HOUSE OF COMMONS

# Science and Technology Committee

## Oral evidence: UK telecommunications infrastructure, HC 2200

Monday 10 June 2019

Ordered by the House of Commons to be published on 10 June 2019.

Watch the meeting

Members present: Norman Lamb (Chair); Vicky Ford; Bill Grant; Darren Jones; Stephen Metcalfe; Carol Monaghan; Damien Moore; Graham Stringer; Martin Whitfield.

Dr Julian Lewis, Chair of the Defence Committee, also attended.

Questions 1-248

## Witnesses

I: Professor Rahim Tafazolli, Head of the Institute for Communication Systems, University of Surrey, Professor Andrew Martin, University of Oxford, and Professor Alf Zugenmaier, Munich University of Applied Sciences.

II: John Suffolk, Global Cyber Security and Privacy Officer, Huawei.

III: Mikko Karikytö, Head of Network Security, Ericsson, and Steve Sampson, Head of Technology, Nokia UK & Ireland.

IV: Alex Towers, Director of Policy and Public Affairs, BT Group, Brendan O'Reilly, Chief Technology Officer, O2, Patrick Binchy, Chief Technology Officer, Three, and Scott Petty, Chief Technology Officer, Vodafone.

# Examination of witnesses

Witnesses: Professor Rahim Tafazolli, Professor Andrew Martin and Professor Alf Zugenmaier.

Q1 **Chair:** Welcome to all three of you. Thank you for coming to give evidence this afternoon. I will ask you to introduce yourselves; could you also say whether you have any financial interests that you want to declare? First, do any members of the Committee want to declare any financial interests at this stage?

**Darren Jones:** I have a relatively long list. I used to advise BT, Three, O2 and EE as a lawyer and latterly worked as a legal counsel at BT. My wife also works there. I co-chair the all-party group on PICTFOR, a technology forum, which has Huawei as a sponsor, including at events in previous years. A couple of years before my election, I visited Huawei in China on a Foreign Office and British Council delegation, but I can confirm I am not employed by the Chinese state.

Q2 **Chair:** Thank you. Can I ask the panel to introduce themselves and offer any declarations? We will start with Professor Martin.

***Professor Martin:*** My name is Andrew Martin. I am professor of systems security in the department of computer science in the University of Oxford. I do research on hardware and software security, and how you build secure systems out of components that may or may not be trustworthy. I also lead cross-disciplinary action activity in the university that looks at cyber-security in the round as a socio-technical problem, so I talk to lawyers, politicians, business people and a bunch of others. I do not think I have any relevant interests to declare. I told your researcher about all my funding sources, but I do not think they are very relevant.

**Chair:** But the funding sources are not relevant to this.

***Professor Martin:*** I don't think so.

***Professor Tafazolli:*** Good afternoon. I am Regius Professor Rahim Tafazolli, director of the Institute of Communication Systems and founder and director of the 5G Innovation Centre at the University of Surrey. I have more than 30 years of experience in 2G, 3G, 4G, satcom and 5G. To declare my interest: I and my team work on research and innovation with everybody.

**Chair:** Are there any funding issues that you need to declare?

***Professor Tafazolli:*** No.[1]

[1] To note: Professor Tafazolli has since written to declare industry funding for the 5G Innovation Centre of which he is the Director, which has sponsors including Huawei, EE, O2, Vodafone, AirCom, BBC, BT, Cobham, Fujitsu, Rohde & Schwarz and Samsung. Full details can be found at www.surrey.ac.uk/5gic/members/network.

***Professor Zugenmaier:*** My name is Alf Zugenmaier. I am a professor at Munich University of Applied Sciences. I believe I got invited because I consult for NTT Docomo in the 3GPP standardisation group in the security working group. There I was the rapporteur for 5G security specification and also for SCAS—at that time it was called SECAM: security assurance methodology. As I said, I do consulting for NTT Docomo, which is a Japanese cellphone operator. Other than that, there is nothing.

Q3 **Chair:** Thanks very much. By way of guidance, we have a lot to get through this afternoon. Don't feel you all have to respond to every question if others have given an acceptable answer as far you are concerned.

What is the damage that we are talking about in terms of the impact on national security resulting from an attack on a 5G network? What is the concern we are focused on here?

***Professor Tafazolli:*** We need to bear in mind that 5G has been rolled out, with EE and others. It very much depends on the core technology that 4G has. It is bigger, faster and more powerful than 4G is, but it runs mainly on the core technology that 4G has. So if there is any security threat that 4G has, 5G will inherit that.

Q4 **Chair:** But is the potential damage greater with 5G than with 4G?

***Professor Tafazolli:*** I do not see why it should be greater, because in the next three or four years the mobile broadband aspect of 5G is being introduced. In probably three or four years, when 5G will serve the mission-critical industry applications, the reliability and security resilience, mainly of the network, becomes more important.

Q5 **Chair:** Presumably an attack three or four years down the track could have more significant consequences than now.

***Professor Tafazolli:*** Let me elaborate on that. I wrote an article for *The House* magazine published two weeks ago; the title was "5G is more secure than 4G". and then in simple language I explained why. It is for a number of reasons: the 5G architecture is layered, the service layer, the network function architecture layer, the core network, and the radio access network. There are different layers where different security mechanisms can be applied and enforced. At the same time, it manages the services much more flexibly. The authentication from the users' identification has a more enhanced version than 4G has. The network, for the next three or four years, will be operated as non-standalone, which means 5G has to ride on the back of the 4G network. When it is standalone, the security mechanism will hopefully be enhanced and will then be an end-to-end sort of security and resilience.

Q6 **Chair:** Professor Martin, you seemed to be nodding when I suggested that three to four years down the track, the potential damage could be greater with 5G compared with 4G.

***Professor Martin:*** That would be my expectation, yes, in that if more and more applications use such a technology, our reliance on it will go up, whether in smart cities or autonomous vehicles.

Q7 **Chair:** Could you paint a picture of the sort of damage that could be done with an effective attack on a 5G network further down the track?

***Professor Martin:*** Let us suppose we have a smart city full of autonomous vehicles. With the right kind of attack, I could inhibit their operation in some way, whether by causing them to stop, to go in the wrong direction or to collide with each other. Potentially, I could do that in a very targeted way if I had enough control of the network.

Q8 **Chair:** That is the sort of thing to fear if we get this wrong. Is that right?

***Professor Martin:*** I would think so, yes.

Q9 **Chair:** If the information communicated over a 5G network is encrypted, what scope is there for equipment suppliers to enable espionage?

***Professor Martin:*** That very much depends on who is doing the encryption and where it is.

Q10 **Chair:** Could you explain that?

***Professor Martin:*** Many will be familiar with the concept of end-to-end encryption that you see in Signal, WhatsApp and other communications tools. There, you are relatively safe against bad behaviour by the network, because the encryption happens in your terminal and device and gets decrypted only at the other end. But many communications technologies and current mobile phone technologies involve point-to-point encryption, where nobody eavesdropping on your radio signal may be able to intercept it, but within the network itself, the signal may not necessarily be encrypted or it may be encrypted under the control of someone other than the end points, and so is much more subject to interception at that level.

Q11 **Carol Monaghan:** You said that autonomous vehicles, for example, may be affected. Is that because we are moving towards a situation where there will be more autonomous vehicles out there, or is it simply because it is going to be a different type of network?

***Professor Martin:*** The intention is that we build more and more different applications that rely on this kind of network.

Q12 **Carol Monaghan:** So it is do with the applications rather than the network itself?

***Professor Martin:*** I believe so—my colleagues here know more about 5G than me, but that is my understanding.

***Professor Tafazolli:*** I would like to highlight that in the scenario where we have autonomous driving or a connected cars environment, they will not be operated only be one network. In the UK, we have four network operators, so each of them will be responsible for different aspects and different networks. It is not as though, if there is a security issue or attack

on the network, the whole car and transport system on motorways will stop—that is impossible. In a way, it is security by isolation, so the surface attack on security is minimised by having more players running and operating the network.

Q13 **Chair:** So diversity is helpful?

***Professor Tafazolli:*** Absolutely.

**Stephen Metcalfe:** Is the risk the same with 4G in the autonomous vehicle example? From what I am hearing across the whole piece, 5G is based on 4G; the risks are the same. Why was there such outcry when we were told that 5G might be underpinned by technology that we are already using, and was that just being whipped up by the media? On the ability to hack in to, say, a range of autonomous vehicles, presumably if we were still using 4G, the risks would be the same. Those are two separate points.

**Professor Tafazolli:** I believe that the risk will be the same as 4G in non-standalone operation of connected vehicles. When it comes to standalone architecture—when the core network is specific for 5G, which at the moment is being standardised but is not deployed yet—one of the aspects of the 5G core is reliability. There is a huge amount of emphasis on the connections being reliable and available in the order of 99.999%—five 9s at least—of the time. No system—no network—has ever been designed and operated with such high reliability. That reliability has to be tested so that, for example, when cars travel at 70 mph on the motorway, the connection does not break down.

Q14 **Stephen Metcalfe:** Except that an autonomous vehicle—we are using that as an example—should not be dependent. It should be totally autonomous; it should not be dependent on being connected. If it feels that it is being hacked into, it should have a system that says, "I'm going to ignore all external information and just rely on my radar, sensors, sonar, lidar," or whatever else is driving it. The danger is that if we put out this idea that the system or your car can be hacked, we will put the development of the technology back quite quickly.

***Professor Tafazolli:*** Absolutely.

***Professor Martin:*** Yes, that is a fair point. It is a straw man example here, but we shouldn't put too much on to that particular example. The general sense of having lots of communicating devices and disrupting their operation is the more important point.

Q15 **Chair:** There is a lot of talk in the media about core and non-core parts of the system. Can we still make that distinction with 5G as we could with 4G? Alf, you are nodding.

***Professor Zugenmaier:*** To use a technical term, you have the radio access network, which encompasses the radio link, and the connection that goes to what is called the core network, where the core functions are located. It is called the core network, but given what we will maybe see

one day—mobile edge computing—the core network, as defined by the functions, may be moving out closer to the cell sites.

Q16 **Chair:** Does that mean that the distinction becomes more blurred?

***Professor Zugenmaier:*** If you are talking about geographic location, yes, but if you are talking about the actual function, it is very clear what functions are core network and which are access network.

Q17 **Chair:** So in the future it would remain possible to exclude a particular company from the core, just as it is now possible? The blurring geographically does not prevent you from excluding particular providers from the core.

***Professor Zugenmaier:*** Yes, and that depends on what you want to achieve by exclusion. We are now seeing a shift from boxes that you unpack, plug cables into and put somewhere, to virtual network functions that run on hardware that is sold decoupled from the function itself. Now you have the question, where do you want to exclude your manufacturers from? Do you want to exclude them from the hardware as well?

Q18 **Chair:** Suppose you want to exclude them from the bits that might cause concern in terms of national security.

***Professor Zugenmaier:*** Okay. If you understand which bits those are, yes, you could mandate certain deployments.

Q19 **Chair:** Can you minimise risk by excluding any provider that one is concerned about from all those core functions with 5G?

***Professor Tafazolli:*** Yes. There is a clear distinction between core and radio access networks wired through a unified interface, which is standardised in the 3GPP standardisation. We know where the boundary is between core and radio access technology. That is done purposely so operators have the option of buying the core from one vendor and radio access from other vendors. They can inter-operate with each other from that point of view. That flexibility has always been there in 4G and 3G—not so much in 2G, but from 3G onwards.

Q20 **Chair:** Under 4G, there has been advice to networks to protect the core from national security concerns. It has been, as I understand it, quite a varied picture about which networks include providers from China, for example. Do you think there should be a clearer ability, through regulation, to require networks to exclude any provider causing concern from recall?

