anything in this? What can we do to make sure we do not get exposed to it?", to verify at a whole level. I have been asking to do that recently and I got some assurances around that. No, if you go to RAF X, there is no Huawei or high-risk vendor in the communications or other networks.

Q195 **Mr Jones:** There is not going to be either. Is that right?

Ben Wallace: There is not going to be, no.

Q196 **Chair:** Do you accept that, if you have Vodafone or BT, you actually have Huawei there as well? At the moment, they are working together.

Ben Wallace: On the hardware and the hard part of the MoD network, there is no Huawei.

Oliver Dowden: You are right to look at entire network security. It is the case that, regardless of the nationality or the host nation of the vendor, there are risks all the way along the chain, in terms of where they are manufactured—Nokia manufactures a lot in China, for example—through to the people who are installing it. If you take both Nokia and Ericsson, they are non-UK companies, so there are risks there and there are risks in terms of the people working for those companies. All those reasons are why we need to look at the overall security of the network, particularly through the telecoms security Bill.

In respect of Huawei itself, this is why we have asked the NCSC to examine the impact of the sanctions, both on the hardware and targeted at the patents that underlie that. That is not just the hardware but the application of those.

Ciaran Martin: On the question of US sanctions, we were prompted by the new US sanctions in May to look very carefully at this. The future supply of chips is of fundamental importance to a company's ability to meet these demands. It is very different from the initial entity listing of a year previously. I would endorse Mr Jones's point about the holistic approach to security, software-based attacks and so forth. We have to look at the whole picture.

Q197 **Bob Seely:** My question is to the Secretary of State for Digital, Culture, Media and Sport. Oliver, you talk about the US sanctions being an additional element. Is there also an additional element in Huawei's role in Xinjiang province, about which we heard quite a lot yesterday? There is a lot of concern among parliamentarians, because you have a company that you want to allow to have up to a third of the UK 5G network involved working with the Chinese authorities in building what is effectively a surveillance state in Xinjiang and other provinces. Does that concern you? Are you going to make the telecoms security Bill amendable on human rights grounds? If not, may I ask why not? That is the first question.

Chair: We are going to come to the Bill in more detail in a second.

Oliver Dowden: Briefly, it is not within my power to limit the amendability of the Bill; that is a matter for the Speaker. I cannot imagine why any amendments would not be called, as long as they remain within scope, which is for the Speaker to determine.

In respect of Xinjiang province, the United Kingdom Government have been very clear in calling out human rights abuses. The Foreign Secretary has done so recently and it is a standing item, as it were, when we have interactions with representatives of the Chinese Government. We have asked the NCSC, as part of its analysis, to understand the impact on the viability of Huawei products, given the sanctions. If that necessitates any change in policy, that would be agreed with the Prime Minister and then through the National Security Council. It is up to the National Security Council to consider any other factors it may wish to. China's overall human rights record is fairly well established. The changed fact here is that sanctions have been imposed on Huawei.

Q198 **Bob Seely:** Secretary of State for Defence, you said that there is no Huawei kit on military sites, which I am sure is accurate. I know that it is not a military site, but there was a rumour about 10 years ago that BT phones were put into GCHQ. When everyone realised that there were sensitivities with Huawei kit, they stopped using the phones, which were clearly not used for super confidential or secure information, and people then moved to a new secure system in GCHQ. Are we sure we are 100%

correct that there is no Huawei kit in any form in some of our more sensitive sites?

Ben Wallace: I can give you the assurance that, on our sensitive sites and in our secure networks, there is no Huawei equipment. Some sites are entirely sensitive, if you know what I mean—everything about them is sensitive. We make sure that we have high levels of assurance, checked and supported by GCHQ, of comms and security around whatever we use as those networks. If someone is standing in a military base and uses their mobile telephone at the moment and they lock on to Vodafone, for example, as we know, some of those networks have Huawei in them, but no one should be going on to their mobile phone in a military base and discussing sensitive information. That would be in breach of all the information security rules and the protective security requirements and rules. We simply do not do that at all.

Ciaran Martin: I think the best way I can answer, to endorse what the Secretary of State has said, is to say that there are no national security capability dependencies, whether that is confidentiality of information or availability of capability, that are dependent on the sorts of networks we are talking about in the way that is being talked about. That is probably the best assurance I can give.

Q199 **Chair:** Let us turn to the telecoms security Bill and what might or might not be in it. How would the planned telecoms security Bill make our networks more secure? How does legislating provide more security for the UK?

Oliver Dowden: In short terms, it will implement the National Security Council's recommendations in respect of telecoms security and put that on a statutory footing. At the moment, we are relying on the good will of telecoms operators to stand by that. Until we put it on a statutory footing, we cannot compel them to do so. They are following it up to this point, but good practice is to put it on a statutory footing.

Q200 **Chair:** You have to put it into law. How are you going to incentivise the best practices from this legislation itself? Will it be focused enough and provide the necessary guidance, or will there be wriggle room?

Oliver Dowden: In terms of broad structure, there will be overarching duties in the legislation. We will then produce specific codes in terms of security. The purpose of producing those specific codes under it is to give us the flexibility so that this legislation is futureproof, so that we can keep up with further developments. Putting it on a statutory footing is the incentive. If companies do not follow it, they will not be following the law.

Q201 **Chair:** You mentioned the National Security Council. Has it had its meeting yet to determine its recommendations? If it has not, when does it meet?

Oliver Dowden: The process is that, led by Ciaran Martin, the National Cyber Security Centre has pretty much completed its evaluation of the

Huawei sanctions. This is why I have taken a step back. Remember that the original policy was endorsed by the National Security Council in January and announced to Parliament at that point. We have pretty much concluded that process. We are determining what policy changes, if any, will be required. Once that determination has been made and agreed by the Prime Minister, it will be put to the National Security Council. If that gives rise to a change of policy, the first thing I will do is come to the House to explain what that new policy is.

Q202 **Chair:** You are choosing your words very carefully indeed. Mr Martin, is your work done? Have you slid your recommendations across the table? Is your work complete?

Ciaran Martin: I do not want to get ahead of what the Secretary of State is going to say to Parliament. The best way I can put it is that we are at the stage of fielding questions from the Secretary of State and his Department: "What does this mean? What does that mean? What are our options?" The bulk of the analysis is done. The Secretary of State is now testing it with us and formulating in his own mind whether he can recommend something to the Prime Minister and the NSC. That is the best I can do.

Q203 **Chair:** That means that, if I could read your body language or your thought bubbles, I would know the answer now. Is that right?

Oliver Dowden: I do not think that is the case, because the purpose of having a National Security Council is that it is for all the relevant Departments, of which clearly the MoD, the Foreign Office and others will be significant players.

Ben Wallace: I have not read it yet.

Mr Francois: We know your view.

Oliver Dowden: I believe the Defence Secretary is bound by collective responsibility.

Ben Wallace: I am bound.

Mr Francois: Yes, but we still know his view.

Oliver Dowden: Off the back of that, the NSC will want to similarly scrutinise it, and then we will make a determination. The reason I am being a little cagey about all this is that the decisions have not been made and any changes in policy would be exceedingly market sensitive. If policy changes, it is right that that should be announced in the proper way.

Chair: Yes, and it is not yet 4 pm. The markets are still open so we would not want you to make any huge announcements today. We understand that. Looking to high-risk vendors, Mark Francois, do you want to take this?

Q204 **Mr Francois:** On the Bill quickly, Secretary of State, perhaps you could assist us. What are the likely timings for the Bill? When can we expect Second Reading?

Oliver Dowden: I am very mindful of the commitment that I made to the House during the passage of the telecom leaseholder Bill, where I said I wanted to bring it before the House before the summer recess. If it is the case that the Huawei sanctions necessitate changes to the legislation, the choice I will be faced with is to bring forward a Bill that, given the timeframe we are working to, does not fully reflect that, or to ask Parliament's forbearance to make those necessary changes and have a slight delay. The first thing I would do would be to come to the House to explain that position.

Q205 **Mr Francois:** The NSC has a new chairman, a new National Security Adviser, who no doubt would want to look at this. If there is a change in policy, you are going to come to the House and make a statement anyway. We thank you for that commitment. In the Lords last night, the Alton amendment was not pressed, although he gave notice he might bring it back on Third Reading. There are different rules in the Lords and the Commons, where we would not normally do that. The Government could probably yet still lose that vote anyway. Views may differ on this Committee, but there was a previous rebellion in the Commons on the leasehold Bill about Huawei involvement, in effect—the Government's majority was cut from 80 to 24, and that was all pre-covid. Is the truth not, in actual fact, that everyone, including you, knows that the Bill is already as dead as a dodo unless it very clearly excludes Huawei? Otherwise, it will die on Second Reading, won't it?

