HOUSE OF COMMONS

Defence Sub-Committee

Oral evidence: The Security of 5G, HC 201

Tuesday 28 April 2020

Ordered by the House of Commons to be published on 28 April 2020.

Watch the meeting

Members present: Mr Tobias Ellwood (Chair); Stuart Anderson; Sarah Atherton; Mr Tanmanjeet Singh Dhesi; Martin Docherty-Hughes; Richard Drax; Mr Mark Francois; Mrs Emma Lewell-Buck; Gavin Robinson; John Spellar.

Foreign Affairs Committee Members present: Alicia Kearns; Stewart Malcolm McDonald; Bob Seely.

Questions 1 - 47

Witnesses

I: Emily Taylor, CEO, Oxford Information Labs, and André Pienaar, CEO and Founder, C5 Capital.

Examination of witnesses

Witnesses: Emily Taylor and André Pienaar.

Q1 **Chair:** Welcome to the Defence Sub-Committee's inquiry into the security of 5G. I am pleased to see that all Committee members have dialled in. Thank you very much indeed to André Pienaar from C5 Capital for joining us here today. Can you hear me okay?

André Pienaar: All clear. Thank you, Tobias.

Chair: Thank you also to Emily Taylor from Oxford Information Labs. You know what we are looking at today. I will invite you to introduce yourselves, but I would first make it clear that, given what is happening in the wider world, Parliament will be pausing for a minute at 11 o'clock. The parliamentary estate will be paying tribute to key workers who have lost their lives in a one-minute silence. We will be participating in that, so please be aware of that for 11 o'clock.

Emily, could I invite you to say a few words about your background and how it is relevant for our inquiry on 5G?

Emily Taylor: Thank you for inviting me today, Chair. My name is Emily Taylor. I am the CEO of Oxford Information Labs, which is a cyber-intelligence consultancy. I am a lawyer by background and I have been involved in the internet environment for the last 20 years. I am an associate fellow of Chatham House, the international affairs think-tank, and editor of its *Journal of Cyber Policy*. We are very involved in tracking the development of technical standards internationally, particularly through the UN. With Stacie Hoffmann and Samantha Bradshaw, I have co-authored a book chapter on 5G and on the geopolitics of the build-out of these networks.

Q2 **Chair:** Thank you very much indeed, Emily. You are very welcome. Over to you, André.

André Pienaar: Good morning everyone. My name is André Pienaar. I am the chief executive of C5 Capital. We are a British investment firm that is focused on investing in fast-growing cyber-security companies. I started my career in cyber-security in the 1990s when the internet still had about 20 million users—that tells you exactly how old I am. We work very closely with some of the world's leading cyber-security companies, for example IronNet Cybersecurity, which is led by General Keith Alexander, the former Director of the National Security Agency. We are focused on making sure that Britain remains a centre of excellence in the field of cyber-security and a leader in this field worldwide, in terms of our investment strategy.

Q3 **Chair:** Thank you very much indeed. You are both very welcome today. The study we are doing has, I think, risen in prominence given the reaction or the conduct of China during the coronavirus, which has illustrated the type of character of this growing superpower. From the

Government's perspective, the integrated review has been delayed for a year. So it is no understatement to say that our inquiry into 5G and the security of our infrastructure is probably the most important inquiry that we will be doing in the foreseeable future.

It has been a very live debate in the House of Commons and in the country as a whole. That is why the Committee has decided to focus on the security implications, because many of the decisions fit into the change in the conduct of war, which is less state-on-state territorial aggression and more causing economic harm, for which our ever greater reliance on the internet and the movement of data is very much the new battleground.

It is fair to say that the level of understanding on this issue of 5G divides into two camps. We have some specialist groups that have been studying this—I should add that we welcome a couple of Foreign Affairs Committee members to this session—but many parliamentarians are not familiar with the background, the details and indeed the exposure that we might be offering ourselves up to in a very uncertain world. It is in that context that I hope we can pursue some of the issues and explore some of the challenges that we face.

Emily, could you please outline why it is that this generation network—5G—is so different from its predecessors in changing the world as we see it in the future, but also the exposure from a security perspective as well?

Emily Taylor: 5G is the fifth generation of mobile broadband and it builds on previous generations—3G, 4G and so on—but it is a step change in the architecture of the network. This is a very simplified version, but previous generations such as 4G have essentially been fairly dumb networks. There is a lot of cleverness involved in managing traffic on the network, but essentially it is about pushing data through to users and making sure that everybody is connected.

5G really changes the way that the network behaves. It embeds software into the core of the network, so that it can be much more responsive to demand. Say you have a massive event in a stadium, and many tens of thousands of people gather together at one stage. Instead of the network failing, it could scale up to support that sort of demand and then scale back down again, so it will be much more dynamic.

It will enable a lot of things that we have been looking forward to and, with our security hats on, perhaps dreading. It would be a great enabler of the so-called internet of things—smart devices, driverless cars, smart cities, smart water systems, power systems and power grids. There will be a lot more infrastructure, because you will be operating at much, much higher speeds, and that means there will be a lot more masts and antennae visible to us—they are talking about one on every street lamp, so that type of frequency.

However, there will also be a lot more devices connected to the mobile network. In the past generations, like 4G and 3G, the types of devices that you connect are fairly predictable—they are usually phones. But now we

will have all sorts of things, and we know from our study of the so-called internet of things—these smart devices—that often a lot of them are, sadly, built with very poor cyber-security. So you will have a lot more things connecting to the network and with a range of cyber-security abilities, if you like. And our reliance on that network will be great. We all know that where there is great reliance, there is also risk involved, because if those things fail or if they are compromised, the impact of that failure is all the greater.

Q4 **Chair:** Thank you. André, Emily spoke about the fact that you will need a tower—a node—literally on almost every single lamp post. Can you put in perspective the timescale? We are having a debate on 5G at the moment, but is 5G about to be rolled out across Britain or indeed across the United States? Will this happen in the next months, or years? The idea that we will have automated cars, the internet of things, smart cities and so forth seems a bit further down the line, even though decisions need to be made today. Is that correct?

André Pienaar: Yes. If I may, I will for a moment just step back in time before we step forwards in time. As Emily explained, the previous generations of telecommunications standards enabled different things: 1G and 2G enabled voice and texts; 3G enabled us for the first time to access the internet on our phones; and then 4G and 4G LTE really created the app economy and all the consumer convenience that we today take for granted, with applications such as Uber being able to do online and e-commerce and shopping. And 5G, as the next standard, will be even more transformative, for a number of reasons.

The principal reason is that 5G operates on different frequency bands simultaneously, including a higher frequency range, and at this higher frequency range you have more significant transmission challenges, which requires this proliferation of telecommunications infrastructure that Emily referenced. That means we will go from the big mobile phone towers and base stations that we are all so familiar with seeing on our landscape, to microcell devices and microcell-connected antennae, which will have to be proliferated first in our cities and then in rural areas to enable this level of connectivity.

As Emily said, this new standard of telecommunications will enable much faster speeds and a much lower level of latency—the time it takes devices to connect. This will enable us to connect more devices and to accelerate the speed at which we receive data and video, but it will also open up a whole new range of areas of innovation and use cases, including defence and national security. All of this will require long-term investment. Today, we are still a long way away from actually implementing 5G in the UK, and certainly in the US. It will require long-term and very significant capital investment.

Q5 **Chair:** Would it be fair to say that you are likely to get areas of development? For example, a university campus or a particular town centre may develop a 5G network first and then it will expand from there, rather than seeing a mass roll-out.

André Pienaar: That would be a very accurate way to forecast the development of 5G. The current generation of telecommunications standards have been so dependent on 4G LTE, which is very much consumer facing. The 5G network will be much more focused on enabling private networks, business-to-business applications, business to Government, and Government to Government. We expect to see much more development of private networks, either in an area of research and development, in a city or in a particular use case.

Chair: Thank you. Over to Gavin.

Q6 **Gavin Robinson:** Good morning to you both. Perhaps I could address this question to Emily in the first instance. You talked about the spectrum of devices and the uses that 5G will have. Is that where the inherent security vulnerability comes? Can you give us a sense, from a security perspective, of the distinct differences? Perhaps it is the software embedded that you mention. What are the distinct differences, from a security perspective, between 5G, 4G and 3G?

Emily Taylor: There are several layers of concern when we look at 5G or any network that is so big and so relied upon. Yes, you are absolutely right about the type of devices, the number of devices that will connect to them, and their characteristics. A lot of smart devices—for example, baby cameras—have been involved in major cyber-attacks, because a lot of devices that are fairly straightforward and simple are poorly secured and easily compromised. One area is the type of devices and the number of devices.

However, as you mentioned, the type of network itself is changing from a more static network to something that is dynamic and software-driven—it is virtualised. I work with software programmers. Software contains errors because it is made by humans, and there are millions and millions of lines of it. Nothing is perfect. Software contains errors, and those errors can form vulnerabilities that are exploited by adversaries.