***Professor Tafazolli:*** There is already provision in the standards. As long as all the vendors—it doesn't matter where they are or in which part of the world—follow and comply with the standards, their radio, core and mobile phones should be able to interwork with each other.

Q21 **Chair:** Bluntly, my understanding is that some networks have Huawei equipment in the core of their networks. Does that need to change? Do we need to be able to require networks to exclude from the core, if we have a particular national security concern?

***Professor Tafazolli:*** Can I elaborate on that? We are talking about vendors. Vendors sell equipment, hardware and software, but most of the responsibility is on the shoulders of the network operators. When they buy their equipment and they deploy it, they have to make sure that each node as well as the whole network is secure and operated securely—

Q22 **Chair:** But should Government be able to require networks to exclude?

***Professor Tafazolli:*** I think they have not met with operators, especially the four operators you have in the UK; most of them have been operating the networks for more than 30 years. They know how to manage the situation and to operate the system.

Q23 **Chair:** So we just leave it for the networks to determine our national security?

***Professor Tafazolli:*** I believe so.

Q24 **Chair:** Is that you view, Professor Martin?

***Professor Martin:*** That level of detail for 5G is outside my expertise.

Q25 **Stephen Metcalfe:** Back in 2010, the Huawei Cyber Security Evaluation Centre was established, with a view to checking and looking for major vulnerabilities in both the hardware and the software. In one of the early versions of the system there were 1 million lines of code; in the current system there are hundreds of millions of lines of code. How reasonable is it to expect an organisation to be able to evaluate that hardware and software?

***Professor Martin:*** I looked up the numbers and I believe the evaluation centre has 38 staff. If a multi-billion pound business could improve its security to the point of not having any problems with 38 staff, I am sure they would all do it.

Q26 **Stephen Metcalfe:** Yes. Anything further? Judging by that comment, can anyone do it?

***Professor Martin:*** Eliminating vulnerabilities is the stuff that all software and hardware vendors are endlessly trying to do; it is exceedingly difficult. Looking at someone else's code to find vulnerabilities is particularly difficult. The report from the evaluation centre seems to say that in the case of the work they have been doing, it is—I have forgotten what the word used was; not chaotic, but something approaching that. Looking for vulnerabilities is like shooting fish in a barrel—there are plenty to find. Proving to yourself that there are none is hypothetically impossible anyway.

Q27 **Stephen Metcalfe:** Is it a pointless exercise?

***Professor Martin:*** No, because the whole point of that centre, and other similar activities, is to build your level of assurance that you know what is going on.

Q28 **Stephen Metcalfe:** It is better to have some level of assurance than none.

***Professor Martin:*** Yes, or to know that you should not have any assurance, but to rate it and to be able to make an informed decision.

***Professor Tafazolli:*** I wanted to bring your attention to this: 3GPP, through a security assurance process, are defining each node and how it should be tested for 5G—we have similar specifications and processes for 4G but not for 5G yet; it is being developed—and what the processes are for each device in the network that needs to be tested for security assurance. Also, the GSMA is coming up with the verification test and certification of the network nodes to be tested through the independent test labs; that needs to be done. I am pleased to say that this process is being defined. It is not fully defined yet, but more than 50 operators are involved in that. More than five vendors are involved in that specification—helping 3GPP, which are global standards, as well as GSMA, to have a process of testing each piece of network equipment. But I cannot comment on the human factor.

Q29 **Stephen Metcalfe:** Once you have gained that security assurance yourself, through looking at code or whatever process you use, how do you ensure that what is deployed matches what you have evaluated?

***Professor Tafazolli:*** That is the point I mentioned: it is not only the vendor's responsibility; it is the network operator's responsibility as well. In the UK we are quite fortunate in that most of our network operators have been in this business for more than 30 years, and security was as important in 2G as it is today.

Q30 **Stephen Metcalfe:** One final quick question. As you do this evaluation—as you go through the code and look at the process—how easy is it to distinguish between what may be the inclusion of an inadvertent security flaw and a deliberate backdoor? Are there very obvious differences? Not being someone who would be able to code in either of those, I wondered about that. Does it become obvious?

***Professor Martin:*** I think if you were designing a backdoor, your very first task would be to make it look like a mistake. If you were halfway competent, that is certainly what you would do, and there would be no way to tell whether it was a mistake or deliberate.

Q31 **Stephen Metcalfe:** So that is the answer.

***Professor Martin:*** A deliberate mistake would look like a mistake, yes. You could, I suppose, design something that was easier to exploit, but that would be almost the proverbial smoking gun, so I do not think you would do that. You would make it look like a mistake.

Q32 **Stephen Metcalfe:** Does anyone disagree or want to comment further on that?

***Professor Tafazolli*** *indicated dissent.*

***Professor Zugenmaier*** *indicated dissent.*

Q33 **Dr Julian Lewis:** Could I just ask you if I would be right to summarise

the situation with self-driving cars, for example, as follows? Is it basically the case that we are building new systems that are more and more dependent on a technology that cannot really be safeguarded? Would it be anyone's role in society to ensure that, if we were involved in some sort of conflict with an adversary that was able to exploit those vulnerabilities and close down those systems, we would have some sort of fall-back so that, if we did not have self-driving cars, we could still drive cars ourselves?

***Professor Martin:*** Guided by the previous comment, I think we should be careful about using cars as an example. Indeed, my colleagues who work on autonomous cars say that they certainly need to design the safety so that the car is actually autonomous and not reliant on the network. But to the general point, yes, we are building a society that is more and more dependent on network functions. If we were ever in a situation of conflict, we might discover that all sorts of unexpected things stopped working.

Q34 **Dr Julian Lewis:** Whose responsibility is it to plan for that?

***Professor Martin:*** I think it falls on a lot of people, but ultimately is it a matter of critical national infrastructure, I suppose, and for those who take responsibility for such things.

Q35 **Dr Julian Lewis:** I would have thought it was a Government responsibility rather than one of private companies. Talking of private companies, if we were in a conflict with an adversary, would there be any greater danger arising from our dealing with a firm like Huawei, for example, than from our dealing with a firm from another country with which we were in a less adversarial relationship? Or would the vulnerabilities be the same irrespective?

***Professor Martin:*** That has a very complex set of answers, because we are talking about global supply chains. We may be dealing with one vendor, but they may get their components from another place. Indeed, the vulnerabilities within any particular piece of equipment may not be under the control of the management of the vendor in question anyway; there may be some other party who wants to sell them to a third party. It is going to be a very complex picture behind the scenes.

Q36 **Dr Julian Lewis:** Let me give one final example. We have just been talking about backdoors dressed up to look like vulnerabilities. Would there be a greater chance of an adversary knowing where these backdoors or exploitable vulnerabilities were if they had been involved in constructing the system than if they had not?

***Professor Martin:*** The designer and constructor of a system is always in a much better position, yes.

**Chair:** Professor Zugenmaier, do you have any comments on that?

***Professor Zugenmaier:*** Yes. In this discussion about 5G, people are ignoring that it is all happening on top of IP technology—the technology we use for internet routing, so you also have all the IP routers in your network, even in the core. So if you think of 5G as what is defined by the

3GPP, a lot of the functions are not really visible because they are underlying.

Another thing that needs to be considered when discussing this, especially when looking at the complex supply chains, is that your supply chain is not just linear; you need all the compilers and so on and libraries at many different stages. So if you really wanted to subvert some function, there are many places where you could do so.

There is also the question whether the label on the top of the box and the country of origin will give you assurance that what you are getting is actually what you hoped for—namely, a reliable product. Very often, it is also a matter of how much money you are willing to spend on your security functions and features. If you tell a manufacturer, "I would like to have a product which is next to free," maybe you can get some functionality, but you have to ask yourself: what quality are you getting? Security is a quality of product. So if you are trying to save money, you have to consider where money can be saved.

Q37 **Chair:** I should have said that we are pleased to have Julian, the Chair of the Defence Select Committee, with us for this session. I apologise; I should have introduced you at the start, Julian.

On Julian's point about it ultimately being Government's responsibility to protect the state from attack, should the Government require networks to exclude providers and suppliers from the core in 5G to improve protection in terms of national security?

***Professor Zugenmaier:*** It depends. First, why would you have that only for the 5G core and not other places as well?

Q38 **Chair:** Potentially other places as well, but should Government play a stronger role in requiring networks to act in a way consistent with national security?

***Professor Zugenmaier:*** I would take the stance that if there are smoking guns or evidence that certain products do not fulfil the requirements, it does not help you if you have bought something from, say, a US vendor and you find there is a hard-coded password in it as a backdoor as opposed to getting something from another country. So if Governments are worried about the security of networks, it would make more sense for them to have requirements on the quality of security than on a label on a box that says "shipped from".

**Chair:** Understood. Thank you.

Q39 **Bill Grant:** I am very much a layperson, but I am sensing that somebody has to take responsibility for identifying the risks that will be known and the perceived risk. When you put out the specification to a contractor, and I believe there may be only three contractors capable of fulfilling the 5G roll-out, is it clearly the Government's responsibility to identify the risk to the system and embed that in the specification put out to tender for the persons to install it? Is it wholly a Government responsibility?

***Professor Martin:*** Wholly is a strong word but, certainly, Government sets regulations to make sure we cannot blow ourselves up with badly made engines. I do not see any reason why Government should not make similar regulations to make sure that someone else cannot blow us up with badly made networks.

Q40 **Bill Grant:** It seems to me that amount of traffic that would flow in 5G is far more significant than in 4G, and therefore the risks of being able to interfere with or damage that system rise in line with the traffic that flows.

***Professor Martin:*** Yes. On one level, it is merely a commercial contract between the user and their network provider, but if we are going to rely on that network for all manner of public goods, as we seem to be, it surely is part of the function of Government to protect us all.

**Bill Grant:** To identify the risk and engineer that risk out in the specification.

***Professor Martin:*** Yes.

Q41 **Darren Jones:** I want to go back a little to when we were talking about core and edge, to explore a little what weight would be given in a risk assessment to the physical security of a base station. My understanding is that in previous iterations in 2G, 3G and perhaps 4G, the base station might be physically secure in a locked exchange that someone such as Openreach might manage, and the access points will be external to that and connecting in. I think that we heard earlier is that in 5G capabilities, that base station technology is moving out towards the edge, into locations that might not be physically secure in the traditional sense of an exchange. If that is the case, what is the weight of a risk assessment of tampering access if the base station is somewhere else, compared with just the interface between the two?

***Professor Zugenmaier:*** I think it is the other way around. In 4G, the base stations were moved out to the cell site, closer to the antenna, while in 5G there is the possibility of having a distributed central unit split where the distributed unit would be closer to the antenna, and the central unit can be moved further towards physically protected processing sites. We are slowly moving that point further in again. The interesting part is that the way that the encryption is specified is that it starts at the mobile and at least for the encryption that is specified for the 5G system, if you were to use it without anything on top, your encryption would terminate in the central unit of the radio access network. Afterwards, you would re-encrypt and have hop-by-hop security, as was mentioned earlier, to have an IP set connection to the core network. Within the core network, you can have those IP set connections. That is deployment-specific, whether you do that within one data centre or not. If it leaves your network, it is without any protection, unless the communicating party puts in a layer of encryption on top.