Oliver Dowden: I will bring forward a piece of legislation, assuming the Prime Minister asks the Department for Digital, Culture, Media and Sport to bring forward legislation, which I am sure he will, that reflects the advice I have received and the decision from the National Security Council. That will be based upon the decision made in January, as amended, if it is amended, by any further considerations in respect of the reliability of Huawei. My job as Secretary of State, with the other Ministers, will be to convince you and other Members of the House to back that piece of legislation.

Q206 **Mr Francois:** Yes, but the practical reality is that you have already lost. Would it not save everybody a lot of time if you came to the House tomorrow and put your hand up?

Oliver Dowden: We did not lose. We defeated that—

Q207 **Mr Francois:** It was by 24 votes, pre-covid.

Oliver Dowden: Yes, and, as I said in the Chamber, I was left in no doubt about the views of many Members of the House. I have outlined to you where we are with the progress of the Bill.

Q208 **Mr Francois:** Talking about legislation, according to the BBC lunchtime

news, the Chinese Parliament will today pass a Bill effectively allowing a massive crackdown in Hong Kong, totally in contravention of the Basic Law and the deal that we, the British Government, did with the Chinese when we handed back Hong Kong. That legislation is probably going to happen today. In the light of that, and all the human rights abuses that will follow from a totalitarian state that locks up a million Muslims for having the temerity to believe in God, are you really telling us that there is still a possibility we will allow a company effectively owned by the Chinese communist party to have a meaningful role in our telecommunications network? Is that really your position?

Oliver Dowden: In respect of both of the points you have raised, the Government have been very robust in expressing our profound disagreement with the Chinese Government in respect of the changes they are making to the laws and constitution of Hong Kong. Similarly, we have not stinted in condemning actions against minority groups in China. The process, though, for this piece of legislation and the balance of risk is to understand from the National Cyber Security Centre where those risks lie and the appropriate balance. It will then make recommendations to Ministers, initially to me, and then to the Prime Minister and the National Security Council. We will weigh up those factors.

If there is a change in policy, I will come back to the House immediately to announce that. Then it will be for Members of Parliament to determine whether they support the legislation as it goes through the House. There was a clear indication of views on the leasehold Bill. We are very mindful of that, but I am afraid you will have to wait to see the legislation that we bring forward.

Q209 **Mr Francois:** You said that the policy may change. Perhaps you could clarify what the current policy is.

Oliver Dowden: The current policy, as set out by the Foreign Secretary to the House in January, is that we will be imposing new sets of requirements in relation to telecoms security on telecoms providers. In respect of high-risk vendors, of which Huawei is one—the other much smaller one is ZTE—we are restricting them in three respects. First, we are banning them from the core. Secondly, we are banning them from sensitive sites. Thirdly, we are putting a cap of 35%. Moreover, we have also said that, over time, we want to address the market failure that has led to us having any high-risk vendors in the system at all. Over time, we do want to be in a position where we are reliant on high-risk vendors.

Q210 **Mr Francois:** To be clear, is the current policy that we aim to reduce them to zero, even though that may take several years—yes or no?

Oliver Dowden: We want to get to the position where we do not have them in the system at all, yes. We have not set out a timetable for doing so and that was the point of contention before the House.

Q211 **Mr Francois:** This is really important. The policy is that we have already decided that we will exclude them, but the question is how long that will

take.

Oliver Dowden: We have said that we do not want to have high-risk vendors in the system at all, so of course that will mean at some point I want us to get to that point where we do not have them. That is why I am pursuing—and I am sure we will come on to it in subsequent questions—a diversification strategy to correct this failure that has led to us relying on them in the first place and not having a sufficient diversity of other telecoms providers.

Q212 **Mr Francois:** It is not if but when.

Oliver Dowden: Ultimately, but there is a big difference as to the path for getting to that point.

Q213 **Chair:** We got there. The question is how quickly this bus is going to move. The point that Mark Francois is making, quite powerfully, is the fact that this is not just a technical decision on security; it is a political decision. We will explore this a bit later, but it is so important to push this home, which is why this resonates with colleagues. Is China—I pose this as a question— a country that you want to do business with, given how it conducts its own business with its own indigenous population, and indeed wider afield? That is the big question that we need to explore, which we will do in a few minutes.

Oliver Dowden: May I respond very briefly to that point? The Defence Secretary may wish to come in. Is China a country with which we wish to do business? We do business with China all the time. As a Government, we are not going to end up in a position where we are not going to do business with China. We are clear headed about the risks of Chinese companies, particularly given their intelligence laws. We are clear headed and robust in expressing our concern, in particular about their human rights abuses.

The principal focus of the advice we will get from the NCSC—we have done previously and subsequently—is about the risk in terms of the security of our telecoms networks. To your point, Chair, the National Security Council does not just view things in the narrow prism of the specific advice from the National Cyber Security Centre about the risks; it also has to take into account all those wider geopolitical considerations. That is the proper process for doing it. Then the Government explain their position to the House and Members of Parliament express their view through legislation.

Chair: Not only Parliament but Britain and the world are recalibrating their views on China, given China's recent conduct. It has not matured into that global citizen that we hoped it would become. That is why questions are now being asked, not least from our friends, the United States. On that note, can I turn to Gavin to probe a little further into the relationship with the US and the sanctions?

Q214 **Gavin Robinson:** Perhaps I could direct this question to Ciaran Martin—it

is nice to see another strong Ulsterman attending the Committee this afternoon. Perhaps, Mr Martin, because you are in a separate location, you will be able to answer this question unfettered by the scrutiny of your Secretaries of State. Could you give us a sense of how, from your perspective, the US sanctions encourage us to take a decision of a further review on the presence of Huawei products in our network.

Ciaran Martin: I will not take the bait on separating myself from my ministerial masters—they are only a mile up the road. We were asked to do this security review of telecoms as a whole by DCMS way back in October 2018. It is a very complicated set of technical issues. I know obviously the geopolitical questions have just been raised and the Committee will come on to that. Even within the narrow confines of the technical, it is a very challenging and complex problem.

One of the criteria that we consider when looking at our framework for vendors, and high-risk vendors specifically, is whether these people are going to be able to do what you require of them. As the Secretary of State for DCMS has already set out, we are going to have much more rigorous security standards and they are going to be enforceable in law. Are particular companies going to be able to meet those? Legal risk, including legal risk of US sanctions, was always part of the framework.

In May 2019, the US placed Huawei on the entities list. That immediately triggered a review of the initial advice to Mrs May's National Security Council. It turned out that those sanctions did not materially impact its ability to provide 5G in the way that we initially thought they might have done, because we did a rigorous technical analysis. The May 2020 sanctions are a different creature. They are deliberately more targeted at Huawei's future ability to source hardware, particularly chips and things that would more affect 5G. We have had to have a fresh look at that.

We are at the part of the process that the Secretary of State for DCMS and I have explained, where we have more or less completed our work and he is testing it for policy recommendations. When we saw the sanctions announced in May 2020, we viewed it instantly as potentially a material change in the facts. Therefore, we began a reassessment of our January advice to the National Security Council. I hope that answers your question.

Q215 **Gavin Robinson:** Yes. To follow on from that, Ciaran, helpfully, if your assessment of the May 2020 sanctions was that there could be an impact on the future presence within the networks, are you still of the view that the sanctions from May 2020 have no impact on the current presence in the existing 4G network?

Ciaran Martin: We will settle that out when the Secretary of State has completed his deliberations. In part, there are policy choices around potentially how you would manage impact. I think it is safe to say, from publicly available analysis of this, that the material impact of the May 2020 sanctions on future deployments is far greater than any impact on

stuff already there, particularly in terms of managing national risk. In the UK context—I say this as a matter of fact, not an argument—quite a lot of UK Huawei equipment is quite old because it has been here in various guises since about 2003. In terms of national risk management, the focus of the analysis is very much on the more recent and future deployments.

Chair: Stuart Anderson, do you want to turn to the timeframe again? Let us look at that in a bit more detail.