In very high-level terms, it is much harder to guarantee security where you have complexity. Nobody would claim that you could ever guarantee 100% security, but with 5G there are layers of concerns: the devices, the nature of the network and the physical safety of the equipment. This is something that we have seen in recent days and weeks with the debunked theory that 5G was in some way causing coronavirus. We started to see actual infrastructure being vandalised—we can often forget about physical security when we are thinking about cyber, but that is another aspect.

The management of all these networks requires a lot of sophistication, so you have a management layer for the network, which itself, if it is connected to the internet, is accessible by adversaries. That could be another entry point.

With any security issues, you can end up running away with the concerns, but we also need to bear in mind the context of what 5G can bring to our economies and our lives. Here we are, meeting virtually in the context of a

complete lockdown because of a different type of security concern—a public safety concern. The internet and technology are enabling us to have some kind of normality and some kind of economy as this pandemic rages. While we should be concerned about security and national security when it comes to 5G, we should also bear in mind the context of what it can bring and what it can enable. Environmental benefits, for example, could flow from the smart management of resources.

Q7 **Gavin Robinson:** Thank you very much indeed. André, would you agree with that response from Emily? Is there anything that you wish to add? On scaleabilty, could you conceptualise for us, given the increased number of uses that there will be for the 5G network, what the consequences of network failure would be?

André Pienaar: Yes. When you think about cyber-security in the context of telecommunications, there are, at a high level, three aspects to think about: the supply chain, the security architecture and the operational practices. As Emily said, 5G is increasingly being virtualised—this is a general trend that we see in the telecommunication industry. We find that hardware equipment is being replaced by software in a process that we describe as virtualisation.

The second important area, which Emily highlighted, is the proliferation of 5G network infrastructure, for the reasons that I described in my earlier comments. That relates to the frequency bands that 5G will use.

The third area where 5G has national security and defence implications is the use cases to which it will be applied. Several countries, including China, are building their warfare doctrine on information dominance. In line with this thinking, the belligerent party that dominates the information on the battlefield and globally will be the winner of the wars of the future.

Many years ago, Winston Churchill said, "The empires of the future will be empires of the mind." The impact and ability of 5G not only to accelerate the speed at which data and information move, but to enable new areas of technology, like virtual reality and other use cases—for example, developing a common operational understanding on the battlefield—will give the edge to the countries and nations that have the ability to deploy 5G. This is a technology with some very significant national security and geopolitical implications.

Q8 **Chair:** Do you think we have become over-reliant on data and the movement of digital capability on the battlefield itself? It seems that there isn't a missile or weapons system that doesn't now rely on, let's say, GPS or some form of communications. Are you worried that we are over-exposed, given how vulnerable we could be if we do not have that ability to communicate with satellites and with our allies?

André Pienaar: Sharing common data and having a common view on what is happening in the theatre and on the battlefield have become critical and mission-important capabilities. The wars of the future will definitely be decided by access to data, the availability of data and the reliability and integrity of data. All of that emphasises and underlines the

importance of cyber-security, ensuring that we can continue to have access to the data, rely on the integrity of the data and have that data available at speed.

Q9 **Sarah Atherton:** Good morning. I have a question with two parts. Emily, you spoke about security risk and adversaries. Huawei, a high-risk vendor, has stated that it has developed a new robust security framework for telecoms, supported by the National Cyber Security Centre risk mitigation model and based upon the Government's new telecoms security requirements. Are we to take reassurance from that, given that Chinese law, in 2017, established that the state can compel companies to assist with intelligence?

Emily Taylor: Thank you for that question. One of the approaches that the British intelligence services have taken to Huawei, throughout their experience with Huawei in the UK going back to 2003, is risk management. Huawei has always been considered to be a high-risk vendor. It has always been considered that whatever any of the parties say, Chinese law and practice—as you put it in your question, national law in China—requires operators to share data with the Government. The approach of the National Cyber Security Centre has been to assume that those things would or could take place.

However, Huawei is here in the infrastructure. It is here in 4G and has been since 2003. The approach has been one of risk mitigation and risk management, to ensure that our people understand how the equipment is working and what its vulnerabilities and flaws are. The 2019 annual report from the Huawei Cyber Security Evaluation Centre made grim reading. Huawei clearly has a long distance to travel before the quality of its software and its cyber-security practices are deemed to be satisfactory. Those reports highlighted serious and systemic risks in its software and its cyber-security practices. Huawei has made promises of significant investment—billions of dollars—in updating its software core and resolving some of those concerns; it still has some way to go.

An evidence-based, pragmatic approach has been taken in this country, particularly over the past 10 years. None of us lives in a perfect world, and this is a classic case of looking for directions and saying, "I wouldn't start from here." But there aren't enough competitors in the market. Even if you decided today, "I don't want Huawei in this country," what will you do about all the 4G infrastructure that it is providing? How do you manage that risk? It is about taking evidence-based steps and ensuring that this country is reasonably satisfied that it understands the equipment that is being put into the ground and that the cyber-security practices are in focus, along with all the other elements that come together in purchasing decisions.

Q10 **Sarah Atherton:** Thank you, Emily. Perhaps the second half of my question could go to André. Huawei has been afforded 35% of the access network, albeit periphery at present. But I am unaware of where that 35% came from, which makes me question what is currently sensitive and what is non-sensitive, what is core and what is periphery. I then further

question how much of our vital Government communication is already undertaken on the peripheral network. I am obviously thinking there about our security and cyber-hacking. I wonder whether you have any observations, André?

André Pienaar: Yes. The National Cyber Security Centre has designated Huawei as a high-risk vendor and has set out compelling reasons why it has given Huawei that designation. One of the reasons is the fact that under China's national intelligence law, Chinese companies could be ordered to act in a way that is harmful to UK interests. The National Cyber Security Centre has also confirmed that the Chinese state and its associated actors carried out and will continue to carry out cyber-attacks against the UK and our national interests. Against this background, Huawei is excluded from all critical networks, that has both security and national security implications in the UK. GCHQ and the National Cyber Security Centre have accepted responsibility for managing that risk for us.

In terms of the 35% equipment market share allocation, the point of departure there is dealing with the reality that Huawei at the moment has the largest market share of telecommunications equipment in the UK, and trying to manage it downwards from there. The Defence Secretary has said that the goal is to manage high-risk vendors down to zero in future. As Emily said, that will require other players to come into the UK market, and given that we are using market dynamics as the principal lever here, they will have to come into the market with attractive pricing. Hopefully that will establish more diversity of choice for the telecommunications operators in the UK.

Chair: Thank you. We have three indications of questions, so we will go through those very quickly and then we will press on. I have Bob, Richard and Alicia. Bob, go ahead.

Q11 **Bob Seely:** Emily, you were talking about understanding the kit that has been put in. I have to say I was shocked when I spoke to a Government adviser on this who said that the Government could give guarantees on Huawei and China for seven years. That started a year ago. When the Government talk about guarantees, if you ask them how long those guarantees go for, they say another six years. That goes to the heart of what you are talking about, because other countries are saying, "Why take the technical risk when in 10 or 15 years' time we will not necessarily know how this kit works? We do not know what sixth generation looks like."

Emily Taylor: None of us do know the future, and all we can do is to try to prepare for it and to ensure that we are as well informed as possible. This country's Huawei Cyber Security Evaluation Centre is a good step and a welcome step. It is not perfect—it has been criticised in the past—but its governance has been improved in the past few years so that it is accountable directly to the National Cyber Security Centre. But yes, we do not know when 6G and the successive generations of mobile broadband will arrive or what they will look like when they do. When we are looking at how to build out the network and how to benefit from the social and

economic benefits that the new faster connections in mobile will bring, we have to look at the vendors. As André said, there is a real problem with the lack of competition for vendors, and I hope we will be exploring that in more detail in future questions, but building out national infrastructure does require the ability to meet the demands of scale.

Q12 **Bob Seely:** But on building out the kit, you could say, "Huawei is here anyway, therefore, we have to work with them." Again, that flies in the face of the Australian security signals agency and the Americans, all of whom say, "We don't know what it is going to look like. We can't deliver these guarantees." When you say the kit is here, if I understand correctly—this is a technical issue and I understand why some of your answers are more political interpretation, which is great—you can build somebody out of the network over a four to eight-year period, when that network is effectively replaced anyway and, indeed, much of the software is going to be replaced on an almost continual basis. Building out a high-risk supplier—again, "high-risk" is the phrase here—can be done reasonably efficiently over a five-to-eight-year period. That brings back the question, if other suppliers, such as Ericsson, Nokia in France, Fujitsu in Japan, and Samsung in Korea, can build these networks and they are low-risk contractors, why take the option of a high-risk contractor, unless it is fundamentally for political reasons?