***Professor Tafazolli:*** Bear in mind that there are two major parts to the edge. One is just the antenna—for us an amplifier—because we need more

of those for the purpose of coverage. There is no intelligence there and each covers an area of 200 or 300 metres. If one of them goes down, only the coverage for about 200 or 300 metres goes down. Most of the intelligence aspect goes on inside the network. That could be in an area that manages a number of remote radio heads, which were referred to. Each of them cannot be responsible for all the network. There are many of them inside the network, and each of them is responsible for a geographical area. If there is an attack, it will knock down the coverage in a small area.

Q42 **Darren Jones:** That already happens in 4G, so we already have this—they are not all locked up in our exchange building.

***Professor Tafazolli:*** Yes.

Q43 **Darren Jones:** You will have read and heard that a lot of the political concern is about the Chinese state's ability to influence or direct Chinese-owned companies. Do we know whether the supply chains of non-Huawei competitors—Ericsson, Nokia and others—are free of any other Chinese companies?

***Professor Tafazolli:*** It does not matter who the vendor is; most of the equipment comes from China on the hardware side. The supply chain comes from China, India and other countries where the human resources are not that expensive. It is a global business. It is not that vendor A only makes the products in their own country. That is why the supply chain is quite sophisticated and complicated. When everything is put together, which is the responsibility of the vendor, with their own brand on it, it needs to go through the process of security assurance as a whole. Once it meets the certificate, it can go to the next step. It does not matter what the supply chain that puts everything together do. That process of certification is being defined which will be in place before the end of this year.

Q44 **Darren Jones:** If our concern is that there could be interference at some point in the supply chain, it does not actually matter whether you end up going with Huawei, Nokia or Ericsson, because at some point, from the bottom to the top, that risk exists between all three.

***Professor Tafazolli*** *indicated assent.*

***Professor Martin:*** I think it might be an overstatement to say that it doesn't matter, in that, each of those vendors is ultimately responsible for the products that they sell and they are supposed to assure their supply chain. The question comes back to how much assurance you have that they are indeed exploring their supply chain correctly.

Q45 **Darren Jones:** Can you illustrate what that looks like?

***Professor Martin:*** Hundreds of components or thousands of components.

***Professor Zugenmaier:*** If you think about compilers, maybe it goes back 50 years, because one compiler is used to build the next one, which is used to build the next one. This is what I was alluding to earlier. It is not

just a linear supply chain in which you extract ore, make chips and so on, but you somehow have to build on something that allows you to create a chip. You have to use development tools to create software, so your supply chain becomes more like a tree than a simple chain.

In theory—it gets more difficult to put something in the further you are from the finished products—you could have problems anywhere along there. You may have heard that when Huawei was put on to the list of companies you could no longer export US technology to, people started saying, "Oh it could be that Huawei phones are now becoming less secure," because they couldn't get the software updates from Google anymore, to update the software that was on the phone—just to make clear how complicated the supply chains are these days. As you said, at the end the person who puts the label on at least they should stand for the quality with their name.

**Darren Jones:** It is hundreds of companies and it is built on legacy technology, so it is quite complicated, I suppose.

***All witnesses*** *indicated assent.*

Q46 **Darren Jones:** My last question for this section is trying to understand the difference between an unlawful interception from a technology company and a third-party attacker, whether a state or a terrorist group, whatever it might be. Is there any significant difference in terms of an attacker's ability to interfere with the network, based on the fact that they have provided an aerial or a bit of technology, compared to a country, for example?

***Professor Tafazolli:*** In the mobile networks, most of the cyber-security threats are denial of service attacks. It is not so much about stealing people's information or whatever. They try to bring down the network by stealing some of the services. I think that amounts to about 70% of the total cyber-attacks—at least, a couple of years ago those were the sorts of numbers.

The user data security is quite robust. It goes through encryption and different security mechanisms, which are managed by the network operators, because at the end of the day it is extremely important to the operator's business to keep that security and the privacy of customers' information. Attacks happen—we have seen attacks on the internet, for the denial of service. We saw the attacks to the NHS, because a different version of the software was not upgraded in time. That sort of thing is quite common. To minimise these attacks in 5G or 4G+, whatever is distributed, the functionality is not all in one place—not geographically and not even logically. There is a separation between the service architecture and network function architecture and between the core network and radio access network. In a way, it is security by isolation; and it is better in 5G than 4G was.

Q47 **Chair:** Do you conclude from that that the risks of using Huawei, in a controlled way, are manageable? That's the critical question.

***Professor Tafazolli:*** Everything is manageable, provided that the actors in the chain—the supply chain, the vendors and the operators—do their job properly.

Q48 **Chair:** Do you agree with that, Professor Zugenmaier?

***Professor Zugenmaier:*** I think we are missing whoever is relying on the application. If our application relies on 100% availability of the network or on any sort of quality that the network does not provide, we will run into difficulties. If you think of this as network operations, we sort of understand where we are, but people may believe that the network has different qualities from what is actually in the contract and they may not provide for contingencies or for problems that can occur anytime. You could have major flooding somewhere and have a major power outage. It doesn't matter what the availability was supposed to be before; suddenly it's not there because there is no power. There are lots of other things that you may need to consider when society starts to depend on an infrastructure. The network may work as designed, yes, but in terms of the applications, society depends on the network in various ways. In terms of the resilience of the society, you would always have to think, "What would we do if this didn't work?"

Q49 **Chair:** Taking all that into account, and given that in this country at the moment there is a big debate about whether we should follow what the Americans are arguing that we should do—exclude Huawei—or include them but manage the risk, what is your conclusion?

***Professor Zugenmaier:*** I would always argue for trying to manage the risk, and if the outcome of the risk management study is to exclude certain vendors from certain points, that's it, but I am more of a technologist; I'm not a politician, so I can't really say that because there is a country of origin—

Q50 **Chair:** But your understanding of technology allows you to understand whether there is a threat to national security.

***Professor Zugenmaier:*** There are threats to national security that are beyond technology. As long as it's within the realm of technology, I think I can understand, but when it goes beyond that, it's outside my area of expertise.

Q51 **Chair:** But your view overall is: manage the risk.

***Professor Zugenmaier:*** Yes.

Q52 **Chair:** Professor Martin, you wanted to comment on the question that Darren had asked.

***Professor Martin:*** Yes. This is an evolving situation. Historically, telecoms operators have been a little bit separate from the rest of the internet security cabal. Relatively few people—academics or hackers—have looked at the security of telecom networks, because the equipment is expensive and it's just hard to get your hands on things. That is evolving very quickly, partly because these new technologies are much more

software based, cloud based and so on and partly because more people are paying attention. It's clear that when you do pay attention, you find all sorts of nasties in many products. That is perhaps a cause for alarm.

On the question "Who should you trust?", I was quite shocked by reading the report of the security evaluation centre and the rather damning words there about the quality of the software engineering in the products, because if you do expose those to a large number of hackers you will get a large number of vulnerabilities found by who knows whom. That may apply to other vendors, and you would have to ask those who do evaluations to comment on those vendors, but I would tread very carefully.

**Martin Whitfield:** I just want to explore another aspect of the transparency in this image of a tree that you have given, which is really about funding and the input of funding into academic research in the UK. I know that Oxford University expressed concern at the beginning of this year; they were not going to pursue new funding opportunities with Huawei and gave reason for it, principally over public concerns. So my opening question is this: how significant is Huawei's funding to academic bodies with regard to 5G research in the UK?

***Professor Martin:*** Well, it is not significant to us at the moment.

***Professor Tafazolli:*** In the 5G Innovation Centre, Huawei is one of the industry partners among many; I believe that there are 25 different global industry partners. All the UK operators are investing in this; all of them are here. They are investing in research on 5G, together with Huawei, Samsung, Sony, Fujitsu and many other companies. So that money—the funding—is important and we use it not only for us to do research but to support UK small and medium-sized companies to come and use our test-bed that we have developed, in order for their product to be internationally competitive. This is extremely important; we have more than 55 UK SMEs that utilise the facility that we have to advance their products. So I would say research and innovation, short and medium term to long term, is extremely important for our own prosperity.

Q53 **Martin Whitfield:** It makes sense that the companies that are most interested in 5G are the ones that will invest in the academic research to drive their research and development.

***Professor Tafazolli:*** On R&D, we have many good UK SMEs that are developing games or applications, or simply making a beautiful antenna, for example, but they want us to test whether their solution actually works end-to-end for 5G and where they stand compared with other companies internationally. So from that point of view it is not just funding university research but many ecosystems within the country are important.

Q54 **Martin Whitfield:** I think it is right to say that Huawei, with regard to the University of Surrey, is a platinum-level funder, which I have read somewhere was $7.5 million. Would that figure be right?

***Professor Tafazolli:*** Yes. It is £5 million sterling.

Q55 **Martin Whitfield:** £5 million sterling? Oh, well, there we go.

***Professor Tafazolli:*** And they are platinum members, the same as Vodafone and EE are platinum members, and they are among many different platinum members, and we have many different gold members.

Q56 **Martin Whitfield:** Would it be right to say that the platinum members are the biggest players in the field, because obviously—?

***Professor Tafazolli:*** Because they give us more money.

Q57 **Martin Whitfield:** They give you more money—yes, absolutely. The question that follows from that is: is there any pressure on academics to downplay any aspect? Obviously the aspect we are looking at today is security. Because of the funding source, is there pressure on academics to change their view or defend a position that they may not otherwise support?

***Professor Tafazolli:*** It is important—extremely important—for us as an academic institute to be impartial. I have been in advanced research for more than 30 years and I work with all the manufacturers—the old ones, as well as the new ones—and all the UK operators, not only within the country but also in Europe and elsewhere. One important aspect to realise, which I always tell our guys and friends and colleagues, is impartiality.

We are not religious about any particular technology. Our job in the 5G Innovation Centre is to tell the truth—the technical truth: what is the art of possibility? Then the industry will take it up, package it and shape it, decide whether it should be standardised or not. That is the mission that we cannot deviate from, and that requires funding.

Q58 **Martin Whitfield:** I presume, Professor Martin, that you would agree on academic independence—the right to say what is academically correct?

***Professor Martin:*** Of course that is always our objective, but equally I am aware that there is nobody completely objective in this world. In other contexts, when I have had funding from vendors for particular work on particular technologies, I have become more familiar with their narrative around the technology, and that must affect the way I talk about it. Even if I am aiming to be objective, I can't know that I am.

**Martin Whitfield:** I appreciate that.

**Chair:** Thank you all very much indeed for your time this afternoon; it is really appreciated.

## Examination of witness

Witness: John Suffolk.

Q59 **Chair:** Welcome. Thank you very much. I think you were here from the start, so you probably heard that we have a routine of asking about any financial interests. Is there anything you want to declare beyond your

position representing Huawei?

***John Suffolk:*** None whatsoever, Chair.

Q60 **Chair:** Thank you very much indeed. I will start the questions, if I may. What services are included in Huawei's safe city projects?

***John Suffolk:*** Safe city is just a generic term for cities in particular to look at how they can improve their efficiency or safety. It might include traffic light control or CCTV systems. It depends what the objectives of a particular city are. Safe city is not one standard set of tools, processes or outcomes; it is very variable, depending on what your objective is.

Q61 **Chair:** You will be aware of the Australian Strategic Policy Institute report, which suggested that Huawei's products have often been deployed in countries with poor records of political stability, rule of law and corruption. It also stated that in some countries, public security technologies have "created a range of political and capacity problems, including alleged corruption; missing money and opaque deals; operational and ongoing maintenance problems; and alleged national security concerns." Do you accept that?

***John Suffolk:*** No. Our point on this is really quite simple. Our starting point in the 170 countries in which we operate is: what is the law, and what does the law define as acceptable and unacceptable? I think it is right for Governments to determine, in essence, their objectives and enshrine that in law.

Q62 **Chair:** So if it is a dodgy regime, you will go with it?