Q216 **Stuart Anderson:** Secretary of State for Defence, in April you told us that the goal was to manage high-risk vendors down to zero in the future. We have just heard from the Secretary of State for DCMS that there is no definitive timeline. This is key for us to understand. When we speak to senators and congressmen over in the US, they want it done as quickly as possible. We spoke with Dr Levy from NCSC. He said that there are different stages, from three years to seven years, to the lifecycle of a product. We need to understand the timeframes with this. To say the goal is to do it leaves us very unsure of this. Can you expand on some timelines for that?

Ben Wallace: The Secretary of State for DCMS and I both say the same thing, which is that we want to get it out of the network. How we achieve that and in what timeframe came up in the debate on the legislation, where people wanted to set a time limit. All this goes back to the technical advice.

Chair, as you said yourself, there are two parts to this: one is the geopolitical debate and the discussion about our relationship with China and trade—it is an entirely legitimate debate and people have lots of strong views on the issue—and the other is the issue of taking the technical advice about what you can mitigate and live with right now, and how you can turn round an oil tanker.

As you yourself said, Chair, we had all hoped that China would emerge, through trade and capitalism, into a modern democracy, where alongside trade would go respect for rights and so on. Most people in Parliament believed that for many years. That was the economic partnership relationship over decades that was set up with the Chinese. You do not just suddenly switch it off and put a handbrake on your oil tanker.

That is why, when it comes to taking the technical advice about what we can do here and now to protect ourselves from high-risk vendors, I turn to the world-leading experts of GCHQ. If GCHQ and the National Cyber Security Centre tell me that they can take steps to mitigate that in a realistic horizon that allows time to replace hardware as it comes to the end of its life, who am I to ignore what I believe is the world's leading SIGINT intelligence agency of GCHQ? That is my view.

I am very happy to have the bigger debate about whether we should discuss things with China or trade with China, but fundamentally the timeline will be set by two things. One is what other states are doing. The

latest round of US sanctions is a fact. It is a better set of sanctions than its earlier set and it is specifically designed in a smarter way to put countries that have high-risk vendors—specifically Huawei, I think, in the American sanctions case—under greater pressure. We will have to take steps, depending on the technical advice, which I have not yet seen, to mitigate that. That is one part of it.

The other part is that we feel that, in the here and now, we can take that step of banning it from the core, capping it on the outer core and working towards cutting it out of the system at a date that fits the technical advice. No one in Government wants to compromise security—no one. No one is ignoring our technical experts' advice on security. If Ciaran Martin said to me tomorrow morning, "We have discovered this or that", I would be the first to jump out of my seat and say, "That's it. Switch it all off." They do not, because they are world-leading experts and they know that is the technical position.

We are working towards removing high-risk vendors, country-agnostic. That is the other thing we need to make a point about. We do not want shoddy, poor-quality, badly designed kit in our system. No one should want that, whether it is made in China or in Timbuktu.

Q217 **Stuart Anderson:** Thank you for that answer. We have been very fortunate to be able to speak to those experts as well. If we remove Huawei from the network, that will leave two providers in our network, both with more than a third. We do not trust any provider because there are gaps in every system. What is the plan to transition from a 35% presence of high-risk vendors down to zero? I know that you say you are waiting for the timelines from the experts, but there has to be a plan. There are significant ramifications of how we would remove high-risk vendors.

Oliver Dowden: We made it clear back in January, and indeed before January, that we needed to correct this market failure that had led us to two vendors, in Ericsson and Nokia, plus a high-risk vendor, in Huawei, and our reliance on that. We needed to start a process of diversification. The diversification process has three core elements to it. The first is to secure the existing two incumbent providers. The worst thing you could do for diversification would be to lose another one of those vendors. Given the situation with Nokia's share price and speculation over potential takeovers, for example, there is always a risk there.

The second thing, and the single best way of dealing with this, is to get other vendors into the market. Both Samsung and NEC are obvious vendors that we would like to get into the UK market that are in other markets.

The third thing is then, over the medium term, to look at the whole structure of vendors, moving to more open radio access networks. The idea is that you can then have interoperability between different bits of the kit, so you could have companies from different countries providing

different bits of the kit that then link together. To achieve all those things, we cannot just act unilaterally as the United Kingdom. We are working with our other partners across the world, and not just the Five Eyes, but the G7 and other countries such as India, South Korea, Japan and so on. We are continuing to advance work on that. That work is ongoing.

Q218 **Bob Seely:** Ciaran may be the best person to answer this. When I was speaking to the cyber leads on this issue a couple of months ago, I asked them how long these guarantees last. I was absolutely shocked to be told that we can provide a security guarantee against Huawei for seven years. You are not talking about generations. You are not even talking about a decade. I was told the guarantees last seven years and the clock on that started ticking a year ago, so effectively the guarantees run out some time early in the next Parliament. Would any one of our interlocutors care to comment on that?

Ciaran Martin: I am not exactly sure of the specific conversations you are referring to. The framework that the Secretary of State is bringing before Parliament, both generally for telecoms security requirements and specifically for high-risk vendors, is designed to be much more flexible, to adapt to continuing changes in the circumstances. Even before the Bill has been brought before Parliament, we are already showing that we will respond to changes in circumstances by reviewing the technical advice from January in response to material changes in the facts on the ground.

For example, the high-risk vendor framework is not just elegant bureaucratic code for Huawei. As things stand in the radio access network, that is what we are primarily talking about in the here and now. There are, for example, scenarios where one company becomes very dominant. This is purely hypothetical. I am just saying that this is what the framework is designed to do. If one company were to become very dominant but have weak security practices, that would be a risk and we would manage that as a high-risk vendor, and the Secretary of State and the regulator would.

It is not designed to have a five-year or seven-year limit. We have an ongoing and enduring framework that is designed to be adaptable over time. I would not associate myself with a five-year or seven-year timeframe, if that is what you are referring to.

Oliver Dowden: To add to what Ciaran has said, the legislation is specifically designed to give us the flexibility to be able to change the rules as the advice changes. We will not be setting out the restrictions on high-risk vendors in a permanent way. Those will be in the form of directions that are given by the Secretary of State. Clearly, for me, for the Prime Minister and for members of the National Security Council, the first priority is to defend national security. We will keep this under review. If the advice about the risks posed by high-risk vendors changes, we would immediately change the rules in respect of them.

As Ciaran has said, even before the legislation has come forward, a significant issue has arisen with one of the high-risk vendors—the principal one, Huawei. We are examining that and, if it necessitates changes to the rules, we will not hesitate to make those changes.

Q219 **Bob Seely:** Apart from the fact that, if you have already allowed them massively into our network, it becomes almost impossible to change it afterwards, doesn't it?

Oliver Dowden: No, in two respects. First, there is a lifecycle for these products, so they churn over time anyway. In extremis, if we really thought there was a significant risk, we would have to look at removal of that risk. We would have all those powers at hand.

Q220 **Mr Jones:** Unlike Mark, I actually support the present Government's position on this, as outlined by the Secretary of State for Defence just now. We have the balance right between risk and dealing with the reality that is facing us. The more important thing is the telecoms Bill, which will not just talk about Huawei but drive up security across the network, which is vitally important. In coming to a decision on Huawei, some people forget the economic cost. There is an economic cost if we ban it completely for 5G, but also a huge economic cost if we have to strip it out of 4G and 3G networks that already exist. Have you done any analysis of what that would cost? How will that influence your decisions?

Oliver Dowden: Clearly, we examine all these options. Take the decision from January, and the restrictions we placed on Huawei. We need to be slightly careful, because we are working with individual companies and they give us commercially sensitive information, but BT chose to put the impact of that into the public domain. That was £500 million. We think the impact of those restrictions we imposed is roughly £1.5 billion, with about a year-long delay. Clearly, if we impose further restrictions, there will be costs associated with that but, as I am at pains to keep saying, our primary consideration is national security. We will not do anything that puts national security at risk. Of course there are costs associated with it.

To a certain extent, we are also looking at how we ensure there are not unfair cost advantages to certain providers by having lax security standards. That is why the whole of the telecoms security Bill and the advice on telecoms security is about tightening up standards across the board. It is worth noting on the rip point that even the US is not currently calling for the ripping out of existing vendors from the 4G network.