Emily Taylor: Whether or not it is for political reasons, as you said in your question, Mr Seely, Huawei is here anyway. Even if we took the decision that 5G was not going to involve Huawei at all, because 5G technically will sit on top of existing infrastructure you are going to have to manage that high-risk vendor in the existing networks, at the moment and at least for the medium term. You are quite right that as technology improves, the infrastructure will need to be repaired, replaced and upgraded. As you said in your question, with a software-driven core a lot of that enhancement can possibly take place through upgrades in a virtual way, as we upgrade the software core.

There was one thing in your statement that I wanted to come back to: the situation in the US and Australia, which, as you say, have done outright bans of Huawei and ZTE. They are coming from a different base layer. They enacted bans on Huawei in 2012, so their existing infrastructure is not nearly as dependent on Huawei as ours is. Therefore, they are, if you like, more free to manoeuvre. However, everybody in the world has the problem of not many competitors to choose from in this market.

It is a bit like saying, "This operator is high risk and not secure. Therefore, another operator or another set of equipment is secure." We have heard from André and others that this is going to be a very difficult network to secure because of its complexity and because of the reliance on it. Also, if you choose to exclude one of three potential vendors then you are starting to create security risks, because what if one of those last two vendors fails? What if their stuff does not deliver on the security that you would want it to?

Bob Seely: Isn't the answer to that to—

Chair: Bob, we are going to have to make some progress; apologies.

Q13 **Richard Drax:** Emily and André, good morning to you both, and thank you for coming. Just quickly, Emily—to clarify to, I think, many—would it be possible to remove Huawei entirely from our existing network, how much could we remove now if we chose to do so, and how far behind are we to get in place an alternative that would be more vendor-friendly to the west?

Emily Taylor: Anything is possible. Huawei, for example, is present in some rural areas in the United States, and the United States is talking about a so-called "rip and replace" type of strategy. We have heard that Huawei provides a lot of infrastructure in this country at the moment, so the rip and replace would be not just for a small rural area; it would have to go throughout the country. That will be costly, and it will take a lot of time.

Of course, anything is possible; it depends on how the risk is balanced. However, technology markets do not just have first-mover advantage; for the first mover, it tends to be "winner takes all". If we decide that we are so unhappy with the idea of a high-risk vendor being in our infrastructure—despite the fact that that high-risk vendor has been in our infrastructure for the past 15 years—that we are going to delay our 5G until we have got every single last bit of Chinese equipment out of the country, it will bring economic and social risks.

It will also cause delays. We are a very innovative country. We have a very innovative tech sector. We are not so great at making the world-beating tech giants, but those industries will also be impacted by a delay in building out 5G. There are pros and cons to all of these things. Huawei has a lot of attention, and rightly so, but it is not the case that they are Chinese and that no other technology supply chain involves China. When you dig into most technology supply chains, you find China. If you are going to make national security type decisions based solely on the flag of the vendor, you are going to have to do a lot of digging right back into the supply chains and all the manufacturing of all vendors and try to root out China. It is not a "four legs good, two legs bad" equation. Huawei is often a lightning rod for justifiable concerns relating to how comfortable we feel about a technical world order in which the superpower is China and not the US, with all the western values that are embedded in its technologies. We are going to have face up to that. The UK's approach to date is quite evidence-based. The UK is saying, "Let's make sure we understand what sort of equipment we are putting into the ground, and that we manage those risks as far as possible".

Russia has conducted cyber-attacks on our mobile infrastructure. Russia did not provide any of the equipment, as far as I know, and you do not need to provide equipment in order to compromise it. We are living with cyber-attacks from bad actors all the time. Some of them are state-sponsored, some are not. They go into software flaws, complexity and poorly secured devices. We have to take a holistic view of the cyber security of this network. We must understand that it will never be

completely secure, but we need to think about our resilience and about managing that risk in the best practical way possible.

Chair: Thank you. Before I invite Alicia to ask a question, I will qualify something. DCMS have confirmed that there are essentially six global players; please say if your understanding is different. They are Ericsson, Nokia, NEC—essentially Fujitsu, based in Japan and only operating there—and then Samsung, which focusses on Korea alone, and the two Chinese companies which are ZTE and Huawei. So, the international choice for 5G is very limited indeed. There are three telecoms constructs in the UK: BT EE that uses Nokia and Huawei, Vodafone that uses Ericsson and Huawei, and O2 that uses Nokia and Ericsson. That summarises how limited the choice is for any country trying to do a 5G roll-out. It raises the question that you touched on: given China's growth and advance in global status, should we be doing what Beijing does and investing far more Government funds—similar to the American Apollo programme when we were racing to the moon—rather than just allowing the magic of the private sector to conjure up the results? Clearly, we are now falling behind. I will leave that there.

Q14 **Alicia Kearns:** Morning, André and Emily, and thank you for joining us. André, given that 2017 Chinese intelligence law requires all Chinese companies to comply with intelligence efforts if asked to do so by the Chinese state, and given China's goal of information dominance, as you discussed, does that indicate that it is relatively unimportant whether Huawei has access to the core or just the periphery, since any access will be exploited to gather and extract intelligence if so ordered by the Chinese state?

Chair: May I just issue a qualification to advance Alicia's question? The DCMS broke down the British infrastructure into four key parts: the transition networks, which are essentially the pipes, if you like, which Huawei is allowed into; the core, which they call the "brains", so the encryption, the payments, the tariff and so forth, which Huawei is not allowed into; the access network, essentially the radio masts, which it is already doing; and, finally, the management system, which is business support, which Huawei is not allowed to do. That, in crude terms, is the four parts of the 5G capability, of which Huawei is allowed currently into two.

André Pienaar: Alicia, thank you for the question. The National Cyber Security Centre highlights the risks associated with China's national intelligence law of 2017, which enables the Chinese state to order any Chinese company to act in a way that could be harmful to UK interests. More broadly, it is worth reflecting on the fact that Huawei is entirely different from the other players in the market that the Chair highlighted—Ericsson, Nokia, Cisco and Samsung—and it is different because of how Huawei is embedded in the Chinese state.

The founder of Huawei, Mr Ren Zhengfei, is of course a former engineer in the engineering corps of the People's Liberation Army, so he started his career in the People's Liberation Army. He became a member of the

Chinese Communist Party in 1978, and he has been a member of the Communist Party since. Recently, he was highlighted as one of the top 100 entrepreneurs in China on whom the Politburo of the Chinese Communist Party relies for the future of the party.

In the Chinese state, the Chinese Communist Party is embedded in all major corporations—like Huawei—that are considered to be national champions. It is calculated that the Chinese Government have financed the growth of Huawei with some $75 billion over the past three years to enable it to achieve the kind of market dominance it currently has in telecommunications equipment.

It is very hard to compare Huawei with the other players in the market, because that is comparing apples with pears. This entity has a completely different construct and make-up to what we consider to be independent companies with independent governance and independent shareholders. Huawei is embedded in the Chinese state, and that is why the National Cyber Security Centre for the first time has created this designation of a high-risk vendor and, so far, only named Huawei as a high-risk vendor embedded in UK infrastructure.

Chair: Alicia, any follow-up?

Alicia Kearns: No, not particularly. I think it highlights that, regardless of whether it is one point or four points, any access provides an opening. As Emily said earlier, once you have access to one thing, you will mole your way through to find access to others.

Q15 **Chair:** That is the difference between 5G and 4G. Emily wanted to come in.

Emily Taylor: I think yes, to an extent. If you compromise any device—if your printer at home gets compromised—that compromise will flow through to any access on your network that the printer enjoys. Part of the design of any network, particularly a national network, is to bear in mind that any compromise should only go so far and not create a systemic failure. The debates around where the core and the edge begin and end are very key to this debate.

Malcolm Turnbull, the former Prime Minister of Australia, said: "The core is no more" with 5G but, as I understand it, the way that the National Cyber Security Centre is approaching the core versus the access layer, or edge, is to say that while you might theoretically take the core—the intelligent bit, the brains of the system—right out to the edge, to the antennae, why would you ever want to do that? That would create a huge physical security headache for you as a network operator and, where these antennae go wrong or are vandalised, that would create massive vulnerability. The National Cyber Security Centre is saying yes, while in theory the two may blend, in practice they will not, for lots and lots of really good reasons. Therefore, it is safer to keep a high-risk vendor out of the brains of the network. It is feasible and plausible to do so as a way of managing risk.

Chair: Thank you, Emily. Emma wanted to come in, I think, and Stuart also.

Q16 **Mrs Lewell-Buck:** Thanks, Chair; I will be brief. Good morning, André and Emily. I'm understanding that removal of legacy equipment can probably never be 100% foolproof. With that in mind, is there any indication that China's national intelligence law has been used on existing parts of our network that Huawei are already embedded in?

André Pienaar: As the National Cyber Security Centre highlighted when it designated Huawei as a high-risk vendor, the Chinese state and its associated actors have carried out, and will continue to carry out, cyber-attacks against the UK. In our work with cyber security companies across the world, we see that on a daily basis.