***John Suffolk:*** I don't think it matters whether it is a dodgy regime; it matters what is in the law. We do not create any moral judgments on what we think is right or wrong. That is for lawmakers to do. We execute within the law in 170 countries.

Q63 **Chair:** On that point about moral judgment, what products and services do you provide for local government in Xinjiang province?

***John Suffolk:*** That is not actually one of our projects; it is done via a third party. Typically, what we would provide is a range of data centres or storage, and then it is for that third party to put that into whatever the package is that they are trying to offer for their particular customer.

Q64 **Chair:** But do you have products and services in Xinjiang province in terms of some sort of contractual relationship with the provincial government?

***John Suffolk:*** Our contracts are with the third parties. It is not something we do directly.

Q65 **Chair:** I see. So there is an intermediary, but your products and services end up there?

***John Suffolk:*** Yes. Typically on a safe city, as I said earlier, it is not one thing. You might find there are 100 or 200 different vendors in, all providing a little bit. While Huawei appears to be quite a large company, it

is not possible for us to provide 100% of all technology solutions for all situations.

Q66 **Chair:** I understand, but I am interested in your involvement in Xinjiang at the moment. The Australian Strategic Policy Institute report alleged that Huawei supplies and assists the Public Security Bureau in Xinjiang, which has, in turn, been accused of surveillance and of human rights abuses, including, according to the report, "an estimated 1.5 million Chinese citizens and foreign citizens" being detained. How do you respond to those allegations?

***John Suffolk:*** As I said, our job is to provide technology and services to partners. In this instance, that is what we have done. The—

Q67 **Chair:** Do you have no concern about being, in a sense, complicit with such outrageous human rights abuses?

***John Suffolk:*** I do not think it is for us to make such judgments. Our judgment is: is it legal within the countries in which we operate? That is our criterion. It is for others—predominantly the Government—to make judgments about whether they think it is right or wrong.

Q68 **Chair:** But we are faced with a situation in which Huawei is involved in the provision of technology and services that has led to significant human rights abuses. Is that not something that concerns you?

***John Suffolk:*** I do not know the specifics of whether they have or they have not, based on one report but—

Q69 **Chair:** Do you condemn those human rights abuses?

***John Suffolk:*** We always condemn human rights abuse in any country in which it occurs.

Q70 **Chair:** Even where it involves your equipment and services.

***John Suffolk:*** In any country in which it occurs. We believe, in essence, that our objective is to understand the law in the 170 countries in which we operate, and to operate within the law as defined by those Governments.

Q71 **Chair:** If Huawei co-operates with the Chinese Government on state surveillance in China, particularly in Xinjiang province, to what extent can it resist pressure from the Chinese Government to enable surveillance abroad? You have demonstrated a willingness to work with the Chinese Government in a province where there are, allegedly, gross human rights abuses, and that suggests a close working relationship with the Chinese Government. Should that cause us concern in terms of your work here?

***John Suffolk:*** I would not accept that characterisation. I would say that, in essence, we understand the law. It is the Government's role to set the law, whether in the East or the West, and it is our job as a supplier to work within that law. It does not matter to us what the name of the country is; it is whether it is lawful.

Coming back to your question about whether we could be put under influence, we are quite clear, and it is quite proven, that we are an independent company. No one can put us under pressure. We have made it very clear that, regardless of the country, if we were to be put under any pressure by any country that we felt was wrong, we would prefer to close the business.

Q72 **Chair:** Should we do business with a company that is complicit in human rights abuses?

***John Suffolk:*** I think you should do business with all companies that stick to the law.

Q73 **Dr Lewis:** There is a lot of law in China, isn't there? Just like there was a lot of law in Nazi Germany. Some laws are good laws and some laws are bad. Some countries are totalitarian, repressive one-party states, and that includes communist China, doesn't it?

***John Suffolk:*** We do not make judgments about whether laws are right or wrong. It is for others to make those judgments.

Q74 **Dr Lewis:** Do you have a view as to whether China is a one-party state?

***John Suffolk:*** China is a one-party state, yes.

Q75 **Dr Lewis:** Do you have a view as to whether that Chinese one-party state is repressive of human rights?

***John Suffolk:*** I don't have a view on that, no.

Q76 **Dr Lewis:** You don't have a personal view on that.

***John Suffolk:*** I don't have a personal view on that.

Q77 **Dr Lewis:** You are a moral vacuum.

***John Suffolk:*** I don't believe so, no.

Q78 **Dr Lewis:** Is there any country in the world with a repressive Government that you would be unwilling to take a job from if you were offered it?

***John Suffolk:*** I have never given that any thought, so I cannot answer that question.

Q79 **Dr Lewis:** Well, here's an opportunity—give it some thought. Is there any regime in the world that you would not be prepared to work for, as long as your work involved observing the laws in that country?

***John Suffolk:*** As I said, I have not given that any thought. If you want me to answer the question with some thought, I cannot do that now.

**Chair:** That is a remarkable position you have stated.

Q80 **Darren Jones:** Mr Suffolk, you agree that there is a difference between ethics and law, correct?

***John Suffolk:*** Yes I do.

Q81 **Darren Jones:** Does Huawei have any ethics regarding who it supplies to?

***John Suffolk:*** Our starting point is always, in essence, that the law defines the ethics as far as we are concerned, because it is for Governments to define what is right and wrong, just as the UK defines what is right and wrong or what it will and will not allow. That is enshrined in law. That is our starting point.

Q82 **Darren Jones:** Companies are an entity in their own right, aren't they, Mr Suffolk? They can make decisions about whether they want to do business with certain customers. Following on from Dr Lewis, have there ever been any customers that you have chosen not to supply to?

***John Suffolk:*** I don't think we do it on customers; we do it on products. We stay in the commercial space, for example. We don't—

Q83 **Darren Jones:** But you do have customers.

***John Suffolk:*** We have customers, but the customers—

Q84 **Darren Jones:** Can you answer my question, Mr Suffolk? Have you ever declined to supply to a certain customer?

***John Suffolk:*** I am not in the sales, so I couldn't answer that.

Q85 **Darren Jones:** If you could write to us with that answer that would be great.

***John Suffolk:*** I am very happy to do that.

Q86 **Darren Jones:** My second question is about the third party in Xinjiang province. Do you have any controls over that third party's behaviour with the Chinese state?

***John Suffolk:*** Not that I am aware of, no.

Q87 **Darren Jones:** So, if the Chinese state asked that third party to interfere with equipment that you supplied to it with what we have understood to be poor quality programming, they could go ahead and do that without any oversight or control from you as a supplier. Is that correct?

***John Suffolk:*** I have no knowledge of whether that is right or wrong.

Q88 **Darren Jones:** If you could write to us with the answer, Mr Suffolk, we would be obliged.

***John Suffolk*** *indicated assent.*

Q89 **Carol Monaghan:** I want to ask some more about the law in different countries. We are looking at a situation where the 5G network could be provided by Huawei. Would that be operating under the laws of China or the laws of the UK?

***John Suffolk:*** Any operation of a network is always operating under the local law where it is deployed. In that context, it would be operating under UK law.

Q90 **Carol Monaghan:** So what access would your 5G equipment have to data that was being sent? In other words, would it be able to see the communications?

***John Suffolk:*** We do not run networks; we provide equipment to telecommunications operators. They run the network. We have no access to any of the data that are running across that network.

Q91 **Carol Monaghan:** What about your equipment? Would it be able to track the motions of a certain individual?

***John Suffolk:*** As I said, because we do not run the network, we have no access to the network. Whatever capability the operators are building in is purely under the control of the operator.

Q92 **Carol Monaghan:** What about the equipment itself? Would it be able to access the movements of a particular individual?

***John Suffolk:*** Let us take, for example, mobile phones. If you turn on GPS on your mobile phone because you are using something like Google Maps, that sort of product can track where you are. Generally speaking, that information is then sent to the central telecommunications network.

Q93 **Carol Monaghan:** But that is my choice, whether I turn that on or not.

***John Suffolk:*** That is your choice.

Q94 **Carol Monaghan:** If I decide to turn that off, will your equipment have the ability to track my movements?

***John Suffolk:*** If you think about what telecommunications does, it tries to connect you with a base station, wherever you are, in order to connect you to the network. It therefore does know where you are, because it knows where the information is coming from. In that context, telecommunications networks from all vendors know where you are, so as to connect you to those networks. Huawei's equipment is no different from anyone else's equipment.

Q95 **Carol Monaghan:** Would Huawei be able to remotely access equipment that was supplied to the UK?

***John Suffolk:*** We have no ability to remotely access anyone's equipment unless the operators have granted that permission or even have that capability. Different operators around the world have different ways of accessing. Sometimes they want people physically on site, and sometimes they will ask for controlled remote access, but that is under the full control of the operator.

Q96 **Carol Monaghan:** So you would be able to remotely access if the operator gave you that permission.

***John Suffolk:*** Only from Europe. We have a support centre in Romania, and that connection is turned on or off via the operators.

Q97 **Carol Monaghan:** So Huawei has an operations centre in Romania, so people in Romania would be able to access that?

***John Suffolk:*** If the operators granted that from the UK, yes.

Q98 **Martin Whitfield:** To pursue that, if we look at the current 4G network that Huawei supports, also from Romania, the software in essence is updated from Romania remotely with the consent of the operators who grant that. Is that the same model that you expect or hope to use with 5G as well, so that you would have remote access from Romania for updates, rather than physically having to visit everywhere?

***John Suffolk:*** That is not actually the way it happens. The upgrade of any software is under the control of the operator, and operators have different policies. Most will do it on site for the big central data. Where you tend to use somewhere like Romania, which is a pretty standard model around the world, is for fault identification, where you say, "We have a bit of problem. Can you look at what the data is telling us?" Once you have identified the problem, it might mean some upgrade, but that upgrade is done in situ. Typically, it is not Huawei employees who are involved in that upgrade. Again, that is down to the operators' choice. They control all of that.

Q99 **Martin Whitfield:** But on the current 4G, it is Romania that monitors for the faults. That is where the little light goes on to say there is something wrong in the system. Would that be Huawei's intention with the 5G, if the operators agree to that?

***John Suffolk:*** The use of Romania is at the operator's discretion, but as the previous panel said, 5G is building on 4G, so our plan would be to use broadly the same models unless the technology or the customer demanded something different.

Q100 **Bill Grant:** I am trying to understand Huawei. Who are the key shareholders or stakeholders in the company? Is it operated by a board? Can you pop along and put your hand on its ethical policy?

***John Suffolk:*** It is employee-owned—it is owned by about 96,000 shareholders. There is a full governance structure, which we have published for many, many years, from the board down to all the supervisory committees. We have what we call a business conduct guideline, which I am very happy to send to the Committee if it would like to see it.

Q101 **Chair:** But you claim that you have no links to the Chinese state.

***John Suffolk:*** That is true.

Q102 **Bill Grant:** One of your key themes is that you would enter into 170 or 171 countries and you make the clear statement that you would obey their laws. Would you turn a blind eye if they had wicked and bad laws in those countries? Is it simply that whatever their law says, you are happy to work with them?

***John Suffolk:*** Our starting point and our end point—I am sorry to repeat this—is that we understand the laws in the country. That can be a difficult thing to do, but once we understand the law, we will operate within the law. We do not make judgments.

Q103 **Vicky Ford:** Before I ask my question, I have to make two declarations of interest. First, I co-chair PICTFOR with Darren; Huawei is one of a number of tech companies that are members of that organisation. Secondly, I am a PPS in the Foreign Office, so I will not ask any questions related to foreign policy.