Q221 **Mr Jones:** No, but that is where we have got to. I have found it annoying, because a lot of this debate is around people who want to sidestep the technology and security issues, rather than fight, as I think the Secretary of State for Defence just said, bigger geopolitical issues. I have no problems with some of those issues against China, but if we are going to exclude it from telephone networks for geopolitical issues, there are a hell of a lot of other parts of our economy where you are going to

have to start ripping out Chinese investment, which will have huge economic costs.

Can I just touch on a point you made about diversification? Having looked at it, there is not a great deal of money to be made in the hardware. I accept there are a small number of vendors and that is possibly how we got to the position we are in. We saw a presentation a few weeks ago showing that there are opportunities on RAN systems in terms of the software. Could you tell us what you are doing to try to generate home-grown businesses around that? To me, from a security point of view, that seems a far more productive avenue, in getting diversification but also driving up security, rather than wondering who actually makes an antenna.

Oliver Dowden: That is the medium to long-term solution driving OpenRAN. We have already taken measures in respect of that. First, we are launching flagship OpenRAN testbeds with mobile network operators. Clearly, that is going to be at a small scale to begin with. Secondly, we are looking to co-ordinate R&D funding with our other partners, particularly Five Eyes, because it would make sense if we co-ordinate between different specialisms within the different elements of an OpenRAN.

We are also looking to work with our partners around the world on having common standards, since the more common standards we have, the more interoperability we have, and similarly trying to influence standards bodies. We are then looking at what financial incentives we can create for mobile network operators to start adopting an OpenRAN system.

Chair: You touched on European operators, Ericsson and Nokia. Can we explore whether they themselves are vulnerable?

Q222 **Bob Seely:** This is for Ciaran Martin. Is there any evidence that Huawei's equipment is more vulnerable to cyber-attack than that of Ericsson and Nokia? One hears stories and I read in certain bits of the advanced comms media about the flaws, either accidental or deliberate, that allow backdoors. Everyone has backdoors, because you need that to provide security and so on, but these are ones that vendors or western Governments may not know about.

Ciaran Martin: There is a lot in that question. I know you have looked at our oversight board reports for Huawei in the UK, in terms of their present equipment. Those have revealed that Huawei's general practice of security is objectively lower at present than their main competitor. We have set out the evidence for that. We said very clearly that that is evidence of poor engineering and security practice, and does not constitute direct evidence of deliberate insertion of so-called backdoors by the Chinese state. The sorts of flaws we are talking about would not normally be referred to as backdoors. They are basically weaknesses and vulnerabilities that can be exploited by a range of actors. As someone on

the board of GCHQ, I do not think they are the sorts of vulnerabilities that a nation state would insert.

The broad answer, in net to security terms, is that they are objectively weaker in general standards. I wanted to make that point and draw the correct conclusions from that. Therefore, one of the impacts of the new legislation, should it pass, would be a much greater obligation on the operators, subject to regulatory penalty, to make sure they were not employing suppliers that failed to meet the standards.

Q223 **Bob Seely:** To follow up, would you know about backdoors you did not know about, so to speak? Secondly, is the report from the Banbury cell late coming out this year? When do we expect it? They talk about these sorts of issues.

Ciaran Martin: On the first question, by definition, so-called zero-day vulnerabilities in anything, whether as part of telecoms equipment or some other part of internet infrastructure, are things that people do not know about. It is perfectly theoretically possible that we do not know about a backdoor in Huawei. We do not know about a backdoor that someone has inserted unbeknownst to Nokia or Ericsson either.

There are differences in the trustworthiness of companies, their corporate intent, their culture, the rule of law and their adherence to what we would understand to be normal rules-based commercial practice. We would not put Huawei in a category with Nokia and Ericsson. There is a difference between their trustworthiness as corporate entities in their countries of origin and trusting their equipment. We do not trust any of the equipment. We cannot trust any of the equipment. That is important.

On the second part, the report has been delayed by a number of factors, principally covid-related disruption and the fact that the people who would normally do the report have been doing the foreign direct product rule analysis. We are aiming to get it out as soon as possible. I hope it will be out fairy soon.

Q224 **Chair:** It seems that you have three choices to make. You could jump out if Ciaran Martin says, "Get out tomorrow", as Mr Wallace was suggesting might be an option. You then have two to three years, which I think is one that has been mooted. Then there is seven years, which we understand is the natural lifecycle of the kit we are using. Do you have any economic costs about the impact of those three decisions? How much will it cost us to do any one of those?

Oliver Dowden: Just as in any market, the more restrictions you place on the free market, the greater the cost of doing so. That is a standard regulatory cost. The more stringent those restrictions are, the higher the regulatory cost. If you were to ban a vendor, that would impose additional costs on the operators because there would be less competition and less supply. If you were then to put restrictions on how long you have the equipment in, there would be additional costs on that. To be

clear in all this, if national security requires it, we will not hesitate in taking decisions that will impose additional costs on mobile network operators. The primary consideration is the national security implication of it.

Q225 **Chair:** Can I make it very clear? It could be that, from a security perspective, you are saying, "It is coming over the hill. We need to do it in a number of years." If you have done any economic modelling on the speed at which you remove Huawei, or any other risky vendors, from our systems, please could you share that?

Oliver Dowden: Yes. Sorry, I hope you did not think I was being obtuse in my answer. If we make any changes in policy, as we do so we will set out the costs and timings associated with that and provide them to the Committee and the House.

Chair: Thank you very much indeed. We touched on our relationship with the US. I was first made aware of what Huawei was up to when I visited Australia a number of years back, so there is an implication to our Five Eyes community in addition to the US.

Q226 **Sarah Atherton:** Good afternoon, gentlemen. We know that GCHQ sets the gold standard for preventing network exploitation. How confident are you that if we use Huawei in the UK's 5G network it will not compromise our sensitive communications with our intelligence partners?

Chair: In essence, it is the wider impacts on our intelligence community, particularly the Five Eyes, in sharing intelligence with them. It has been very much on the front pages. Is there any impact as we are moving forward?

Ben Wallace: I have seen no change whatsoever in the level and detail of the intelligence sharing between the Five Eyes.

Oliver Dowden: I would echo that. We have had no indication that it would have an impact on that.

Ciaran Martin: As an operational leader, I would echo that as well. There has been no diminution in the co-operation yet from the US.

Q227 **Sarah Atherton:** There have been reports that some US politicians are attempting to hinder the deployment of the US F-35 fighter jets in Britain because of our involvement with Huawei. If that is the case, it is widely believed that China will have succeeded in forming cracks in the US-UK special relationship. Secretary of State for Defence, is that a risk worth taking, given this evolving situation?

Ben Wallace: The reports you refer to are discussions from US lawmakers on the Hill. People have talked about it. It does not bear a linkage to security vulnerability. Not sending the F-35s to bases in the UK is the example you are talking about. It is not logically technical, or it is not technically logical—I do not know which way around you would say it.

If you do not like 5G or you do not think our 5G network is trustworthy, that is nothing to do with whether you put an F-35 fighter in a base in the UK. It is an apples and pears comparison.

It is true that there are a number of United States politicians who want the UK to choose between their view and other people's view, and who will use sanctions to do that. It is a fact that the latest round of sanctions is designed to make 5G supplied by Huawei very hard to do, or potentially unviable. That is why our technical experts are looking at what the impact of that is. It is more symbolism. I cannot think for American politicians. They will have to answer for their view.

We run very secure bases. We run very secure production processes. We make part of the F-35 just outside my constituency, in Samlesbury. By the way, every single F-35 in the world will be made partly in Samlesbury, so I do not think it is entirely linked. I do not think it is a measure that would make anyone safer.

Chair: We will turn to other vendors that possibly could work here in the UK but are not yet here.

Q228 **Martin Docherty-Hughes:** Ciaran, I think you might be the best person to answer this question. I wonder about the idea of new vendors—for example, NEC, Fujitsu and Samsung. Is there any likelihood that they will come to the market? If so, when would that possibly happen?

Oliver Dowden: To update you, the Minister for Digital Infrastructure in the Department, Matt Warman, has been having constructive discussions with all those vendors. They have all expressed an interest in entering the UK market. The challenge we need to overcome is how we ensure that this is a market they feel comfortable entering, given that they are not currently present and there is actually quite a high cost of entering a new market.

That is why we are looking at things such as trade incentives for incoming vendors, financial incentives and how we can help them create scale. None of the vendors you referred to has any significant presence in the EU at all, so how can we work with other countries to do that? We are also looking at, for example, diversity requirements, potentially in spectrum licences. We are looking at all those ways of trying to ease a pathway in for them, because there is clearly the desire to enter but at the moment there are blocks to that happening.