These cyber-attacks include advanced surveillance to collect information about key individuals. It involves the theft of intellectual property on an unprecedented scale in the history of the global economy, and it involves in certain instances the disruption of capabilities and networks. It also involves the prepositioning of cyber weapons that do not get operationalised, but get prepositioned and placed for future use on networks. All of these activities by China and by companies and actors associated with the Chinese Government are of great concern to all of us in the cyber security industry, and I am sure they are also of great concern to GCHQ and the UK security services.

Chair: Stuart, did you want to come in?

Q17 **Stuart Anderson:** Yes, I did. Hello to you both, and thank you for coming today. I wanted to follow on from Alicia's point about the 2017 international law in China. Emily, you have said that everywhere, if you look deep enough, you can find China. Is there anything in Nokia and Ericsson where we would find China, and is there anything in their supply chain or the setup of their infrastructure where the 2017 international law in China would be pertinent to them as well?

Emily Taylor: Ericsson has a very long history of relationship with China. It has been established in China since the 1890s, and it has 50% market share in mobile communications and 10% in fixed networks in China. Its Nanjing factory offers, according to Ericsson's literature, "the most advanced manufacturing facilities in the world", producing 5G and 4G radio technology products, most of which support providers in China—most. In Jiangsu, there is a project called Robotechnik, a partnership with China Mobile in which Ericsson is providing 5G smart manufacturing.

Nokia, with China's FAW Group, is providing a 5G trial network for joint research on 5G and smart-connected cars in China, and it co-operates with FAW to develop 5G network slicing, which is going to be really important as 5G takes off in the future. Nokia uses facilities in China to make and assemble equipment for the US 5G market.

Q18 **Stuart Anderson:** Just a quick clarification: with the infrastructure that they've got in China, would they also fall under that 2017 international

law?

Emily Taylor: My understanding of the 2017 law is that it covers critical communications providers established in China, so to that extent, I think it would. That would be my understanding; it is not something that I have looked into deeply. André probably has more on that.

Q19 **Chair:** André?

André Pienaar: Any mobile phone operator that operates in China will be subject to control and access by the Chinese security apparatus, but this law is principally applicable abroad and in the UK to Chinese companies. China would not be able to use this law, for example, to compel Ericsson and Nokia to comply with this law in the UK. The foreign application of this law, the collection of foreign intelligence and the support of foreign intelligence operations into these laws, is only applicable to Chinese companies.

I think it is worth highlighting that, in addition to Nokia and Ericsson, there are other players in the market who I think will give the United Kingdom more choice in the future. There is Cisco, of course, which has been a long-standing and leading US company in this area. There is also NEC and Samsung, two very reliable Korean companies. At the moment, Samsung has about 3% of the global share of telecommunications equipment network.

The real drivers that would give the United Kingdom choice in the future will be the national building of new partnerships to enable innovation. European innovation opens up a whole range of new possibilities. I think building partnerships with the United States and reliable allies such as Korea, Japan, Singapore and India all open up new possibilities, not only for choice in terms of vendors, but also in terms of innovations. Emily highlighted in her remarks at the beginning of our conversations that software is eating everything, and the telecommunication industry is no exception.

At the moment, Huawei's dominant position as the leading network solution provider in terms of market share worldwide is very much premised on the fact that, with all the subsidies they are receiving from the Chinese state, they can sell their hardware equipment at a ridiculously low price point. Software, however, in the next three years will increasingly begin to replace hardware in the telecommunications industry. This will be transformative, because the high capital expenditure costs in building our hardware appliance to scale in the communications networks have always been a major hurdle to market entry for most players.

Software is now beginning to replace so much of the hardware equipment that it enables a whole range of new possibilities. For example, in Japan, the leading Japanese e-commerce player, Rakuten, has recently used a cloud platform to create and launch a virtualised 5G network. These innovative solutions will very significantly erode the global market dominance that Huawei and the Chinese state have accomplished in hardware and network solutions. The keys to the UK's national security

and future is in building new partnerships with reliable allies that are not conflicted with our national interest and in innovation.

Chair: Tan, over to you.

Q20 **Mr Dhesi:** Good morning, Emily and André. As you know, the UK Government have decided to limit Huawei to non-core functions and to cap it at 35%. What do you personally think of that decision?

Emily Taylor: I think that the UK had very little room for manoeuvre, given the reality of its 4G infrastructure and its long-standing relationship with Huawei. It also had a very difficult line to walk between managing this high-risk vendor and managing its relationship with key allies, notably the Five Eyes. The US and Australia have been extremely vocal in their opposition to using Huawei, so it was clear that the UK did not have the same flexibility to just get rid of Huawei in a way that was open to the US and Australia. The UK did not want to compromise the Five Eyes and other relationships. We had a situation where the US Secretary of State and the President were making overt statements that they would have to limit intelligence sharing with allies who chose Huawei. What do you do?

It was clear that the compromise position was reached with some reluctance. We were waiting for that decision for nearly a year. Meanwhile, the operators had started their commercial roll-outs of 5G in some cities in the UK. It is about really trying to walk a very thin line, which is: how do you manage Huawei, given that it currently has a large market share in the UK? How do you convince your allies that you are not just going to be opening up the intelligence of your network to, potentially, a foreign adversary? How do you make sure that you are not delaying or imposing cost on mobile operators who have not been as profitable in the last decade as their software counterparts? As André said, software companies—the US giants—have been making profits in the last 10 years that eclipse those of the mobile operators. It is not like the mobile operators have tons of money and they can just afford to dig up all existing infrastructure. It was a very constrained decision, and I think it was the least worst outcome.

Q21 **Mr Dhesi:** André, what do you think? Do you think it was a sensible decision?

André Pienaar: In the context of the UK, I think it was quite a dramatic intervention into the marketplace. Historically, we have had an open market in the UK, with very few red lines for foreign investors of any kind. Historically, our Government have spent very little time scrutinising the national security risks associated with foreign investment. For the UK Government to make an intervention, where they very clearly draw a red line around a particular foreign investor and very clearly state that they will not allow this foreign investor to increase its market share in the UK, in the context of how open our economy was, this was a very significant intervention.

Q22 **Mr Dhesi:** For a lay person like myself, can you explain the significance of 35%, or is that just a random number plucked out of the air?

Emily Taylor: My understanding is that it is quite close to Huawei's current market share. We talked about the different segments of the network. The Chair highlighted the transition layer; the core, or the brains of the network; the management system; the access layer - the antennae, the masts. André and I in our earlier statements talked about how the visible infrastructure is going to be vastly increased. We are going to have lots and lots of tiny antennae everywhere, like streetlamps, everywhere you could place them, because the range of these 5G signals is much lower than with its predecessor technologies. Given that the physical equipment at the edge is going to be a lot greater, the figure of 35% is consistent with that decision to say that Huawei can provide that kind of layer along with others, but not the core.

Q23 **Mr Dhesi:** André, can you please enlighten us further about the 35% figure?

André Pienaar: I wouldn't focus too much on the 35%. As Emily said, that percentage was largely derived from Huawei's current position in the marketplace, in terms of providing hardware to our telecommunications providers. The most important thing here is that the National Cyber Security Centre and GCHQ have drawn a red line around Huawei and said this is a high-risk vendor. Clearly, in a very open and transparent way, they outlined the reasons they designated Huawei as a high-risk vendor, and have made a very clear, firm statement that Huawei will not be allowed to increase its market share and increase its engagement beyond its current position.

Q24 **Mr Dhesi:** André, the last question from me is: does the fact that there are only a small number of viable suppliers in the UK, as you have highlighted, make the decision to include Huawei inevitable?

André Pienaar: As I think Emily said, Huawei is here—Huawei is in the United Kingdom, and it is a significant player in the marketplace. It is one of our largest providers of smartphones to consumers. It is involved in the economy in a number of ways, not just in our mobile phone network. Huawei is marketing cloud services and selling smartphones on the high street. The only viable way forward is to find innovative ways in which you can create new possibilities, which will create new choices and enable new vendors, in addition to the regulatory measures that the Government is taking. For example, the trusted and secure telecommunications Act has been passed recently in the US. The US Government will not provide any further Government funding for the procurement of Huawei hardware equipment, and the Government will also provide financing to small and medium-sized service providers that can play an active role in removing Huawei equipment. These kinds of legislative measures are other measures and steps that one could consider.

Chair: Thank you. I invite Stewart McDonald to come in, then Sarah.

Q25 **Stewart Malcolm McDonald:** Thank you, Chair, and I thank both witnesses for their contributions so far. Can I ask two follow-up questions? First, to go back slightly, a question to Emily. You mentioned the balancing

act of not compromising the United Kingdom's relationship with Five Eyes countries. To what extent do you think that relationship has been compromised? To speculate based on your expertise, will the relationship change going forward because of the decision that the UK Government has made? Secondly, when the Government announced the 35% cap, it actually said it would cap it at 35% and try to get the market share down. I want to ask both witnesses what kind of percentage the Government can reasonably expect to get it down to, and over what timescale.