I want to ask a question about technology. An article in the *Financial Times* suggests that "Huawei could…use software updates to inject vulnerabilities between source code inspections." Why would a company want to do that? More specifically, what safeguards are there to prevent that from happening?

***John Suffolk:*** The whole debate that we saw in the first panel about vulnerabilities, patching and injection is an interesting one. Many of you have technology on your table here, and you will all be aware of the WannaCry ransomware last year and its significant impact on the health service, for example. That had nothing to do with the telecommunications vendors at all; in essence, it was about a faulty piece of software that had not been patched for the right period of time. The reality is that all software, regardless of whether it is new or old, has the likelihood of some vulnerability, and therefore everybody is going through a patching exercise.

Let me give you an example. Mr Metcalfe, I think you asked about the value of the UK CSEC. The UK CSEC is there to find whether there are vulnerabilities that people can spot. We can argue about whether that is a good thing or a bad thing, but our model is quite simply this: we allow any country and any company to review and inspect our products. That is not because we expect them to find 100% of the issues—if we did that, we would be in the software engineering business, not the telecommunications business—but because we believe passionately that the more people you have looking, inspecting, poking and prodding, the more chance you have of finding something.

Going back to your question, I would say that there is no point in anyone trying to inject something into software when, in essence, every week somebody is doing an announcement for a Microsoft Word patch or a Google patch. As you will know, you in Parliament have been subject to phishing attacks coming in through your email inboxes. That is a different way of breaking into software. As a good burglar would tell you, why break into a house with all the lights on, security and a dog barking, when you can go next door where no one is looking at you?

Security is more than what people think. It is very hard to inject. From our perspective, we believe in full openness and transparency. We want people to find things—whether they find one or 100, we do not care. We are not embarrassed by what people find. People have talked about poor coding or poor engineering. We stand naked in front of the world; it may not be a pretty sight all the time, but we prefer to do that, because it enables us to improve our products, and we all benefit from that.

Q104 **Vicky Ford:** So no safeguards?

***John Suffolk:*** We believe you have to put safeguards all the way along the line. We mentioned the supply chain earlier. In Huawei products, only about 30% of the components are Huawei's; the rest come from a global supply chain. We inspect that global supply chain by taking apart and checking things coming in from manufacturing. We are building in segregation of duties so that one person does not have access to all of the products. We limit what engineers can do. So wherever we have a part of a process, we look to build a control into it. CSEC is one of those controls.

Q105 **Stephen Metcalfe:** Good afternoon. You talk about the CSEC set-up. It has an oversight board, and for the second year running it has commented on the poor cyber-security in your products as well as the lack of action being taken to address that. Can you expand on what the plan is to address those concerns? Perhaps you can take us through what that process is and how transparent it will be.

***John Suffolk:*** The first thing to say is that we conform to all of the Government's published standards and policies on security. We also conform—you can check with our customers later—to all their bid documents and contracts on security. So whatever we have been asked to do from Government policy to a security requirement in a customer's perspective, we have fulfilled.

The CSEC report has required that we do better in many areas. We accept that. I think, as was said earlier by one of the professional speakers, some of the software is quite old, and what was in our view good five years ago is not what we think is good today. I guarantee that if we are sitting here in five years' time, we will not think that what is good today is still good.

On what we are going to be doing, first, we have built up a lot of clutter in some of the code. We have multiple versions of the same piece of code. You might ask, "Why do you do that?" Let me explain. One thing we are incredibly proud of is that some of the countries we operate in are not rich countries, and they do not have rich customers. They do not have the ability to buy the latest shiny bit of tin; they want to sweat the asset and keep their equipment going for 10 or 15 years. One of the routes we have taken is always to ensure that we maintain code that we know will run on 10 or 15-year-old equipment. It is a bit like me saying, "Can you take your modern equipment here, take what is on there and make it run on something from 10 or 15 years ago?" Typically, that is not possible.

We have to simplify that, but do so in a way that does not cause a resilience issue. We were talking about autonomous vehicles earlier. I think I would be sitting here for another reason if we ran too fast to change the software and the networks kept going down. So resilience for us is the No. 1 priority—keep those networks up. That means we have to be cautious. Any fool can drive at speed; it is whether they can do it safely. We are taking our time to get it right so that we do not affect carriers around the world who are supporting more than 3 billion of the world's population.

Q106 **Stephen Metcalfe:** You are drawing up a plan about how to do that, and

you will do that at a pace that maintains resilience so that you do not damage the system already in place, but when will that plan be in place? Will you share it with the oversight board to demonstrate how you will move from the current situation—I understand about the clutter in the code—to a simplified, easier set of commands to understand and spot where there may be any issues?

***John Suffolk:*** First of all, we have already taken UK customers and the oversight board through the plan, and we have already agreed what is the first set of products to go through the upgrade process. Those products have gone through the upgrade process, and they are going through evaluation at the evaluation centre now. We do not determine the sequence of the upgrades; that is done via the oversight board.

So some of the work has already been done. It is done on a priority basis set by the oversight board—the CSEC and the UK operators—and the first products are already in there.

Q107 **Stephen Metcalfe:** So the board, if we got them in front of us, would feel involved in this process?

***John Suffolk:*** Yes, in essence, they are setting the agenda in terms of what the sequence will be.

Q108 **Stephen Metcalfe:** Finally, Ryan Ding, who I presume you are aware of—

***John Suffolk:*** Yes.

Q109 **Stephen Metcalfe:** He told us that, in his view, this transformation process will take three to five years to see tangible results. First, do you accept that that is an accurate evaluation of how long this will take? Secondly, does that mean that equipment will continue to be potentially vulnerable and there will be no improvement in cyber-security on equipment until 2022?

***John Suffolk:*** Where Ryan Ding was coming from was that to do all of the products that operate within the UK will take three to five years. As you can imagine, some products are really very important from an infrastructure perspective.

Q110 **Stephen Metcalfe:** Are they being prioritised?

***John Suffolk:*** They are being prioritised. So the oversight board, with the UK operators, has set the priority. It is on the big projects that have the big difference. The ones that you sold only 500 of are at the back of the queue. To do the whole lot will take three to five years. But progress has already been made because the first set of products are already going through the evaluation centre.

Q111 **Stephen Metcalfe:** So it is slightly unfair of him to make that comment. Is that right? You have challenged it. It will be five years before we see any improvement in cyber-security.

***John Suffolk:*** You will see improvements before five years, definitely. I am not sure whether the NCSC would be even less complimentary if it was going to take three to five years.

Q112 **Chair:** Why do you think the oversight board, two years running, has raised, in effect, the same concern? They are quoted as saying, "Huawei's transformation plan could in principle be successful". The board, however, "currently has not seen anything to give it confidence in Huawei's ability to bring about change via its transformation programme and will require sustained evidence of better software engineering and cyber security quality verified by HCSEC and NCSC." Why are they reaching that conclusion that no progress has been made?

***John Suffolk:*** I think it is fair to say, Chairman, that we—Huawei—could have done a better job on communications.

Q113 **Chair:** Did you take your eye off the ball?

***John Suffolk:*** No, I don't think it is about taking your eye off the ball. It's about talking to our other customers around the world. Our products are shared by all countries. While we are taking on board the ideas and suggestions from the oversight board, we need to go back and check with other customers whether those changes in some way have a negative impact on the other customers and countries. I don't think we have done a particularly good job of explaining ourselves to the oversight board in terms of where we have got to in that thinking. It is not just about solving today's problem. We have talked about autonomous vehicles; we have not really talked about autonomous robots. You have talked about, in essence, artificial intelligence. The issue for us is not just thinking about looking back and how we can improve to get ourselves to a reasonable position today. It's about looking forward to understand how the technology and the threats might change, and to try to cater for some of those.

Q114 **Chair:** Are you saying it has just been your failure in communicating all the progress you have made to the oversight board, or that you have not made sufficient progress and you need to up your game?

***John Suffolk:*** I think it is both, Chairman.

Q115 **Damien Moore:** In a previous answer, you said that Huawei did not have any links with the Chinese state. Has there been an opportunity when it has failed to comply with a request from the Chinese Government?

***John Suffolk:*** We have never had a request from the Chinese Government to do anything untoward.

Q116 **Damien Moore:** Anything at all.

***John Suffolk:*** Anything. Let me be honest here. We have to pay our taxes, so I want to be clear. They never speak to us, but in terms of the purpose of this Committee, we have never been asked by the Chinese Government, or any other Government, I might add, to do anything that would weaken security.

Q117 **Damien Moore:** Would there be anything for any other Committee that

might give a different answer to that question?

***John Suffolk:*** Our answer would be the same. Are we asked to do things or build things into our products? Our answer would be: we have never been asked to do those things.

Q118 **Damien Moore:** Liang Hua, Huawei's chairman, has reportedly said that Huawei "are willing to sign no-spy agreements with governments, including the UK government, to commit ourselves to making our equipment meet the no-spy, no-backdoors standard." What is that standard, and how would such an agreement work?

***John Suffolk:*** There isn't an international standard on this. It's a request we received from one mainland European Government: would we consider signing a no-spy deal? It is fair to say that different Governments have different approaches to how they want to deal with security. If it is relevant for a Government to sign a no-spy deal, then we are happy to do that, but at the moment you would need to craft a deal. Our view would be that to make it worth while, you would need to link it to the contract of the operators that you are serving.

Q119 **Damien Moore:** To the best of your knowledge, do you know of any other provider that has had to commit to doing this?

***John Suffolk:*** I am not aware of any, no.

Q120 **Dr Lewis:** You said the Chinese Government has never asked you to put any weaknesses in the system. Does that mean that you are saying that the Chinese intelligence and security agencies couldn't get into your systems if they wanted to?

***John Suffolk:*** If we remember Edward Snowden a few years ago, he amply demonstrated that Governments of capability can break into most things, including Huawei servers, so you can never say that a Government, whoever they are, if they have the capability, cannot break into systems. That is what Governments do.

Q121 **Dr Lewis:** But surely there is a law in China that requires Chinese companies to co-operate actively with the intelligence services, and surely that applies to Huawei in China, doesn't it?

***John Suffolk:*** Well, all laws in China apply to all companies in China, not just Huawei. That is point No. 1. Secondly—

Q122 **Dr Lewis:** Yes, but Huawei is the company we are considering. Why don't you just admit the fact that Huawei is obligated to co-operate with the Chinese intelligence services in China?

***John Suffolk:*** There are no laws in China that obligate us to work with the Chinese Government on anything whatsoever. We have looked at all of the Chinese laws. We have taken on board professors in Chinese law and we have had their views validated via Clifford Chance in London, and there is no requirement on us or any other company to undertake what you are suggesting.

Q123 **Dr Lewis:** So the law of 2017 doesn't exist.

***John Suffolk:*** No, the laws do exist, but it is the scope and context of what those laws enable you to do.

Q124 **Dr Lewis:** That law states very clearly that Chinese organisations and individuals are required to co-operate with the Chinese intelligence services, and you are saying that Huawei isn't required to do that.

***John Suffolk:*** I am saying our legal advice is that is not the case. That is not their interpretation, and it is not our interpretation.

Q125 **Chair:** When your company wrote to me, you focused on the fact that it didn't have extraterritorial effect. Julian is asking about inside China. China's national intelligence law appears to be very clear on its requirement on individuals and organisations.

***John Suffolk:*** I think it is fair to say, Chairman, that many countries produce laws that are unclear, and we have had to go through a period of clarification with the Chinese Government, who have come out and made it quite clear that that is not the requirement on any company. We have had that validated by our lawyers and revalidated again by Clifford Chance. I believe there is no such obligation.