Ciaran Martin: I concur with that. Under the leadership of the Secretary of State and the Minister for Digital Infrastructure, the discussions with companies are going well, but these are huge, capital-heavy commitments. There are short, medium and long-term aspects to this: the short term is to try to attract people in there; and the medium and long term is to try to reshape the market. I will not repeat that, because the Secretary of State has covered it in a number of previous answers.

The only addition I would place on the table relates to a point Mr Jones made. Over time, some—I stress some, not all—of the functions we are talking about that at the moment are dominated by a small number of providers, some of which are high-risk vendors, can become software-based and virtualised. That is a benefit in two ways. First, the barriers to entry are far, far lower for software. Secondly, securing software is something that quite a lot of people, including plenty of people in the UK, in Government and the private sector, are quite good at.

We want to do this. We want to get through and encourage more providers. Then we want to nudge the system along, working with partners, whether that is standards, virtualisation and so forth, to get out of this current very difficult situation.

Martin Docherty-Hughes: Ciaran, your answer in terms of virtualisation poses far more questions that we would need answered—maybe at another inquiry. There are those of us who have a concern that it is not necessarily the infrastructure but the software, the platforms that are used, that will be the biggest threat.

Chair: We touched on OpenRAN. This is an important opportunity here.

Q229 **Richard Drax:** Secretary of State, you mentioned OpenRAN and the advantages of it, so that question has been answered by you. Perhaps you could help our viewers and certainly me, a bit of a Luddite on all this. If Huawei is given 35% access, and OpenRAN then becomes a reality and this virtual system takes over, you have more providers, as I understand it. Will that override the existing Huawei infrastructure and make us totally independent of Huawei, or will Huawei have its own version of OpenRAN or whatever it is? How is this going to lead us to this more independent and secure network?

Oliver Dowden: I will attempt to answer and then may defer to Ciaran Martin, who has deeper expertise on this than I do. In essence, this is the idea of having OpenRAN. Rather than creating a very high barrier to entry, in that you need to have all the elements of being a vendor for telecoms, you break down the different elements of that and ensure interoperability. You could have one company providing one element and another company providing another element. This is quite at the cutting edge. There is one network in Japan that has managed to procure OpenRAN, but that is starting from scratch.

The advantage is, first, that it is another way of bringing in diversity, because an OpenRAN solution would be an alternative to Huawei, or indeed Ericsson, Nokia, Samsung or any of the other entrants. Secondly, from a UK perspective and working with our allies, while it is quite hard to create a new vendor from scratch in any of these countries, we have sufficient technical capabilities across likeminded countries that we could provide different elements. The challenge is to ensure that there is interoperability between each of these elements, so basically you can pull

out one bit and replace it with another. Ciaran, I do not know whether there is anything you want to add on that.

Ciaran Martin: The Secretary of State has covered virtually all of it. OpenRAN is about reducing, significantly if possible, a very significant incumbent advantage, both vertically and horizontally, in networks. Two things at least can mitigate that in the long term. One is the regulatory framework and the telecoms security requirements. At the moment, there is no regulatory requirement for greater interoperability. There is no incentive, if you like, to do so. It is cheaper to have incumbent advantage in the short term and then it has long-term problems, as we are seeing.

The other is the initiatives that the Secretary of State's Department's paper last summer set out. There is £200 million for a 5G testbeds and trials programme. Some of that is going to things that will encourage OpenRAN. BT and Vodafone are both, as I think you know, Mr Drax, trailblazers in piloting this. We strongly support that.

Q230 **Richard Drax:** When will we see this OpenRAN, if it is so marvellous? When is it going to be rolled out? When are we going to see this take off?

Oliver Dowden: We have to help build the market. We are working with our allies to make sure we influence common standards on that, so you have the protocols that will enable you to work with the different companies in different countries. We are already trying it out, because it is new technology, and we will look to scale up those protocols. We would also look at how then, as we build confidence in it, we can create financial incentives for mobile network operators to start procuring from that.

We will go as quickly as we can, but it is important to understand that we are starting from a very low base. This is new stuff so it will take us time to build up; hence one of the challenges around diversification is the speed that we can go down this path. We are proceeding as quickly as we can. I met with the Foreign Secretary just last week, discussing how we can work even more intensely with our partners around the world, particularly on OpenRAN.

Q231 **Richard Drax:** Presumably the MoD is going to welcome this new virtual system. It will be a new ball game for you too, presumably.

Ben Wallace: Depending on security, you want open architecture technology. Otherwise you get taken to the cleaners by defence primes and technology companies. If you are on a hook and trying to diversify, that is when the money starts getting clocked up. The more we can have that type of open architecture, the less dependent we become on one or two individual suppliers.

One of the things about China is that we should be making sure that Huawei is open eyed about our relationship and trading with it. The best thing to protect us from an abuse of power or dependency is to be less dependent and more reliant on diverse supply chains and suppliers. That is the best way to deal with it, whether that is a country or technology.

Q232 **Bob Seely:** Huawei has closed systems, as I understand it. How does its business model support or make O-RAN more difficult? Generally with Huawei, because it can continue to undercut rivals using credits from the Chinese state, it can effectively make it very difficult—near impossible—for new entrants to the market if it is allowed any role in our 5G comms. Can I have a comment on those two thoughts from the Secretary of State for Digital, Culture, Media and Sport?

Oliver Dowden: That is a challenge with Huawei, which is why we are looking at facilitating OpenRAN as an alternative to Huawei. This is part of the diversification away from high-risk vendors. In respect of undercutting rivals, the biggest risk we have sought to address initially with this is that, by having lower standards, there is a potential for high-risk vendors to undercut. The way we are addressing that is imposing higher standards across the board. That will remove cost advantage to vendors that have lower standards.

Ciaran Martin: Mr Seely raises a very important point about the diversification strategy. Huawei, as a major global provider, has some inbuilt power because of its market share in a global market. While I understand where he is coming from, the concerns he has expressed also arise if there is complete exclusion of Huawei from the UK 5G market. The companies will be looking at this picture across the globe. In terms of patents, interoperability and so forth, where they are no more closed or open, in terms of actual interoperability, than their major competitors, those things still arise.

That is why there are two points. The Secretary of State has made one of them about levelling the playing field in terms of security costs. Secondly, that is why it needs, as both Secretaries of State have been saying for some time in this hearing, really quite significant and difficult co-ordinated industrial policy activity across lots of likeminded countries, not just the UK.

Q233 **Bob Seely:** Ciaran's point about international co-ordination brings us very well to the next question. There have been reports of a D10 alliance of democratic nations to develop alternatives, specifically to Huawei and ZTE, high-risk vendors, and not just Chinese high-risk vendors. How accurate are these reports? Would such an alliance work? I have also seen similar calls from the Huawei interest group and others for an alliance of Five Eyes countries to build up a common set of standards so we can support a western 5G and advanced communications industry ourselves.

Oliver Dowden: For the benefit of others who may be listening—not you, Bob—the D10 refers to the G7 countries plus Australia, South Korea and India. That was not a concept that originated from the UK. I believe it originated from the Atlantic Council's D-10 Strategy Forum. None the less, it is a good description of the sort of countries that we would wish to work with. From all the conversations I have had, with the Foreign Secretary and others, there is definitely an overarching desire to do

something in this space. The challenge is ensuring that all other countries align with us in treating it with a sufficient degree of seriousness and drive, and that they really want to make this happen.

That starts with making sure the international standards and international bodies are in the right place. Bob, you are very familiar with how international relations work. Given that we want to move rapidly with this, the challenge for us will be to ensure that the urgency we are treating it with applies to the other countries we would need to do so. There is definitely the desire. Our challenge is to work through at pace to get these things in place.

Q234 **Bob Seely:** On that point, there seems to be a desire, maybe not with all those 10 states, but certainly with Canada, Australia—which said no to Huawei—and the United States, which is now actively trying to build out national champions or space for its own states at well. You have France. The Czech Republic, as well as others, is looking at non-Huawei alternatives. There seems to be a kernel or nexus of countries that could begin to provide a common set of standards and, potentially, use the very important work that has been built up by your Department in the telecoms security policy paper, much of which has been fantastic.