Emily Taylor: To address your first point—to what extent has this decision compromised the strength of the Five Eyes relationship, the vital intelligence-sharing alliance with the US and other allies—it is very hard to know. It is the first time I have ever come across one member of the Five Eyes essentially threatening others over decisions about purchasing equipment. You have got pretty consistent and overt statements being made by very high-level members of the US Administration, saying that intelligence sharing will have to be limited. That is not just a one-off statement; it has been repeated by the US Secretary of State, the President and other officials. That has not quite caused the sort of shockwaves I would have expected from my conversations with members of the intelligence communities, because they view the relationships as extremely strong. They are very long lasting; they are often on a personal level and go back decades. This raises an interesting issue: why aren't the intelligence services more worried about it, given that the political statements are so binary? It could be a real threat, in which case we should all be worried. I think the US should be worried, because the UK is not just a recipient of information in that network; it is a contributor of information. Everybody is going to end up a bit less secure if that relationship is compromised. The US either mean it, or they don't mean it. If they don't mean it, why are they saying it? Also, if the political masters can say one thing and the intelligence services just carry on doing what they did before, it highlights another issue and other questions about accountability and whom everyone is answering to.

Q26 **Stewart Malcolm McDonald:** On the 35% share that the Government say they want to get down, to what extent do you think that is realistic? If it is, what sort of timescale and percentage can we expect?

Emily Taylor: I know André wants to come in on this, but very quickly before he does, I think it is realistic. What I am hearing from colleagues with connections with the mobile operators is that some of them are already actively starting to minimise their use of Huawei in new purchasing decisions, or also trying to get their networks throughout the European Union to a similar market share to the UK or getting Huawei out of core. It may be that the market does its own thing. I hope we come back to the market—André raised some really interesting points about that and where the market does not deliver security—but I know he wants to come in on this point.

André Pienaar: Stewart, on your question about the Five Eyes relationship, of course the Five Eyes relationship and Britain's role as a country that has some of the leading and most innovative intelligence

services in the world has been long established, and these are very deep relationships of trust. However, having said that, I think we should not underestimate the strength of feeling in Washington on this issue. China has changed its positioning in the world. Under Xi Jinping, it is quite clear that it aims to become the leading country in the world and that in becoming the leading country in the world it will impose new standards and new behaviours on the international system. This decision by the Chinese Communist Party continues to reverberate into every aspect of our lives. As a result, Washington has reassessed its relationship with China. All the debate and discussion that we are currently having about Huawei is part of that reassessment. It is as much driven by the new geopolitical realities of China's determination to be the ascendant power in the world as it is by the implications of new areas of technology.

In Washington there is a very broad bipartisan consensus that China is using every means at its disposal in its ascendant strategy, including its ability to reach into our societies through its telecommunications providers. This is a very strong bipartisan consensus politically. That is why someone like Nancy Pelosi, the Speaker in Congress, has spoken out about this issue and made statements about this issue. It is also a view that is very strongly held in the US national security community. We should not underestimate the level of conviction and the strength of feeling on this issue. There is a very clear view that this poses a threat not only to national security interests, but to issues we care about very deeply, like human rights and the treatment of minorities, and could pose a threat to democracy and the democratic values that we hold dear.

Q27 **Sarah Atherton:** The discussions around the 35% periphery presence raise concerns about the ambiguity in delineating core from periphery. Taking you back to my original point about China's national intelligence law of 2017, the NSCS have excluded the high-risk vendors Huawei from nuclear sites and military bases. To take you to a grassroots example, how much confidence do you have that the Huawei mobile technology used by, for example, contractors in Faslane will not be able to access sensitive data?

André Pienaar: I would definitely advise against using Huawei equipment in Faslane. Huawei equipment should not make its way into Faslane and should not make its way into critical aspects of our national defence and security infrastructure.

Emily Taylor: The difference between the core and the periphery is at the heart of your question. My understanding is that Huawei has always been excluded from highly sensitive networks, and it will be excluded from operating the brains of 5G. The question is: if you are anywhere on the network providing equipment, does this pose a security threat? Two things on that. While in theory the intelligent brains of the 5G network could extend right to the edge, where people interact with the network, in practice it won't. There is a ring around it, which you could plausibly describe as the periphery—as non-core, if you like. Whether or not you should be trusting Huawei to be part of the network in any case comes

back, I think, to, "Well, they are here already." The approach so far has been one of risk management.

To me, it is quite significant that, despite the strength of feeling that André described—it is bipartisan in the political layer in the United States—we have not really been given concrete examples of Huawei's overstepping the line in practice. While, for example, the 2019 Huawei Cyber Security Evaluation Centre report was extremely critical about the quality of Huawei's software and cyber-security practices—Dr Ian Levy of the NCSC called it "shoddy"—they went out of their way in that report to say that they see no evidence of collusion with the Chinese state. I would expect our intelligence services, which we have all spoken very highly of, to really be at the cutting edge of that knowledge, if there really was this firehose of data going. I am not saying that, because we haven't found it, it doesn't exist. The risk is clearly there, but given the long-standing relationship, we can look back on the history to date and see what has occurred. That should give us some measure of it. If we are not happy, we can be a little less concerned about it, perhaps.

I also think it is worth emphasising that you don't have to provide a network to compromise it. André has spoken about China's track record of conducting hostile cyber-attacks—primarily the theft of intellectual property, but also other cyber-attacks. We can anticipate that in the future. The ability, capability and will to do that are not necessarily completely tied with being an equipment provider or having links with an equipment provider.

Unfortunately, the market has not delivered good cyber-security practices throughout the ecosystem, and that is a major problem that we have to face up to as societies. The market actually rewards companies for being less secure, not more secure, so as long as those market conditions persist, it will always be possible for hostile state actors to compromise our systems, whether or not they provide them. Russia does not provide, as far as I know, any core equipment in networks in this country, and yet it has conducted attacks on our networks. Yes, we need to be aware of the cyber-security risks and manage them, but it does not follow that being a provider in the network necessarily means a greater cyber-security risk, because the levels of cyber-security are so low, unfortunately, that it is possible for states and bad actors to exploit vulnerabilities in any event.

Chair: Emily, you make a really interesting point there. I predict that Russia and China, over the next decade, are going to become closer and closer. To put it in cruder terms, Russia is going to become more subservient to China. They are good at cyber-attacks. If Russia understands the weaknesses, the vulnerabilities or the back doors that China provides, it can be Russia continuing to do those cyber-attacks at the behest of China. You can see where this potentially could go. I won't go any further down that avenue. John, do you want to take over the next question?

Q28 **John Spellar:** Thank you, Tobias. I think if Russia do that, they will find that they are riding the tiger, and we know what happens at the end of

that saga.

What I want to do in the question is to try and unravel this paradox—that we've declared Huawei to be a high-risk vendor. This is a very fast-moving industry, where companies either disappear or companies catch up very quickly. So, given that some of their equipment and practices have been described as shoddy, how far ahead is Huawei of its main competitors, such as Ericsson, Nokia and Samsung?

André Pienaar: Huawei's position in the marketplace has really been determined by its ability to sell solution network products at a ridiculously low price point, and in this regard they have really specialised in selling hardware equipment at a ridiculously low price point. They were able to achieve these price points effectively through subsidising the sale of their equipment, because of the extent to which the Chinese Government have been subsidising their operations. Earlier, I mentioned an estimate of some $75 billion in recent years.

So, the whole go-to-market strategy of Huawei is very different from that of the other players in the marketplace, because of the extent to which it is embedded in the Chinese state, and the fact that they go to market with a whole range of instruments of statecraft that the Chinese Government deploy alongside Huawei. And certainly in Africa, that involves corruption.

That is really the reason why we are grappling with Huawei today. They have achieved this very significant market share very quickly, because they have gone to market in a completely different way to the other players. That has enabled them to achieve this level of market dominance in hardware products.

Looking towards the future, however, I think there is now an awareness and an understanding of how Huawei and its sister company, ZTE, operate and how they go to market, and there is a high level of awareness, certainly in legislatures and in Governments around the world, within the Five Eyes community and within Europe.

Secondly, there are a whole range of new areas of innovation opening up. When you think about the power of 5G, we shouldn't see it in isolation. We should see it within the context of the growth of cloud computing, within the context of the onset of quantum computing and within the context of the integration of space in the terrestrial economy. And all these areas of innovation mean that there are new possibilities to create market share, to bring new players into the market share and to have diversity of choice.

Therefore, the key recommendation that I want to give this Committee is to think about how the United Kingdom can build new partnerships and new alliances, and about how the United Kingdom can focus and double down on one of the great strengths of our country, which is innovation, to give our country diversity of choice as we develop the key technologies to give our people quality of life in the future.