Q126 **Dr Lewis:** So you are saying that article 14 of China's national intelligence law, passed in June 2017, empowering the agencies of the Chinese state to "request the relevant organs, organisations and civilians to provide necessary support, assistance and co-operation" to those intelligence agencies does not apply to Huawei.

***John Suffolk:*** I am saying that what that means, according to our legal advice, is that it does not require Huawei to undertake anything that weakens Huawei's position in terms of security.

Q127 **Dr Lewis:** And I am saying that that is entirely unbelievable. Can you tell us whether firms like Nokia and Ericsson are given the sort of access to Chinese critical national infrastructure that Huawei would like to have in the west?

***John Suffolk:*** They follow me, but I will give my view and you can clarify with my friends. The telecommunications market in China is a very vibrant market, and Ericsson and Nokia have very good market share, and they compete with us head on in terms of China, so to answer your question, yes they do.

Q128 **Dr Lewis:** Finally, on 4 June it was the 30th anniversary of the Tiananmen Square massacre. How would you feel about equipment supplied by your firm enabling a similar exercise in suppression by a future Chinese Government?

***John Suffolk:*** I am sorry. I didn't quite understand the question.

**Dr Lewis:** How would you feel about equipment supplied by your firm enabling the Chinese Government, which is the direct descendant of, and absolutely continuously linked, in a linear fashion, with, the regime that

killed thousands of people 30 years ago on 4 June in Tiananmen Square—how do you feel about being complicit in repressive actions of that sort?

***John Suffolk:*** I do not think we are complicit in anything. I believe that our objective is to understand the law and comply with the law. It is for others to make judgments.

Q129 **Dr Lewis:** Like the people who manufactured the gas chambers, no doubt, in Nazi Germany.

***John Suffolk:*** We comply with the law.

**Dr Lewis:** And so did they.

Q130 **Graham Stringer:** I was going to ask a similar question, actually. I listened carefully to your answers about following the laws. Do you think that when we come to write our report, it would be fair to compare your company with IG Farben, who manufactured Zyklon B and sold it to the German Government during the second world war?

***John Suffolk:*** I would paint a different picture. If you are asking us, "Should we ignore the law?", I am sure you would say, "No, you must not ignore the law."

Q131 **Chair:** Basically, what you are saying is, "As long as we comply with the law, that is fine. We are amoral; we have no interest in what is happening", like the one and a half million Chinese people who have been incarcerated in Xinjiang, for goodness' sake. You do not care.

***John Suffolk:*** It is not that we care or do not care; that is not our starting or end position.

Q132 **Chair:** Yes, but you continue to provide equipment and supplies to facilitate that surveillance state.

***John Suffolk:*** I think it is for Governments to determine what is right and wrong. That is their sovereign duty.

Q133 **Chair:** But you will make money out of it.

***John Suffolk:*** We are a commercial organisation.

**Chair:** Right, you would. Okay.

Q134 **Graham Stringer:** Can I have an answer to my question?

***John Suffolk:*** My answer to the question is still the same as it was earlier: that, in essence—

**Graham Stringer:** Is it fair to compare you to IG Farben?

***John Suffolk:*** I do not know the circumstances around that.

Q135 **Graham Stringer:** Are you technically qualified in the kit that we have been talking about in the systems, and if so, can you tell us your technical qualifications in that kit?

***John Suffolk:*** My background, Chairman, is predominantly in technology, since the late 1970s; I have come through all kinds of technology. I am not a telecommunications expert, but I am a secure business expert—i.e. how you secure the whole of a supply chain, how you secure a business. What I am employed to do is look at everything from HR to supply chain to R&D on how we can build in the internal and external validation to improve security. We have teams of technical experts, internal and external, who will do things like cryptography, for example.

Q136 **Graham Stringer:** It is not a trick question of any sort. You understand the systems and the processes leading up to the systems, but not the kit itself.

***John Suffolk:*** I do understand what the kit is, I understand how it works, and I understand the security risks of those kits. My objective is what goes in and what comes out, and how we protect that. If I want deep technical experts to explain how something like how cryptography works in 5G, then I will call in a cryptography expert, and that is the same model that everybody else uses.

Q137 **Graham Stringer:** My final question is this: your company has grown very quickly, and it is a sort-of co-operative—I mean, the way you describe it, it is on the model of John Lewis. How is the capital being raised for growth of that speed?

***John Suffolk:*** Most of the capital comes from the growth of the business. We have grown from about $30 billion turnover in 2010 to over $100 billion in 2018, so most of the capital is raised through the business. The employees buy shares—they are not given shares—so we raise capital as well through the shareholders, and then we use banks for the remainder of the capital that we need to raise.

Q138 **Darren Jones:** You mentioned just now that your role is to secure resilience and security in the supply chain. We heard on the earlier panel—I think you were here to listen to it—

***John Suffolk:*** Yes, I was.

**Darren Jones:** About how supply chains are very complicated. How do you secure that position when there are apparently so many suppliers and legacy technologies in the supply chain?

***John Suffolk:*** We were the first company, I think, to identify all our high-risk suppliers. We went to all the suppliers and got them to work with us to sign what we call cyber-security agreements. Part of that is about the education and training of the people, and part of that is about understanding how they protect their own environment, because if their own environment is not protected, someone can break in and pass something to Huawei.

We then make sure that we are using secure suppliers; there are certain companies in the world that handle secure delivery of components around the world. When components come into our manufacturing centres—some of the manufacturing is also outsourced—we look at all those components

and their specifications. Much of that is automated; we have digital images, and we are scanning the image of the component coming in compared with the stored image is, but we also take a sample apart to see whether there is anything wrong in terms of what goes on there. We are looking at whether the soldering is right. We look at it from working with the suppliers through every stage to breaking some apart to see whether they conform to the standards we would expect.

Q139 **Darren Jones:** Could you give me a ballpark figure on the depth of your supply chain? How many companies are you working with?

***John Suffolk:*** In terms of high-technology companies, just under 2,000.

Q140 **Darren Jones:** So a piece of kit from Huawei might have somewhere around 2,000 companies involved?

***John Suffolk:*** No, not necessarily; it depends on the equipment. For a very simple product, you might not have that. I would need to give that information broadly by product. There is not an average of 57 or an average of 200. It is very different depending on the product.

Q141 **Darren Jones:** It would be useful to see that, because we have been having a conversation about core and edge and the different exposures around kit, so it would be interesting to see the supply chain for those, if you could write to us about that. My last question is this: you were asked just now about your work with government, and you said you had never been asked to do anything untoward. How would Huawei define "untoward" in the 170 jurisdictions that I think you said you work in?

***John Suffolk:*** If they were asking us to break the law.

Q142 **Darren Jones:** If the law in that country allows them to request something of you, you will comply with it, because that is the law and you follow the law in that country?

***John Suffolk:*** The challenge always comes in instances where the law is silent on matters, doesn't it? For example, most laws don't say, "Do not build in backdoors." Of course, from a security perspective, we would look at what we were being asked to do, but our belief is, in essence, that we as a vendor have never been asked to do anything that weakens the security of our product for any of our customers in any country.

Q143 **Darren Jones:** If a certain country had, for example, powers to request access to information that might fall within their geographical boundaries, you would comply with that, because that was the law?

***John Suffolk:*** I would not speculate on something that is hypothetical.

Q144 **Darren Jones:** That is not a hypothetical question, Mr Suffolk; that happens all the time, in this country as well as others.

***John Suffolk:*** I am not aware of that, and I am not aware of any situation where we have been put in that position.

Q145 **Darren Jones:** You are in charge of privacy for Huawei. What geography

are you responsible for?

***John Suffolk:*** Global.

Q146 **Darren Jones:** Global—and you don't know of any situation in which a Government has asked Huawei about lawful interception?

***John Suffolk:*** Lawful intercept is lawful.

Q147 **Darren Jones:** Yes, based on the law. I am just asking whether you would comply with that. Yes or no?

***John Suffolk:*** Yes, of course we comply with lawful intercept.

Q148 **Darren Jones:** You just said you didn't know whether you did, Mr Suffolk.

***John Suffolk:*** I'm sorry; we weren't talking about lawful interception.

Q149 **Darren Jones:** No, I asked you whether, if there was a law, you would comply with it. Lawful interception implies that there is a law.

***John Suffolk:*** If we were talking specifically about lawful interception, I would have given you that answer.

**Darren Jones:** Mr Suffolk, with the greatest of respect, your inability to answer questions directly on this inquiry builds an element of distrust in the way we are having this conversation with you. If I am asking a very simple question, I would quite like a simple answer. I'm afraid you have not been able to deliver that today, but we will look forward to your written answers.

Q150 **Chair:** Finally from me, could you confirm a report that said that Huawei's chairwoman, Sun Yafang, has a background in the Ministry of State Security, China's intelligence agency and—on Graham's point about where the money comes from—that Huawei has been loaned a total of $40 billion by the state-owned China Development Bank? I don't think you mentioned that.

***John Suffolk:*** On the first point, Madam Sun did have a role, I think, in that Ministry. On the second point, we have not been loaned $40 billion.

Q151 **Chair:** How much have you been loaned?

***John Suffolk:*** The facility that I think you are referring to, the China Development Bank facility, is available to customers of Huawei if they want funding for their products. It is done directly with the customer to the bank, not through Huawei.

Q152 **Chair:** But it facilitates your business.

***John Suffolk:*** They could take that loan from any bank they wished.

Q153 **Chair:** Is it to the tune of $40 billion?

***John Suffolk:*** No. My understanding is that less than 10% of $30 billion has been used in the past 10 years.

Q154 **Bill Grant:** I recall the company's pride in the fact that they operate

within the law in 170 countries throughout the world, yet in your base country, China, you saw fit to challenge the espionage laws by seeking legal advice, first in China and, I believe, in London, via an international lawyer, probably at great expense. What caused you to seek that advice? What was the doubt in the mind of Huawei? And this is bearing in mind that when you get advice from a QC, it may not be accurate, because they might have another one.

***John Suffolk:*** There was doubt in our mind because the law was unclear, and the doubt was also in our customers' mind, so our customers asked us to clarify this law as well. So we went back to the Chinese Government to provide clarity, and we went to lawyers to provide clarity, as did some of our customers.

Q155 **Bill Grant:** So the clarity from the Government of your home base was not sufficient. You questioned that, so there were doubts in your mind.

***John Suffolk:*** We did not understand the scope, and that's what we went back to the Chinese Government for—to define the scope, which they did publicly.

Q156 **Bill Grant:** But that has never been tested globally—the advice you have got. It's what you are saying is there, but that advice has never been tested.

***John Suffolk:*** It has never been tested in a court, no.

Q157 **Dr Lewis:** Is it possible to have an independent company the size of Huawei in a one-party, communist, totalitarian state?

***John Suffolk:*** Well, we believe we are an independent company.

**Chair:** Thank you very much. Could we have the next panel, please?

## Examination of witnesses

Witnesses: Mikko Karikytö and Steve Sampson.

Q158 **Chair:** Welcome to both of you. I will make the same point to each of you before you introduce yourselves: if you have any financial interests you want to declare, please do that now. May I start with you, Mikko? Can you introduce yourself?

***Mikko Karikytö:*** Of course, Chair. My name is Mikko Karikytö. I am head of network security at Ericsson. Ericsson delivers all the products needed for a functional 5G network. My responsibility, with my unit, is the security and privacy of all of the Ericsson portfolio. I have nothing to declare.

***Steve Sampson:*** I am Steve Sampson, head of technology for Nokia UK and Ireland. Nokia is a supplier of all the equipment in the telecoms sphere, through fixed and mobile and home and enterprise. I have nothing to declare, either.