Oliver Dowden: That is precisely why we are pursuing all this. That is the enduring way of correcting the market failure that has arisen, where we have become too dependent on a small number of providers. There is a mutual interest between the countries that you have described, where there could be opportunities for companies in all those countries, in an OpenRAN system, to get a slice of the cake. It can be a win-win situation. That is why we are pursuing it with urgency.

Q235 **Chair:** Given the fundamental change we are going to experience over the next 10 years with the roll-out of more data, our entire world will become ever more reliant on the telecoms capabilities that we have. Would you agree that the reason China is ahead is that it has pumped gargantuan sums of money into Tencent, Alibaba, China Mobile and Huawei, companies like this, meaning we simply cannot compete? If you go back to the space race, where America had the desire to catch up and then overtake Russia, it put lots of state funding into that industry to get ahead. Is there that moment where we need to recognise the sheer power that the winner gets in having dominance in the global telecoms capability, not least with quantum computing coming around the corner as well?

Oliver Dowden: There are two important points there. First, it is undoubtedly the case that various Governments have failed to treat this with sufficient seriousness, which has allowed us to get into this undesirable situation of having high-risk vendors in the system. This is why diversification is so important. From the conversations that I have had with the Prime Minister, and indeed if you look at what he has said today, he is very committed to bold interventions to get ahead on this

kind of stuff. There is a realisation that we need to do this, a strategy we are working on and a political determination behind it.

You also allude to quantum computers and the wider questions that will be addressed particularly through the investment security legislation about how we define and protect strategic national interests, which go way beyond telecoms networks. Quantum computing and AI are two very obvious examples of where we need to ensure that we have proper, if not sovereign, capability, but capability within likeminded nations. Maybe I am straying slightly into the Defence Secretary's territory.

Ben Wallace: Remember, the money that China put in is our money. It is because everyone in the west and elsewhere piled into buying manufacturing in China. I am old enough to remember when everything said "Made in Taiwan" or "Made in Hong Kong" on the bottom and when China was not doing that. It goes right to the heart of both this Government's strategy and other Government strategies around tech. We need to grow our own skill base, first and foremost. CyberFirst is an excellent GCHQ competition about getting women and people into cyber. Building a skills base is how we do this.

China is not the only country that has state-subsidised or state-owned competitors. There is France in aerospace. Often you are competing against Spanish yards owned by the state. We have always had some of those practices. We win orders by being better or more productive, with better technology or niche capability. That is no different. That is the path that we, as a capitalist market economy, go down. The challenge for us is that we took our eyes off the ball about the importance of what tomorrow's critical national infrastructure is.

It is without doubt that today's critical national infrastructure is very different from how it was 30 years ago. Telecoms, mobile networks and cyber are as important as gas and water. We should not have allowed other people to run away with those technologies. We should have also not allowed ourselves to be so dependent.

Chair: Let us finally turn to the wider geopolitical implications. This entire debate about 5G has prompted, as I said at the beginning, perhaps a revisionist view of China.

Q236 **Mr Jones:** The decision about Huawei was taken in January, which, as I say, is a position I support. Were you surprised at the reaction, particularly of the United States, to that well thought out, security-first approach we would take?

Oliver Dowden: I should clarify that I was not on the NSC at the time, so I cannot comment on the deliberations that took place. I need to choose my words carefully in commenting on foreign countries. It is undoubtedly the case that the US sees this strongly through a geopolitical prism. It has made its position abundantly clear to us, and indeed

abundantly clear to the world, in the sanctions that it chose to impose on Huawei, the policy implications of which we are now understanding.

Ben Wallace: It is clear—I looked at the evidence sessions from Senator Cotton and others—that this is way more than just pure technology. This is about a view of an emerging China that the United States has pretty much across the aisle. I was in Washington not long before the covid shutdown. There is a strong view in the United States, pretty much across the aisle, that the growth of China is in a direction that they should be worried about and that they wish others to be worried about.

Q237 **Mr Jones:** It is rather hypocritical, though, isn't it? One of the biggest investors in Senator Cotton's state, for example, is Chinese companies. As you have already alluded to, the reason why China can do this is that we have bought manufacturing goods from there. One of the biggest growth areas in some frauds has been, for example, raising capital on US stock markets for Chinese companies. I think the tagline is that we are going to be a strong, independent nation once we leave the EU. Are we? Are we going to just be bullied by the United States into a position? In some of the rhetoric from some commentators and people in the Administration, it could be seen that we are not going to take an independent decision on this. We are going to be bullied into doing what the Americans want.

Oliver Dowden: It is just a fact that the US Government have imposed these sanctions, and it is a fact that they will have consequences for the reliability of Huawei kit. We need to understand the full extent of those consequences. The intent behind it really would not matter. In terms of the consequences for our telecoms security, we have to understand this new fact and how we deal with it.

Ben Wallace: It is not an American sanction against us. It is an American sanction against the use of American IP, not British IP, that seems to render part of Huawei equipment inoperable. The United States is perfectly free to sanction whoever it wants. It is American IP. If it was British IP being sanctioned by a third country, you might say you are being bullied or pressurised, but it is not. In my understanding, it is about chip manufacturers and things coming out of Taiwan using US IP. We would impose our view, and we still do, on IP that we own. I do not think it is a matter of US bullying.

The US is clearly free in its own economy to say to people, "You can trade with us or you can trade with country Y; it is up to you" on certain issues. Because the US is independent, it does not have to make sanctions in accordance with, for example, the EU. In the EU, we all have to agree to make sanctions or no one agrees, which is the current state of the EU sanctions policy. Should the United Kingdom wish to place sanctions on people because of human rights abuses, that is already in the sanctions Act. That was passed by this Parliament last year, I think, so we are free to do that. We could not have done that as a member of the EU.

Q238 **Mr Jones:** No, but if we refuse to go ahead with Huawei and 5G, for example, that decision is not going to be value neutral in terms of the effect on other Chinese investments in the UK, such as students and other areas. That will have a huge implication for the wider economy. I take the view, and I think you do, Secretary of State, that you should address this from a security angle, rather than as a big geopolitical thing.

The Government have turned full circle. I think you were a member, and certainly the Chair was, of the Cameron Administration. You could not get a more panda-hugging Administration, in terms of our relationship with China. As the Chair said, I accept the world has perhaps now woken up to some of these threats. If we are going to take that independent decision, which we are confident has been done for the proper security reasons, that surely has to be the way forward, rather than just saying, because the Americans have taken the decision they have, we will roll in behind what they do.

Ben Wallace: I do not think we would get a choice. It was the Android system, if I am not mistaken, that the US banned from use with Huawei handsets and pretty much overnight decimated the Huawei handset market. That is American IP. The Americans can do what they like with their own IP and it is not for me to tell them. If the United States directs or uses sanctions against its own technology that render Huawei inoperable, that is just a fact we have to face. It is not an attack on us; it is just a fact. If the Huawei network does not work any more because it cannot use a certain type of chip or whatever, it is not about security. It just does not work. We would have to get something else.

Oliver Dowden: We are separating out two quite different things. One is a hard-headed analysis of our relationship with China. I am sure members of this Committee would wish us to have a slightly different nuance, in terms of that relationship. It is then an entirely separate question, which goes to security. Given the fact of these sanctions on Huawei, that is a very relevant factor in terms of the reliability of its equipment, which is why we have asked the NCSC to provide that analysis and see what the policy consequences are.

Chair: That debate must be had. We must have a reset, an understanding, a review of our relationship with China, given the changes.

Q239 **Mr Francois:** Secretary of State for Defence, there were suggestions that, if we carried on down this path, it would affect our access to sharing intelligence with our Five Eyes partners, which is clearly critical to our national security. Is there evidence to date that any of that critical intelligence has dried up?

Ben Wallace: No, nothing at all.

Q240 **Mr Francois:** Good. Does that include Australia? Arguably, among the Five Eyes, if there is going to be an expansionist China in the Pacific, or at least in the south Pacific, Australia is in the frontline. Has there been

any diminution in our intelligence exchanges, including sensitive intelligence, between the UK and Australia?

Ben Wallace: No.

Q241 **Mr Francois:** No. It is still sharing sensitive stuff with us and vice versa.

Ben Wallace: Yes.

Mr Francois: Good. In that case, was it China that attacked Australia a couple of weeks ago?

Ben Wallace: The Australians had a public press conference with their Prime Minister, naming China as the perpetrator of that. As you will know from your time as MinAF, the owner of intelligence is the person who decides how and when to release it, so you would have to raise that with the Australians. They made their public statement. It is not for me to say what I have seen from our Five Eyes partners.