Q29 **John Spellar:** Can I be clear that what you are saying is that Huawei are not technically advanced—so it's not a case of the other companies having

to catch up, and they have the technical capability—and effectively Huawei are establishing their position because of the complacency of Governments' short-term attitude to companies, and in fact they are probably in breach of dumping regulations by putting the equipment cheaply on the market? So, instead of welcoming them in, we should in fact be taking them to the World Trade Organisation, which they joined, but unfortunately Governments have not been holding them to account under the rules and practices of the World Trade Organisation.

André Pienaar: I agree with your assessment.

Chair: Emily?

Emily Taylor: If I can just add a few remarks to what André has said, it's a bit of both, as usual. Huawei says that it has 96,000 employees engaged in R&D, and I think that we should—

Chair: Sorry, Emily, can I interrupt you there? We are going to begin the minute's silence to remember those key workers who have lost their lives at this time. We are a few seconds ahead—it will begin at 11 o'clock—but we will pause now.

The Committee observed a minute's silence.

Chair: Thank you all for joining in an important recognition of the work that our key workers are doing at this critical time.

Emily, do you want to continue?

Emily Taylor: Huawei has made substantial investments in research and development, and this can be seen as part of China's Made in China 2025 strategy to go from being an imitator to an innovator, particularly in technology. Huawei also had 19% growth in revenue during 2019, and when you consider all the things that happened to Huawei during 2019, that is quite remarkable.

Huawei has signed 90 commercial contracts for 5G around the world and says that it has shipped more than 600,000 base stations. That compares with Nokia's 69 commercial contracts in 20 countries and Ericsson's 89 commercial contracts and 31 live networks across 17 countries. So Huawei is doing well; so are others. It is shipping a lot of kit. It is investing a lot more in research and development than its competitors are able to do. This goes to the remarks that André was making about the conditions in which Huawei is operating, and there are two elements that I would like to add to those thoughts.

One is China's role in the Belt and Road initiative and technology equipment's role as part of the currency of the Belt and Road. China has been extremely generous in building out networks in Africa. There is never any such thing as a free lunch, and when these countries get into difficulties, we start to see the strategy revealed. For example, when Sri Lanka was having trouble repaying debts, China assumed shares in a strategic port as part of debt forgiveness. Mexico was offered a very

generous loan on 1% interest, on the condition that 80% of it was spent with Huawei. So we see that technology build-out is very much forming part of the Belt and Road strategy—a patient, sustained strategy that has been conducted over decades.

I would also like to highlight that China is extremely active in technical standards, particularly through the United Nations, and it is putting significant resources into multiple study groups. It should also be a wake-up call to Western countries that have been relying on the market to sort these things out that that investment, that consistency, that level of participation in the technical standards bodies, particularly in the United Nations, has to be backed up by countries that have perhaps a different vision of the future networks and communication systems.

Chair: John, does that answer your question?

John Spellar: Yes, thank you very much.

Q30 **Chair:** Can I probe that a bit further? Is the kit actually any better? When I speak to Ericsson and other operators, they say that they just market themselves better. There is this myth that goes around Parliament and in the debates that we have here, that they are six months to a year ahead in their technology capabilities. Ericsson dispute that. They simply make the kit far cheaper and it is the price attraction that overrides any capability. Would you agree with that?

Emily Taylor: I think that is right. The price point is very attractive. That is my understanding as well. You also have the assessments that have been made independently of Huawei's kit, which is that it is not of the highest quality. Now, what we are lacking is that independent public assessment of all of the operators' equipment; then we would be able to make side-by-side comparisons. Huawei has always been treated differently and has higher levels of scrutiny. That is really useful and in fact means that Huawei has to lay open things that other companies would not normally naturally do, unless they were compelled to do so.

Chair: Thank you. I know Bob Seely wants to come in, and Mark Francois. Bob first.

Bob Seely: Tobias, do you want me to ask the question about core vs periphery, or do you think that we have gone down that route?

Chair: We have sort of covered it. Do you want to come in on this point now?

Q31 **Bob Seely:** Yes, I would like to, but I would also like to give a quote from the Australian Signals Directorate to our guest.

Let me just follow up the questions from John and from you, Chair. There seem to be two premises, which are either false and we need to agree that they are false, or we need to accept are real and explore them. The first is that Huawei is an intellectual leader. Both speakers have said that that is not the case and it goes largely on price. André also said it is also

potentially corruption and belt and road and Chinese political pressure.

The second canard may be that there is no other option but to use Huawei. I just want to check very concisely with the guests whether that is or is not the case. In France, I understand that Nokia and Ericsson are building 5G networks without Huawei, as are NEC in Japan, without Huawei, and Samsung in South Korea, without Huawei. So the idea that we cannot build a 5G network without Huawei is not correct. Can I just check that with the experts?

André Pienaar: May I just finish off the point about the quality of Huawei's product? The National Cyber Security Centre has clearly stated that Huawei's cyber-security engineering is of a low quality and its processes are opaque. So from a cyber-security perspective, Huawei is right at the bottom of the range of quality of product and quality of solution. The question there is whether that is because of mass production and because the work is of a shoddy nature, or whether there are other more sinister reasons for that. I think Huawei has gained an unfair competitive advantage because of the extent to which it has received state subsidies and the extent to which China has placed its statecraft behind its go-to-market strategy.

In terms of whether it is possible to build a 5G network without Huawei—of course. As we said at the outset, we will see many more 5G networks being built at local level and as private networks, and perhaps that would be the best way to launch 5G—not to roll it out at the national level, but to begin by building out 5G networks locally around smart cities, around smart military bases. That certainly would be possible. There are a whole range of solutions in the marketplace that enable you to do that, without using Huawei equipment.

Emily Taylor: So, on your two premises. Is Huawei an intellectual leader? No, however, it is attractive on price. There is also a benefit in having vendor diversity in a highly consolidated market. Therefore, there is a point where having a lack of diversity in your equipment provision creates its own security risks.

Secondly, is there no option but Huawei? Yes and no. Obviously you can build out your 5G network with other vendors. The reality in the UK is that the early 5G development will be sitting on top of existing 4G, and Huawei is very present in our 4G infrastructure, so unless you want to rip out and replace existing infrastructure, you are stuck with Huawei for the foreseeable future.

Just on the point of looking to the future, we have done a lot of "How did we get to where we are?" and "Isn't it terrible?", but I would like to build on André's remarks about the need to shake up the equipment provision market. There is exciting work and a lot of investment going ahead particularly to create the so-called OpenRAN (Open Radio Access Network), which is to have interoperable equipment which could prevent that sort of vendor lock-in that we are all sitting here worrying what to do about. Significant investment is going into OpenRAN start-ups in the UK

and also in other countries, and there have been some trials. This would potentially drive prices right down and give entry points for new vendors into the market, which is very much needed.

Just one last point. The role of software in the 5G environment will also potentially bring very capable vendors into the mobile broadband market: for example, some of the major cloud providers.

Chair: Bob, do you want to reply very quickly, please? We have three other people wanting to come in here.

Q32 **Bob Seely:** I want to ask André if he agrees with the former director general of the Australian Signals Directorate—their Cheltenham—Mike Burgess, who said "the distinction between core and edge collapses in 5G networks. That means that a potential threat anywhere in the network will be a threat to the whole network". From a technical point of view, do you agree or disagree with that?

André Pienaar: I think that assessment from the director of the Australian Signals Directorate will be accurate in the future. As Emily said, at the moment when we build out our 5G network, we will be building it off the existing 4G LTE network. In that context, we can still see a distinction between core and edge. In the future, however, as we proliferate these micro-cells to give us the higher band of radio frequency, we will see the distinction between edge and core increasingly disappearing. We will see more edge computing, for example, connected to the micro-cells and more data being processed where it originates. In that context, in the future the distinction between edge and core will disappear. I think we are five or six years away from that in terms of having it as an infrastructure reality, but that is certainly where 5G is heading.

Chair: Okay. Three people want to make short points: Mark, Emma and Alicia. Mark, go ahead.

Q33 **Mr Francois:** Thank you, Chairman. I did indicate earlier that I have to go at 11.15, but I would like to ask a quick question. Chairman, you indicated earlier that of the six global providers of this kit, two are Chinese, two are Asian and two are Scandinavian. The thing I have never understood is that, as America is still the most powerful and, in many ways, technologically advanced economy on Earth, why is there no American national champion in this market that we could source from if we chose to? Why aren't the Yanks major players in this?

Chair: I think the Prime Minister may have indicated this to President Trump when he was encouraging us not to engage with Huawei. The question is: where is your offering? André, do you want to start off with this?

André Pienaar: The US has focused very significantly on its software economy because there was a policy belief that lower cost manufacturing in China is attractive. That has allowed China to make significant gains in its technology supply network. However, I think that is not a position that

is locked in. The US is one of the most innovative countries in the world and what we are seeing is that Cisco, a long-established player in this marketplace, is stepping up its game. Cisco has a significant part of the global market share and is a very reliable provider of equipment. Of course, it cannot compete with Huawei on price, but it is a very reliable partner as a solution network provider.