Q159 **Darren Jones:** One of my colleagues asked Huawei this question earlier and we are just going to ask the same of you guys. In terms of your 5G

equipment, are you able to illustrate for us what type of information you might have access to by having access to your own equipment?

***Mikko Karikytö:*** That of course depends on the situation. As you have been discussing today, 5G is way ahead on security, as per the definition of the standards, already. I would say that, as in any security situation and in this one, it is a layered approach, actually. It starts with the global standards, obviously: we have a common agreement about the interoperability, the security and the protocols. Then comes our part, which is the hardware and software. That is secure: it is developed in a secure environment; it includes all the functions that are needed for a secure operation; and it is tested and assured that it remains secure. Then the deployment architecture—configuration and parameters—is critical, obviously. That's the third layer. And then there are the operations. The operations need to have all the global best practices, like segregation of duties, segmentation, least privilege—all those principles of security—to actually maintain a secure posture regardless of what has happened before.

Q160 **Darren Jones:** Presumably it is the same for Nokia.

***Steve Sampson:*** It is the same. I would also say that the equipment that we supply is given over into the hands of the operators. We have access to any information that goes through that only at the direct request of those operators. All interactions are fully auditable and authenticated by those operators. We have no continuous access.

Q161 **Darren Jones:** If you were providing an ongoing maintenance service, for example, would they be able to give you access?

***Steve Sampson:*** Yes. There is a relationship whereby, if there were a problem in the network, they would contact us. We would step in as requested. We would analyse the situation and provide the necessary software correction or hardware correction, and it would go to the operators for them to implement it in all cases.

Q162 **Darren Jones:** I don't know whether you heard the answer earlier, but we were trying to decipher the information that is available in the kind of edge bit of the kit compared to the core part of the kit. We had an answer about encryption and communication between the different technologies. Our constituents will want to know things such as how you track my location, whether you can see what I am doing and whether you can read messages. Of the equipment that you supply for the edge of the network—the access equipment—can you see any of that type of personal information of users of the network, or do you have to wait until it gets to the core before you start to see it, because of encryption?

***Steve Sampson:*** As was discussed earlier by the academic community, the standards in 5G are disaggregating the network components, and there are functions that will be placed closer to the antenna system. In the future, those core functions—they are mostly associated with the data paths or the user plane—would be in the mobile edge computing area and could have direct connectivity to other networks from that point, to limit

the latency and reduce the latency for critical services. That is one the main tenets of the 5G service.

The control plane functions will remain mostly in the core of the network and are highly robust. One aspect of moving to this core edge component is that there will be core components, but there will also be virtualised RAN as we discussed. That means that the distinction between core and RAN is no longer so simple. It is not a physical box anymore. It is layered on top of commodity-off-the-shelf hardware with open source software providing a resource that is used by all of the network functions, which make up the 5G network, and everything sits on top of everything else, and all of the security measures need to be built in at every one of the layers, as my colleague here mentioned, so there is no one fit.

Q163 **Darren Jones:** So you cannot just say, "Edge, intelligent, core."

***Steve Sampson:*** No.

Q164 **Darren Jones:** Is there anything you would like to add?

***Mikko Karikytö:*** I would just add that 5G is a tremendous opportunity for the whole society, and if we really want to benefit on all the services and qualities that it brings to us, it is exactly as my colleague has said: some of what we have known as core functions will move closer to the edge, which means that they will be faster and there will be less latency in the service to the edge, so that is definitely the case. Then the barrier between core and edge will be blurred.

Q165 **Graham Stringer:** Do you think you are on a level playing field with Huawei?

***Mikko Karikytö:*** When it comes to security, which is my responsibility in Ericsson—ensuring that all our portfolio delivers on the security and privacy promise, which is what we want to do—I think that, following the best practices, everyone can be on the same playing field.

Q166 **Graham Stringer:** Sorry, I might not have made the question clear enough. You are saying that your project is as good. I am asking whether you think they are involved in unfair competition by being subsidised by the Chinese Government.

***Mikko Karikytö:*** That is not my speciality. I concentrate on the security and privacy of our products.

***Steve Sampson:*** I am afraid I cannot comment on what our competitors do or don't do. All I can say is that Nokia is a global, multinational organisation. It is quoted on stock exchanges and is subject to all the rules of those stock exchanges, and it has a truly international board of directors. We compete in the market as the market is and we make decisions accordingly.

Q167 **Graham Stringer:** Can you explain to the Committee how you co-operate with the UK Government?

***Steve Sampson:*** We have strong co-operation with the UK Government, both through NCSC and DCMS. We have regular meetings with NTAC in order to ensure that we understand the requirements, and of course we follow all the regulatory requirements that our operators in the UK impose upon us through the contracts that we sign with them.

Q168 **Graham Stringer:** Are there any particular problems that you come across in co-operation with the UK Government?

***Steve Sampson:*** I am not aware of any.

Q169 **Graham Stringer:** Can I ask you the same questions?

***Mikko Karikytö:*** Certainly. We basically have the same answer. We definitely co-ordinate with all the Governments where we do business. Also, if we go back to the global standardisation, I believe that UK personnel will also be representing us in the standardisation, so that would be one way of collaboration also. We also want to understand the requirements and want to be able to deliver as best as possible in those, so that is why we also regularly meet with Government organisations.

Q170 **Graham Stringer:** Would you be willing to enter into a similar scrutiny of your products as the Huawei cyber-security evaluation centre? Would you be willing to follow that model?

***Mikko Karikytö:*** Until today, our model that we have been pushing forward—it has been mentioned earlier in this room, I believe—the global 3rd Generation Partnership Project system and Global System for Mobile communication models, where we try to find a global standard for how to assure the security and privacy of these devices. We believe that we need to have a common agreed model, whereby we all know then that when we go through this process and when our development environments are certified according to those standards we can be sure that what we deliver is as it should be.

Q171 **Graham Stringer:** Sorry—I am not clear from that answer whether you would be willing to follow a similar model.

***Mikko Karikytö:*** Of course we need to follow whatever model is put on us in the markets.

***Steve Sampson:*** I have a very similar answer to Mikko. We haven't been asked to do that yet. In all the countries we supply to, all of our equipment is tested by the operators in conjunction with the requirements of their regulatory commitments, and if we are required to do more as a result of any jurisdiction that we operate in, then we would do that.

Q172 **Damien Moore:** Just looking at supply chains, which we have learned throughout the course of today are a bit more complicated than we perhaps anticipated, what oversight do you have of your supply chains, and are any part of that supply chain based in China or any other non-western country?

***Mikko Karikytö:*** In Ericsson, we have a whole model around making sure that the portfolio is secure. We call it the security reliability model. That is

also something that we commonly get asked about publicly; you can find it on our web page, too.

We put all those controls to all of our organisations, regardless of what place on the Earth they are. We are a completely global company, with more than 180 countries represented, and we have research and development all over the globe. All those organisations will follow the same requirements that we set down.

We don't differentiate or give any leeway in that way with suppliers to us. We think that in the end our products have to be delivered into the customer networks as secure and protected as possible.

Q173 **Damien Moore:** Is it the same in any country that you would be operating in?

***Mikko Karikytö:*** Yes.

***Steve Sampson:*** From a Nokia perspective, our supply chain again is secured at a global level. We have very diverse R&D, manufacturing—all aspects of the business are separated in different geographies. And we have a central organisation that oversees all of the partnering and all of the contracting with any other partners and any other customers that we have, to ensure that we are happy that we are complying as necessary.

We have a zero tolerance practice towards any non-compliance, and from an ethics perspective we are regularly in the most ethical companies global list, and we are very proud of that and we would look to maintain that above all else.

Q174 **Damien Moore:** That is quite refreshing to hear. Looking at security vetting procedures, what do you have in place to protect your products from potential vulnerabilities and from those who might seek to do damage to them?

***Mikko Karikytö:*** In Ericsson, we have a long history of protecting our products. It goes back to the establishment of the product security instant response team, for example, where we have a continuous active process of looking for new vulnerabilities across our portfolio, and mitigating them as soon as possible. We do that globally and in collaboration with the security industry and all the other players, obviously, to always stay on top of the current situation.

Q175 **Damien Moore:** And what do you do when you do find something there?

***Mikko Karikytö:*** We have a very well-functioning R&D engine that is working, agile and continuous in the creation and continuous deployment, where we take these findings into the back-up directly and then fix them in the development, and deliver patches to our customers. If need be, an emergency patch would be released in a case of severe vulnerability.

Q176 **Damien Moore:** And is there any particular part that you have found to be more vulnerable than another?

***Mikko Karikytö:*** It all depends on the software type. I tend to think that the more mature software usually has been tested quite a few times more. But I think we treat them all the same and expect the same high quality from all the bits and pieces.

Q177 **Damien Moore:** Do these employees tend to have the same background in terms of which part of the business they are from, and do they have, potentially, the same nationality background?

***Mikko Karikytö:*** When it comes to the competence of our personnel, we have mandatory security and privacy training for all employees. We also have specialised training for engineering, product security and privacy for example, and we also have a certification model in the company. We can promote the importance of security even further among the employees and increase it further.

***Steve Sampson:*** In Nokia, we have a design for security process, which underpins our whole product development, right from the concept through the whole lifecycle of any solution. As with my colleague here, everything is tested in every phase. Vulnerabilities are checked for, and any that are found in any phase are corrected and we move forward with the agile approach. When it comes to faults found in the field or monitored vulnerabilities that are seen globally, we react to and deal with those, either through immediate mitigation or follow-up with permanent fixes as soon as possible.

Q178 **Damien Moore:** Do you identify people who are trying to do this, and how early? With people working within your company, or within your supply chains, how early can you recognise that they are trying to do something?

***Steve Sampson:*** I won't be able to answer that one. I will take it away and we will write to you with an answer, if that is acceptable.

**Chair:** It would be very good if you could do that.

Thank you both very much indeed. That completes our questioning with you.

## Examination of witnesses

Witnesses:, Alex Towers, Brendan O'Reilly, Patrick Binchy and Scott Petty.

Q179 **Chair:** Welcome. You have probably all been here for most of the session, so you will have heard that we are asking for any declarations of financial interest while you introduce yourselves, if that's okay. I have another cautionary note. There are four of you on this panel, which means that if you all answer every question we could be here for a very long time, and it's been a long afternoon, so just respond if you feel that others haven't said what needs to be said.

***Patrick Binchy:*** I am Patrick Binchy, CTO for Three—one of the UK networks.

Q180 **Chair:** Any declarations?

***Patrick Binchy:*** No.

***Alex Towers:*** I am Alex Towers. I am Director of Policy and Public Affairs for BT Group and I have no declarations.

***Scott Petty:*** I am Scott Petty. I am Chief Technology Officer for Vodafone in the UK and I have no declarations.

***Brendan O'Reilly:*** Brendan O'Reilly. I am Chief Technology Officer for O2 in the UK and I have no declarations.

Q181 **Carol Monaghan:** We have been hearing about the vast array of applications for 5G technology. What would be the impact of a major disruption, such as a technical fault or a cyber-attack, on the 5G network?

***Scott Petty:*** I guess it would very much depend on what the nature of the attack was and where it was focused. Part of the debate on this topic has been about which suppliers are using which different parts of the network and what security protections are appropriate in which places. The capacity to do damage is much more limited in what we call the access layer—the transmitters at the very outer edge of the network. The core of the network does all the sensitive business.

Q182 **Carol Monaghan:** In December last year, there was an attack on the O2 network. Is that correct?

***Brendan O'Reilly:*** It was a disruption—it was not an attack.

Q183 **Carol Monaghan:** Apologies. There was a disruption on the O2 network, which caused some issues. May I ask you all whether there are back-up measures in place to ensure continuity of essential services in the event of such a disruption?