Q242 **Mr Francois:** You have no reason to contradict the Australians.

Ben Wallace: What I can say is that the Chinese have already been named on a number of occasions for using cyberattacks against the United Kingdom and our allies over time. I think APT10 was the name of the cyberattack that was attributed by the Foreign Office only last year or the year before. It has a record of doing that, both for espionage purposes, and indeed for purposes of mischief or malign activity.

Q243 **Mr Francois:** If we accept what the Australian Government have said, and other than on cricket we have no reason to disagree with them, we know that China launched a major cyberattack on one of our longstanding international Five Eyes partners. They attacked them. Secretary of State for DCMS, could we possibly feed that small nugget into the ongoing review please?

Oliver Dowden: These are clearly relevant considerations. The only pushback I would say is that, if you take another vendor, they manufacture a lot of their equipment in China. We are wholly interrelated with China through the global supply chains. We have to approach this in two respects. One is understanding the security and getting the analysis of the security implications. The second—and this is the balance the National Security Council has to take—is to consider both that and the wider geopolitical considerations to which you allude.

Q244 **Mr Francois:** They have attacked one of our closest allies. Presumably we at least take that into account, don't we?

Oliver Dowden: Of course.

Mr Francois: Thank you. That is very reassuring, Secretary of State.

Q245 **Chair:** Maybe that is something for the Secretary of State for Defence to explore. Clearly, NATO's article 5 is now out of date, given that the character of warfare is very much changing into this new plane. It is less

about terrain and more about digital.

Ben Wallace: In December, NATO agreed to expand and examine in the area of cyber-warfare and cyber-defence, so that was a success.

Q246 **Chair:** If you could provide the Committee with an update on that, it would be very helpful indeed.

Ben Wallace: Yes, we will get you an update on that.

Q247 **Mr Jones:** The Chinese are attacking our systems every week, whether it be for criminal activity, industrial espionage or other things.

Mr Francois: That might be a good reason not to let them in.

Oliver Dowden: It may reprise the whole argument again.

Chair: Let us get back on point and look at the actual relationship between the state of China and Huawei. That is important here.

Q248 **Mrs Lewell-Buck:** Secretary of State, I want to explore with you how closely linked you feel Huawei and the Chinese state are, bearing in mind that last year you said China needed to modify its cyber behaviour and adhere to a code of behaviour that amounts to fair play. In January, you are reported to have said China is a "friend of no one", but by March you were convinced that any risks from Huawei could be mitigated and that they were manageable. Can you please explain to us your quick change of thinking on this and what your views are on the relationship between Huawei and the Chinese state?

Ben Wallace: In March, I think that was a question around the technical threat that was being posed by China's security. The technical advice is that you can mitigate that threat. It is absolutely the case, as Kevan Jones said, that China on a regular basis, on a regular drumbeat, has been engaged in cyber-espionage and all sorts of things against us and our allies, in the same way Russia and North Korea have been involved in things. Funnily enough, even other countries that might surprise you have been engaged in some form of cyber-espionage against this country.

The thing about fair play goes to Mark's question about what the NSC is for. One of the things we discuss at the NSC is that balance that the Secretary of State for DCMS talked about. One is the technical advice. Technically, can we keep ourselves safe? Secondly, we marry into that the bigger discussion of the geopolitical challenge about what we want from China and what we want China's behaviour to be. My reference to fair play is that I believe we are not the world's policeman who goes around telling people how they should run their countries, but we believe in human rights and respect for international law when it comes to trade, navigation and everything else.

We want China to become the great nation it could be by following that rule of law. Ultimately, the aim of all this, the discussions and when we

attribute cyber-attacks to China by the Foreign Office, is to say to China, "This behaviour is unacceptable. You need to change your behaviour so we can carry on, engage and have a strong and economic relationship with you". That is how you get them to change.

I have made it clear in maybe lay terms that I believe in fair play. This is China-agnostic. Anyone who wants to trade with our country should sign up to certain acceptable rules. There are rules at the UN. There are rules and treaties around intellectual property and respect. We should not only live up to but also enforce them.

Q249 **Mrs Lewell-Buck:** You mentioned changing behaviour and discussions on that. Have there been any discussions with the Chinese state on the change of behaviour in relation to your fair play comments?

Ben Wallace: On a number of occasions, the Foreign Secretary has raised human rights abuses and concerns. Only recently with Hong Kong you saw the United Kingdom go beyond that and offer longer status to passport holders in Hong Kong. At the same time, only today I think the Foreign Secretary has said he is deeply worried by the latest round of legislation and wants to see the detail. The worry is that this goes against the spirit of their obligation. We are concerned about the direction of travel. We are concerned about our friends, the Australians, and what they have experienced.

We also have to provide a thinking policy about how we engage with China and try to use our influence to get it to improve that behaviour. I do not know whether it was a treaty, but the United States certainly engaged about cyber-espionage at some stage when President Obama was in power. For a short time, that changed China's behaviour, so it will change. It has changed on environmental issues. If my memory serves me right, it used to be pretty much not engaged but now it has done a lot more on the environment. We are optimistic that it will continue in that right direction.

Q250 **Mrs Lewell-Buck:** I am assuming that you stand by the comment that you feel these rifts are manageable. How can you then be sure that China's national intelligence law of 2017 will not apply to Huawei's activities in the UK? How is that risk manageable?

Ben Wallace: That is why we have GCHQ and Ciaran Martin here, to make sure it is manageable. I would say one thing about security laws. Having been a Security Minister, we have security laws under which, in defence of our nation, we request that our UK companies, or anyone working here, if they are served legitimately with warrants or whatever else, have to comply with them.

Oliver Dowden: We know that the 2017 law would apply to Huawei, as it does to all Chinese companies. That is one of the factors that played into its categorisation as a high-risk vendor. That was fully taken into

account in the advice we received from the National Cyber Security Centre.

Q251 **Mrs Lewell-Buck:** To clarify, we will have no guarantees at all that it will not apply, will we?

Oliver Dowden: It applies to all Chinese companies, so of course it is capable of applying to Huawei. That was a factor in its designation or categorisation as a high-risk vendor.

Q252 **Bob Seely:** To follow up on what the Secretary of State for Defence just said, maybe I misunderstood. You said that the NCSC was examining the risk. The risk of having Chinese personnel working for Huawei and reporting back on what they are doing is not going to be covered by the NCSC, is it? That is traditional espionage and not technical vulnerabilities in Huawei kit. If the Government have now confirmed, which I am delighted about, that they believe that China's security laws request Chinese staff here to be working for the Chinese state, that is an additional significant issue.

Ben Wallace: No, I think you misheard. I did not say that. I was just saying that there are laws in China, and of course they are not oversighted in the same way our laws are. I would not say they were comparable in any way. I was saying that many countries have security laws that require private companies to comply with law enforcement agencies under warrant and so on. That is what I would say. On espionage, it is also the case that GCHQ and others are part of the effort to stop espionage, wherever that comes from.

Q253 **Sarah Atherton:** We continue to listen to discord in this House about the growing dominance of China on the global stage and Huawei's technology enabling Chinese state oppression. This discussion around engagement with Huawei has shifted towards moral arguments that the people can relate to. What is my right honourable friend's assessment of having such a company provide a telecoms infrastructure that is linked to the Chinese Communist Party and at odds with our own values?

Chair: Essentially, we have a Chinese communist party setting very different global rules than the rest of us. Is it really right that we should continue down this path?

Oliver Dowden: Ben may wish to come in on this. We know that large private companies in China often have links to the Chinese communist party. That is a fact and that was one of the factors that led to the designation of it as a high-risk vendor. You are right to highlight human rights abuses and other areas of moral concern, which are constantly raised by the Foreign Secretary, the Prime Minister and others in bilateral dialogue. The analysis was clear eyed about understanding that risk, and I do not know whether Ciaran wants to add anything to that.

Secondly, we are also very cognisant of the wider geopolitical arguments, which go to exactly the kinds of discussions at the National Security

Council and would factor into the Government's overall approach in approving this. We take the technical advice and then there is a political and geopolitical discussion through the National Security Council.