Secondly, we have seen a combination between the major telecommunications players in the US market and the major cloud computing companies, so all the US telecommunications providers have announced partnerships with the major players in the cloud computing market—Microsoft, Amazon and Google. As Emily said, the future of telecommunication is in open radio access networks, virtualised networks, where software replaces hardware. I think the US will leapfrog what China has done in this space in the next three to five years.

Q34 **Mr Francois:** I think that is very important. We are going to have American options for software, and I think the Chairman said that O2 use a joint Scandinavian solution for hardware, so, as a layman, as there is no domestic UK champion, I suppose one option for the hardware would be to go down the Scandinavian route. But is it practicable that within three to five years, given what you have just said, there might be an American option as well?

André Pienaar: There will be an American option, but we could also create a British option. We should encourage British companies and British software developers and enable them to focus on how we can contribute to the future of the telecommunications industry. Britain has one of the most vibrant and innovative software industries in the world and one of the most vibrant and innovative start-up sectors in the world. We are the leader in Europe in this space and we should focus how our own companies can contribute. The fact that the entry hurdles to the telecommunications market will be lowered in future because of the extent to which software replaces hardware brings all sorts of interesting and exciting possibilities.

Q35 **Mr Francois:** Just to pursue this quickly before I go, is an Anglo-American solution a credible alternative within a three to five-year timeframe?

André Pienaar: An Anglo-American solution that involves our allies in Asia such as Japan and Korea, yes. I think the future—not only in the telecommunications space, but when it comes to clean energy or space—is building an alliance that is focused on the UK, the US, Japan and Korea.

Mr Francois: That is a very important point. Chairman, I think I will quit while I'm ahead. Thank you very much.

Chair: Thank you, Mark, that is much appreciated. Alicia, did you have a question on this issue?

Q36 **Alicia Kearns:** Yes, André, you stated that the quality of the Huawei product is not of the highest standard. Am I right that you then went on to suggest that there could be a strategic intent to that, to create or enable

entry points for hostile interventions and intentions?

André Pienaar: Yes. I quoted the National Cyber Security Centre's statement on Huawei as a high-risk vendor, in which they said that the engineering quality of their cyber-security is very low and the processes behind it are very opaque. Best practice today in cyber-security is to have very high levels of transparency around your programming and to have the highest standards, because we all take cyber-security so seriously. We do not know why Huawei are so shoddy in their cyber-security engineering. One possibility could be that they just do not care about it and it is not important to them; that might be related to the price point at which they sell their product.

Another suggestion could be that they are deliberately shoddy about it and that they are deliberately opening up back doors and possibilities for cyber-security breaches and incidents. I think it depends on your view of the world; I would certainly be highly circumspect and highly suspicious about why anyone, in this day and age where cyber-security is so important, would be so shoddy, so much at the low end and so opaque about the way in which they do their cyber-security. It would certainly make me very wary and very cautious. We would certainly not advise anyone to open themselves up to this area of vulnerability.

Alicia Kearns: Thank you. The last one certainly has grave implications.

Emily Taylor: If I may, I will just add a few remarks to that. I would not run away with the idea that those faults are deliberately placed in it. Do not forget that Huawei is also providing equipment in other markets, such as China. In cyber-security, the worst example is when you create a vulnerability and then it is used against you. A vulnerability can be used against anybody who is using the equipment, including the home team, if you like.

One of the major failings in the market is that software companies are not rewarded in any way for having secure practices and thoroughly testing their software. The market does not reward that; the market rewards getting out to market quickly, doing things cheaply and having lots of features.

Huawei started life as an equipment manufacturer. We are beginning to see this more and more as the internet of things comes on stream. We work with the Internet of Things Security Foundation. There you have people who have spent their entire careers making stuff meeting people who are building software. It is a complete culture clash. People who are in manufacturing have secure and highly mechanised processes that they can repeat and that they have documented. Software is a much more agile, scrummy and messy world.

One of the things that policy makers really need to focus on is, if you cannot rely on the market to create the incentives you need to raise the level of cyber-hygiene and good practice, what is the role of regulation in doing that? We cannot go on with the situation we have with buggy

software. We know about Huawei's bugs because it lays open its code; other software providers do not do that.

Q37 **Alicia Kearns:** Is it not the case, though, that we have no way of ascertaining whether the equipment and approach it takes with its domestic product differs from that which it exports, and when it sends individuals in the last 10 days of an installation of a Huawei project, we are not allowed to interrogate them or ascertain what they are doing to that product?

Emily Taylor: You make an extremely valid point. I think that is totally right.

Chair: We need to make some progress. I want to go back briefly to the OpenRAN point made earlier. Richard Drax, do you want to explore this further?

Q38 **Richard Drax:** Thank you. Could you explain, for me and many others watching this session, what exactly OpenRAN is? I understand it is a virtualised 5G introduced by a Japanese online giant. We have heard you say that the virtualised 5G would not be so reliant on one vendor. How would that help us break free of Huawei, if it could, in the future?

Emily Taylor: The idea of open radio access network (OpenRAN) technology is that it would provide commoditised hardware into the 5G market. The main thing about commoditised hardware is, first, that it is cheaper. Secondly, it is interoperable, so you do not have the vendor locking—are you a Huawei house or an Ericsson house?—but these bits of kit would all talk to each other openly.

That would expand the supplier options beyond the traditional players that we have seen, so it is a great opportunity for innovation and for new players to enter the market. Vodafone and Telefónica have been investing in this technology. The work is ongoing. Trials are ongoing. The reports are positive about it. As we look to the future, we must understand how we got here and why that was, in many ways, not optimal, but we also need to look to the future with excitement regarding the opportunities that that could bring to diversify the supply chain. We are where we are because we don't have a diversified supply chain and the alternatives are very costly, so, where people are making resource-constrained decisions about investment, they are choosing the cheapest option in some way.

I feel quite excited about OpenRAN as a potential way out of the situation we are in. Of course, where software is embedded into a network in a way that we have not seen before, there are all sorts of possibilities that we probably haven't thought of for innovation and new players to join in that market.

Q39 **Richard Drax:** Forgive me, Emily, being a novice, but would this new system, OpenRAN, negate the need for masts in every street, because we would be more reliant on software than on hardware? Have I misunderstood that?

Emily Taylor: No, it would not negate the need for masts on every street, because part of how the 5G technology works is by operating on very high frequencies in the spectrum, which means that it cannot transmit as far. You cannot have a mega base station that just operates on a wide area; the range of each of these devices, these antennae, will be much lower, so you will still need a lot of stuff. It is who provides it, how much it costs and whether it works with other people's stuff.

Chair: Thank you. Bob has been waving, wanting to catch your attention. A quick question, then we will move on to Martin, please.

Q40 **Bob Seely:** Specifically for André, but maybe for Emily as well, following up on the OpenRAN point, Huawei has I understand resisted OpenRAN, and its tech is badly interoperable, as we have seen. This may be obvious, but why does a vendor ensure its non-interoperability with others—why does it ensure locking with them?—and is that not a potential danger in future, both politically and technically, of going with operators that are very unfriendly to interoperability?

André Pienaar: The open radio access network possibilities really favour the strength of British innovation and the innovation of our allies, because it is dependent on, first, the use of cloud computing, which is the industrialised ability to deploy computing power connected to fibre networks, as we see from Amazon Web Services, Microsoft, IBM, Google and other major cloud computing players. Rakuten, the leading player in the launch of ORAN networks, has grown out of the cloud computing and e-commerce space. It used that significant computing power to build virtualised networks, which replace hardware with software.

There are so many advantages to this form of innovation. First, it plays to the strength of our own economy and those of our allies. Secondly, it is software-based and we do not have the tie-in in with the black box hardware solutions that Huawei is marketing at us. Thirdly, we can set higher standards of cyber-security. I want to come back to this point about cyber-security and the shoddy nature of Huawei cyber-security. In this day and age, there is no excuse for a company with global aspirations to be shoddy about cyber-security.

Q41 **Bob Seely:** What about black box?

André Pienaar: Or to be drawing on a black box proprietary solution when we have very little insight of the processes underlying it—the creation of that technology, how it is operated, and the functionality of that technology.

One of the other reasons why Huawei is different from the other players in this marketplace is that it also sells us smartphones, is consumer facing, on our high streets and markets cloud computing services to our major enterprises and to Governments, in addition to being a network solutions provider. Huawei has a responsibility for its cyber-security because it is consumer facing—it has that responsibility under our own Data Protection Acts in the UK and under the GDPR, and with regard to the privacy of our

consumers—so there is no excuse for a global company today, which is consumer facing, to be shoddy about its cyber-security.

Chair: Thank you, André. I now turn to Martin.

Q42 **Martin Docherty-Hughes:** I thank both witnesses. I think they will probably agree with my question: I am just looking for some practical answers as to how the UK Government can take steps practically to increase the numbers of vendors in the UK. I may have a couple of follow-ups to that.

Emily Taylor: Part of what the UK Government can do to proactively increase the number of vendors is encourage the kind of investment in new technologies that André and I have both been talking about, and also to work very closely with the mobile operators who are actually making the purchasing decisions, as they do. I feel that while we all like to criticise the Government and the arms of the state, the management of the Huawei issue has been quite well done in the UK: it has been evidence-based and cautious. Looking to the future, there is definitely a need for more vendor diversity.

To Bob Seely's point, Huawei would not be the first incumbent to resist open technologies. For me, as an internet person coming into the world of mobile telecoms, the internet in a way was originally created to prevent a lot of the vendor lock-in—the throttling by patents and intellectual property—that besets the telecommunications market. Introducing interoperability and open standards does a lot to encourage and foster innovation and competition, and also a lot more transparency, a lot less black box and a lot more scrutiny. However, I would be the first person to say that the internet is not trouble-free; it just replaces, in some cases, one set of problems with a different set of problems.

Q43 **Martin Docherty-Hughes:** André, did you want to come in there?

André Pienaar: Britain is a world leader in cyber-security. We are one of the best centres of excellence in the world in cyber-security, and many countries rely and depend on Britain for their cyber-security. One of the reasons why Britain is a leader in this field is because of the quality of our intelligence services, and the quality of people, innovation and investment that is happening in our intelligence services and in GCHQ as one of the world leaders.

The work that GCHQ is doing to keep Britain safe and to keep our cyber-security safe; the innovative model that we have created in establishing the National Cyber Security Centre; the partnerships that the security community has, working with the private sector—all of those are making very valuable contributions to keep our country and our people safe. In front of this Committee, I want to recognise not only the contribution made by our armed services but also that made by our national security community to keep us safe on a daily basis, and in particular at this time to keep our healthcare sector safe, which is coming under massive cyber-attack in the midst of this pandemic.

Q44 **Martin Docherty-Hughes:** If I could maybe ask some brief follow-ups, Chair, we talk about how we are so forward in terms of innovation. A lot of that will also be to do with the academic institutions across the whole of the United Kingdom of Great Britain and Northern Ireland, and we have a vast number of EU nationals participating in that. Neither of you has mentioned the fact that we are about to leave the European Union, which may have a detrimental impact on that academic knowledge.

I am wondering whether you maybe want to say something on how we can improve vendor access when Ericsson and Nokia, for example, are within the single market, where we already have an existing trade agreement with South Korea in terms of Samsung. We will need to have a new trade agreement with South Korea, and of course a Brexit process that actually has a physical trade agreement. My concern about some of the discourse so far is that we have been talking about the software capability from Cisco in the United States, but our defence structure is already dollar-dominated. How are we going to be able to afford that in a post-pandemic world?

André Pienaar: You have posed some tough questions there, but you have highlighted the very important role that our universities have to play in innovation and providing talent, both for the telecommunications sector and the technology sector more broadly. Nurturing and fostering these centres of excellence that we have in the United Kingdom, which are world class, is of crucial importance. Being able to attract talent from all over the world is also of crucial importance for the open nature and the growth of our economy.

Emily Taylor: Whatever the arrangements that are in place for trade, and our relationship with Europe and the rest of the world, technology markets are inherently global. The supply chains that we have been talking about this morning are global in nature, so it is up to policy makers to ensure that those markets are kept as open as possible, and that additional barriers are not put in place as a result of these changes that further inhibit competition, or that inhibit intelligence sharing. Our intelligence sharing networks with the Five Eyes are really important to national security, but so is our intelligence sharing with European partners. In a lot of ways, our telecommunications markets are more similar to European partners than to the United States.

There are many challenges ahead after we emerge from this pandemic. I echo what André said about the role of the intelligence services keeping us safe, particularly decrying the cyber-attacks against healthcare institutions during the pandemic. It just highlights how vulnerable many of our systems are, particularly in non-technology sectors such as healthcare. Healthcare was also massively affected by the WannaCry cyber-attack in 2017. Whatever the challenges ahead, it is up to policy makers to ensure that the markets are kept as open as possible and that investment still flows, particularly into new and emerging technologies.

Q45 **Chair:** We are coming to the end of our time. Stepping back from Huawei itself—the reason we are focusing on Huawei is as much about the country

that is behind Huawei as it is the company itself—I just wonder whether in the last couple of minutes you could share your thoughts on the direction of travel. What is China's agenda here, given that they are growing technologically, militarily and economically more superior every single day? Huawei is just one part of that factor.

André Pienaar: The leadership of China has clearly stated its ambition to be the leading country in the world and, as part of that, to influence the international architecture and determine the values that will underlie it, down to the standards that we apply to new areas of technology. It is very important for Britain to continue to be a world leader and to be a force for good in the world, and for Britain to continue to play a leading role in not only asserting our values in our foreign policy and in our relationship with our allies but, in a very practical way, helping to set international standards for key areas of technology such as 5G, in the correct international fora.

Britain should continue to nurture and foster our own areas of innovation, our own venture capital and our own start-up community, and continue to invest in the national security infrastructure of our own country. We should think about that in a very open-minded way to see where there are possibilities for innovation and possibilities to build new alliances and new partnerships. That will determine the security and the future of the British people.

Emily Taylor: For the past two decades, we have become accustomed to US dominance in technology markets, which has led to an idea, or even a complacency, that technological standards and technology are neutral. For us, the values and attitudes of the people who build the technology are fairly similar to our own and they flow through into things that are open and interoperable, and support freedom of expression and fundamental rights.

China is quite clearly well down a path where its ambition is one of international technical dominance. There, we will all have to cope with standards, technologies and equipment created by a superpower that does not share our values. Technology is not neutral, and we really have to confront this when it comes to China being the world leader. Of course, Chinese ambitions in this sphere are in a way aided by the fact that at the moment the US is a rather erratic partner at times and is in a way ceding that international space to another party.

If you want to look ahead at what China has in store for us, do take a close look at what is going on in international standards development and, in particular, China's development of so-called New IP, in which Huawei plays an active and central role and which would be a fundamental re-architecting of the way the internet works, in ways that we can expect to benefit Chinese political ambitions.

Q46 **Chair:** The concern I have there is this. If China is to become an ever more dominant world leader, but it is developing its own standards and, as you say, the west is perhaps not united in challenging those standards and

has become risk-averse, there is a worry as to the direction of travel and where this takes us to. It's almost a split, if you like, in world standards, whereby China benefits from a rules-based order, which is eroding all the time, and it doesn't want to assume the responsibility of a superpower, knowing that it can't honour the standards that superpowers should be upholding, for the benefit of the rest of the world.

Emily Taylor: Yes, I agree. I agree with your characterisation: the west has not been as proactive or on the ball on this as it should have been. But probably, when push comes to shove, the west would oppose that sort of splintering. Where I see the main risk area is in developing countries, recipients of Chinese aid and technology, of the Belt and Road, where developing countries are being given technology infrastructure equipment for free. Their alternative is not having the equipment at all, and if it comes with certain characteristics or carries with it certain ways of behaving—well, what's the choice, really? I think that this is where the west has to step up and think about what the alternative offer is and what the strategy is, because those developing countries will determine whether we continue on the same network.

Q47 **Chair:** The Government have chosen to slide back the integrated review. André, you mentioned that the United States is developing a different security relationship with China. Should Britain do the same? Should we be looking at China through a different prism? And do you think that if we did that, our agencies, when they made their assessment of the threat from China, might come out with different recommendations as to our involvement with companies such as Huawei?

André Pienaar: I think the statement made by the National Cyber Security Centre on Huawei is very clear. The National Cyber Security Centre highlights three areas of risk. One is the current market position that Huawei has. It highlights the poor quality of the cyber-security that is being deployed in its products. And it highlights the behaviour of the Chinese state towards the UK national interest in cyber-attacks. I think those statements are all factual and accurate and that, following the current pandemic, many, many countries will reassess and re-evaluate this relationship with China.

At a very practical level, 5G matters to the Defence Committee because data is required to keep our war fighters safe in theatre in the wars of the future. That is regardless of China. We have to ensure that our war fighters have accurate data, timely data and immediate access to data and have a clear vision of the battlefields of the future, and only 5G, alongside the other key areas of technology like cloud computing and space, will be able to enable that. We have a responsibility towards our war fighters to keep them safe on the battlefield with data access. That is why 5G and Britain having access to reliable 5G is of critical importance for our defence in the future. That is regardless of China, and in any situation.

Chair: Thank you. André, you have paid tribute to our armed forces and what they do and to the agencies keeping us safe. The Defence Committee would very much concur with and support those comments. Let me thank

you, André and Emily, for joining us here today. I also say thank you to our Foreign Affairs Committee colleagues for joining us; they have been most welcome. It has been a very illuminating session. We will be exploring the aspect that you, André, last touched on—the importance of cyber-security for the future of defence—in later sessions, but for the moment, I again thank both of you for your contribution today. It is very much appreciated. I thank Committee members as well. That brings this session to a close.