Q254 **Martin Docherty-Hughes:** The Committee should note that, in the last half hour, President Xi of China has actually signed the Hong Kong security legislation and it has now come into immediate effect. I am sure we will probably all agree that Beijing will survive this heinous declaration of this piece of legislation. Sadly, from my perspective, this goes right to the crux of the moral decision on Huawei. Taking that aside, I wonder what role the UK military and intelligence community has in countering Chinese aggression, whether it is this type of legislation in Hong Kong, either bilaterally with the United States or through Five Eyes, NATO and, of course, our allies in the European Union.

Ben Wallace: There is a range of things that we are engaged in against any of our adversaries or anyone that threatens your and your constituents' security. We work together with the Five Eyes in sharing intelligence but also in sharing cyber, for example understanding each other's cyber vulnerabilities, spreading where we find exploits to make sure they are closed off and, where we can attribute someone who is doing it, calling them out to make an example of them or, indeed, embarrass them in front of an international community. That is what we do.

On other areas, you have seen European powers, US and Five Eyes make sure we have upheld freedom of navigation, because we know people are concerned in the Pacific about what China has been doing in the south Pacific sea. You have seen a number of transits by us, friends and allies. We have often also called out the human rights abuse that we have seen, certainly if you think of the Uighurs and issues like that.

All our capabilities are aimed at countering threat. To some extent, they are country-agnostic. They are tailored to a country, but they are country-agnostic. Where we see a threat, we act on it. Where we can disrupt it, we can shut it down or we have to take a stronger action, we shall do so. I do so in conjunction with my colleagues in the Foreign Office and elsewhere. That is something that we are always determined to do and we are always on watch for it.

Q255 **Martin Docherty-Hughes:** Secretary of State, I know you never sugar-coat things when you come to Committee. I am very grateful and it is a bit of a breath of fresh air. You mentioned the Foreign and Commonwealth Office and working with the Ministry. One of the main ways of combating countries such as China is to work in a more co-ordinated development approach with our allies that are the least well off in global society. Maybe you can remind us today that, with the announcement last week of DFID and FCO combining, that certainly will not be a silver bullet to solve defence spending or to deal with an expanding China.

Ben Wallace: No, but it is still the same people sitting around a table in many aspects. You are right that one of the best ways we can roll back inappropriate influence by a range of countries in the world on countries that cannot defend themselves or do not have the rigour is to come and support them in making sure their cybersecurity is up to scratch. At the Commonwealth Heads of Government, there was a commitment from the United Kingdom to help many of those countries in their cyber-protection. We should be proud of the role we play in that.

We are always alert to practices that may undermine those countries. I have been instrumental, in my Department, in making sure we target a number of countries to make sure they get the right help at the right time and to give them resilience. That is the main key. We do not want these countries to be susceptible to undue pressure.

Q256 **Martin Docherty-Hughes:** Finally on that point, I wonder why that decision has been made now, before the end of the integrated review, because it makes it harder for you to say to Back Benchers like me, and also to your own Back Benchers, that spending decision will now have to wait until after the review. You are making this decision based on spending before the end of the review.

Ben Wallace: No, the SDSR 15 gives us plenty of scope to move and take steps to meet any threat. This is not a massive reprioritisation. What may happen in the IR is about whether we increase soft power versus hard power, whether we change how we do something. That is important, but the SDSR 15 gave us plenty of leeway to use defence diplomacy and defence engagement—remember the Fusion and the NSIG model that developed out of the National Security Council—in bringing together the whole horizon of assistance. Whether that is DFID, the Foreign Office, the Department for Education or the more traditional security Departments such as Defence, all of that is already happening.

The integrated review is about a realisation that this constant competition we are seeing from our adversaries is global and real. We are not yet in the right position to face that, and we need to move to face it.

Q257 **Chair:** Can I just echo Martin's comments there? The 5G debate is really only scratching the surface here. We need to have that wider discussion linked in with who we are in a very changing world. The world that we are going to wake up to post-covid, from a security perspective, will look very different indeed. The SDSR—or the integrated review, as it is now called—is the thing that maps out what our vision is, what our role should actually be, yet we see changes in the Whitehall architecture happening almost weekly now, without, first, understanding and doing that appreciation of the threats that are coming over the horizon, taking a stock check of our current capabilities and then working out what we actually want to do.

I say this to two very senior Cabinet members with huge influence on the Prime Minister. Please, can we bring forward that integrated review, so

we can understand what is happening around the world, not least with China? I hear the arguments to say, yes, we have to work with China, but in our lifetimes it is going to become more powerful, economically, technologically and militarily, than the United States. You mentioned the South China Sea. It is only a matter of time before they put in air limitations, in addition to the maritime one that is there already. Once they have done that, it will not be Hong Kong that we are considering. Taiwan will be under pressure there as well.

The question for us all right now is where this all goes. When are we willing to stand up and say, "The trajectory here is leading us to a cold war"? We are seeing a country now taking off the gloves, willing to operate from a very different set of rules, and not only that, but encompass other countries, through its One Belt One Road initiative and other ways of influencing countries, to either neutralise them on the international bodies such as the UN, so they cannot complain, or develop its own world order, challenging what the west stands for. We have become too risk-averse.

I make the point now, which has been made again and again: 5G is an important debate to have, but there is a wider one of what we want to do, working with our allies, such as the United States. I fear that we are repeating the period in the 1930s, with economic depression right across the world, lack of global leadership, no international organisations that are able to arbitrate and no single country willing to stand up for the rules and world order. That, I believe, is something that it is in Britain's DNA to want to embrace. I simply make the case, if I can, to say, "Let us have that discussion." The point of that would be the integrated review.

Ben Wallace: Maybe I can put your mind at ease on part of this. Tomorrow, I am taking the chiefs of all the services for an away day, plus a group of specialists, experts and professionals, to ask them each to paint not only how they would face today's threat, tomorrow's threat and the threat post-2030s, but also how they would envisage the whole of Defence doing that. I am determined that we start with the threat and with a vision of how we are going to meet that threat. There will not be a finance person in the room.

We will them come back from that away day, red team it, test it and everything else, and be able then to say, "Okay, this is how we think we will face the threat in the world today." They have all been told to be free thinking. I do not want them to, behind the scenes, stitch it all up. I want them to come before us and give me whatever they think is the vision. Then we will work backwards from that. We will be honest that we will not have all the money to do everything, I suspect. We will have to talk to the Foreign Office about what our ambitions can really be, but that is the way we are going to do that, so that it is worked out the right way round, rather than asking, "Can we save a bit of money here? How are we going to salami slice something?"

Q258 **Mr Francois:** If you conclude that China is a threat, will you say so publicly?

Ben Wallace: I think we have been pretty clear that we feel China's behaviour is not in line with many of the things we have as our values. We have also said what we want China to be. We want to modify the behaviour.

Q259 **Mr Francois:** Will we stop using all these euphemisms, like "competitors"? If we believe they are a threat to our way of life, western democracy and our allies, will we say so clearly?

Ben Wallace: If the NSC comes to that collective view, it will say that. I am more hawkish than some, but I do not think China is a threat to our way of life at the moment. No, I do not. It is a challenge at the moment to many of our norms. That is what we are trying to encourage it to return to.

Mr Francois: Let us see what your colleagues conclude tomorrow.

Q260 **Chair:** It is fortuitous that one of the people you will be speaking to tomorrow is in front of us in a couple of weeks' time, General Sir Nick Carter, head of the Armed Forces. We look forward to him reporting back on the discussion.

Ben Wallace: No, he will not be allowed to do that. That will anticipate the IR. You have to wait for the IR.

Chair: Okay. Could I thank both Secretaries of State and Ciaran Martin for your time this afternoon? It has been a very helpful and constructive session indeed. I hope that you have understood the feeling around this table and, indeed, from colleagues. We very much look forward to that statement, which is going to clarify what happens next with 5G, and indeed that important telecoms Bill. Who knows? As you go away to pontificate on what might go in the Bill and, indeed, that statement, perhaps what you have heard today will tip that balance. A bit like Sisyphus and his rock, it will take you across the line and make you realise that importance of us recognising that we need to press the reset on the 5G telecoms.

I am reminded of that big speech by Churchill in Fulton, Missouri. He stood up to tell the Americans about the power of an authoritarian state. It would be good to hear another speech of that same order, recognising that another authoritarian superpower is choosing to shun international accountability and pursue a very different approach to the world order. It is important that the west becomes less risk-averse and plays its role in redefining the Bretton Woods organisations, which are now out of date. I very hope much that Britain plays an active role in that discussion.

Secretaries of State and Mr Martin, thank you very much indeed for your time.