***Brendan O'Reilly:*** The disruption that we saw on 6 December happened to a number of networks around the world at the same time—that is worth pointing out. We have measures in place. We have policies that we follow to try to recover service as quickly as possible and then regain service for our customers. We communicate with our customers throughout the period that we have that disruption, but obviously our focus is on fixing any issue that we find and then bringing service back as quickly as possible.

Q184 **Carol Monaghan:** What about essential services such as police or emergency services?

***Brendan O'Reilly:*** We work on resolving all of our services. What we saw on 6 December was a data issue that affected all services, so bringing it back for one customer meant bringing it back for all.

Q185 **Carol Monaghan:** May I ask the other witnesses the same question, although I do not believe that similar disruptions have been experienced?

***Scott Petty:*** There are two key elements. The first is designing the security of the network to ensure that it is secure at all times and that we trust nobody, regardless of where they come from. The second is the resiliency of those services and making sure that we have the resiliency we need in our network. If those services are critical national infrastructure, we build additional layers of resiliency into our network to give us greater certainty that those services will continue to run or will be restored more quickly. That enables us to get critical services back potentially faster than others.

***Alex Towers:*** There is not a huge amount to add. I think we all design the networks in very similar ways. To go back to my earlier point, around the core of the network there is effectively a very large firewall to make sure that those things carry on going, whereas at the outer edge we do a lot of regular monitoring to see what the activity is. It is much more predictable to see what you would expect to see, but if it becomes obvious that something is happening in a particular location, you can isolate that, switch it off and do something about it on an individual basis.

***Patrick Binchy:*** It is very similar. As Brendan said, it depends on the nature of the issue, but yes, it is the same answer for Three.

Q186 **Carol Monaghan:** Some of our concerns are about things like driverless cars, which have been mentioned this afternoon, but maybe we could talk about health applications as well. If health data has been sent or has somehow been impacted, who would have responsibility to ensure that that sort of information is going to be readily available?

***Scott Petty:*** It is really important that in the architecture of the network you have layers of security that protect all the elements of the network from each other. When I say that we trust no one, I mean nobody—none of the nodes, none of the elements of the network, none of the people who operate it. The separation of duties is very important in the security architecture to create that level of certainty within our network.

That is equally true of the device that is connecting to our network. Each, equally, should apply a lack of trust when connecting to it. If it is a health device, it should be applying the appropriate levels of encryption and security so that that data can be encrypted end to end. If it is an autonomous vehicle, it would never depend on network connectivity—that is not the design of autonomous vehicles—but the transport of its data would always be encrypted across that network. We have multiple layers of security at all elements of the network that protect all the elements of the network from each other.

Q187 **Carol Monaghan:** I suppose the concern that the public would have is that if the network goes down, it does not matter if I can text my husband to say that I have landed at City airport, but something more crucial probably does matter. I am trying to figure out how your network separates what is just chit-chat from information that is crucial and has to be sent.

***Scott Petty:*** Again, we separate those through the layers of security. However, if that service was critical, we would highly recommend to those customers that they consume at least two—and potentially all four—of the networks available in the UK, to build an additional level of resiliency so that if one of our networks failed, hopefully the other three would continue to function and those services would continue to operate.

Q188 **Carol Monaghan:** How dependent are network operators on the equipment suppliers to restore functionality if there is a network disruption?

***Brendan O'Reilly:*** We work with equipment suppliers when we find any issues—not just in terms of disruption, but issues as we find them through testing. We work with the equipment suppliers, looking at both their hardware and their software, to resolve them—as the two previous panellists talked through—in terms of how they do patching and how they regularly look at the software that they are putting into the network. We work with them to be able to fix any issues that we find and restore disruption, but for each element of the network, it will be slightly different reliance, dependent on the type of contract that is in place for each one.

Q189 **Carol Monaghan:** So if there were a disruption to a critical 5G network, you would have to work with the equipment suppliers in order to resolve that.

***Brendan O'Reilly:*** It would depend on the type of contract that was in place and the part of the network that it was in. Without having that in place, it is hard to say, but you can see a situation where—at least for information about the criticality of certain natures and parameters—you would work with the equipment suppliers to find out what that meant. Dependent on the commercial contract that was in place with that supplier, it would mean how far that would extend in terms of support.

Q190 **Carol Monaghan:** In terms of the equipment that we have providing our 5G network, if the network goes down, you have to work with the supplier of the network equipment. What happens if the supplier of the network equipment is awkward at that point?

***Brendan O'Reilly:*** Help me clarify what you mean by "awkward".

Q191 **Carol Monaghan:** Well, what if they do not want to work with you at that point? What if they have the ability to switch off the network? You, as operators, are trying to get the 5G network up and running; the equipment suppliers won't talk to you.

***Scott Petty:*** There are a couple of key points to remember. First of all, we would not have a single vendor in any of our networks running the entire 5G network. That is poor network design. The faults would probably fall into two categories: first, a hardware fault, where we would need to replace the equipment. We hold our own spares and we have our own maintenance contracts for that.

If the vulnerability was software-related, if we found a bug that needed to be fixed and the vendor chose to be difficult, I am pretty sure we would all

take the same decision: we would swap that vendor out for one of the other vendors that we already have in our networks to support that particular function. That is good network design—having resiliency of vendors and a healthy ecosystem of vendors that you use to always have the flexibility to replace components if need be, because it is not performing well or you are not happy with the vendor.

Q192 **Carol Monaghan:** Would an equipment supplier be able to switch off a network?

***Scott Petty:*** The job of our security is to protect our network from all external sources, regardless of those external sources. We have large perimeter defences and a lot of security inside our network to monitor the traffic and elements that sit around that. If an external source was able to get access to a device and do something to it, then our security layers have failed; we would detect that and we would replace it. It is always technically possible: all software has vulnerabilities, and it is possible for all software to be broken into. Our job is to build the security layers around that to minimise the impact and be able to restore that server quickly.

***Alex Towers:*** It is also worth pointing out—this is probably one of the reasons why we are here today—that different types of risk apply to different types of suppliers, and we have taken different approaches to how we manage the relationship with some of the different suppliers that are in place. For our fixed network, for example, we work with Huawei. It has been very important to us and to the security services to have access to the source code that would allow us, if we needed to, to step in and run the network ourselves, were there to be any sort of disruption that we could not handle any other way. It is very unlikely, I think, that we would end up in that position, but we take special measures in order to be in that position.

Q193 **Graham Stringer:** I am trying to get some insight into how you assure the security of your networks. Do you have different concerns and different tests for different suppliers? Are you more concerned about some suppliers than others? Would you know if a supplier was introducing vulnerabilities into the equipment, and how do you secure against that?

***Alex Towers:*** Yes, we have taken different approaches to different suppliers. The obvious example, as I was just saying, is we have taken a somewhat different approach to Huawei as a supplier, working very closely with the UK Government, who assess the degree of risk attached to any particular supplier, but there is a different structure and system in place for them. That involves in the first place some important principles about where we use the equipment—whether that is in the core or in the access—the sort of testing that goes on for hardware and for software, and access to the source code, as I mentioned. Then we have a continuing, ongoing programme of monitoring, although to be fair we would have that in place for any given supplier. There is a different approach taken, yes.

***Scott Petty:*** It is very similar. All our procurement decisions are based around the technical capabilities of the product, for which we use the NCSC's risk assessment framework. There is also the commercial offer and the balancing of the market share for those particular vendors of those components. Depending on the location of that equipment in the network, the security scores may be way larger for a core network node than they would be for a remote access antenna node, where the potential damage is much lower. Again, that aligns with the NCSC's security profile.

***Patrick Binchy:*** The only thing to add to that is that we all do independent testing on our components as we are putting them in, and then regularly thereafter.

Q194 **Graham Stringer:** How frequently do you update your security, and how long can you spend examining each update before it is rolled out? Basically, how long does it take? How do you manage those security updates? How involved are the suppliers in those updates?

***Scott Petty:*** It is a constant process. We find tens of thousands of vulnerabilities every month in all elements of the technology that we run. Either they will be provided by the industry itself if a vulnerability has been discovered, or a vendor will notify us that someone else has discovered a vulnerability and released a patch, or we have found those vulnerabilities ourselves and asked the vendor to fix that. It is a continuous process. Every day we are making our security patches and deploying software and updates to network and IT infrastructure to keep it secure.

***Alex Towers:*** We have 3,000 people in the cyber-security part of our business working 24/7 to try to detect and deal with attacks and vulnerabilities. There are something like 4,000 attacks a day on the network in some way, shape or form. It is an endless and ongoing process.

Q195 **Graham Stringer:** How often will you do these updates and checks? Do the bells ring and the red lights come on and you find that something has gone terribly wrong?

***Scott Petty:*** If you are asking whether we have outages related to security patches and change, then, yes, of course. The biggest cause of network outages for any operator would be change-related incidents, where we have upgraded software or made changes to a very complex environment. We work very hard to test that and mitigate those changes to constrain them to one component or element of the network. We do not upgrade all elements of the network at the same time. We do them in steps to ensure that we are validating that. It is a very complex process to maintain all those elements and keep them up to date.

***Brendan O'Reilly:*** I think it is good industry practice to have roll-back, so that if you find an issue, you can move back to the previous software release.

Q196 **Bill Grant:** In a previous life in procurement, I was familiar with BSI, the German DIN standards and EN—the European norm. In your procurement

process, is there a standard set globally, or do you just specify for a particular component for a particular task, or is there a standard across the board?

***Scott Petty:*** The basis for our standards—as you heard from the academics earlier, the GSMA standards are part of 3GPP. We work very hard to ensure that those standards are maintained, and we test that they are implemented effectively. One of the benefits of our industry maintaining a healthy ecosystem of vendors is that we get to test that those standards actually work in the field in engineering and that we can swap vendors efficiently across those particular standards.

Q197 **Bill Grant:** Are you confident that your spec is being met?

***Scott Petty:*** All networks in the UK have gone through swap processes or the replacement of one vendor for another fairly constantly over the past four to five years.

Q198 **Martin Whitfield:** We heard before, and it must be right, that access to your system from the vendors and manufacturers is only with your consent, but we did not get really get very much evidence of how frequently that happens. Given the thousands who have worked for you in security, is it a daily event that the manufacturers are in and out of systems remotely or physically, or is it weekly or annually? What is the frequency of them coming into your system with your consent?

***Scott Petty:*** It is probably important to separate: there is the production network and then there are our test and development networks, for which we validate issues that we find in the network environment. It is quite rare for a third party to have access to the production network. It would need to be a fairly extreme case. In all cases, our network operations centre and secure operations centre monitor every keystroke that they are providing. It is more frequent for them to have access to our test networks to validate new versions of software, to run logs and tests and so on, but that is a test network that has no customer information. It is not connected to the live environment. It runs a set of test data so that we can validate the production environment.

Q199 **Martin Whitfield:** Would that be weekly?

***Scott Petty:*** It depends. Probably weekly. In IT a little more often; in network a little less.

Q200 **Stephen Metcalfe:** Before I ask about your relationship with HCSEC, can I check whether all of you operate only in the UK?

***Alex Towers:*** No, we operate in 180 countries.

***Scott Petty:*** The same.

***Brendan O'Reilly*** *indicated assent.*

Q201 **Stephen Metcalfe:** So which set of ethics do you apply as an organisation? Do you apply UK ethics and only deal with those who share those ethics, or do you deal with the law as it stands in that country? I

just want to be fair to our previous witness about whether or not it was right to mention gas chambers and collaboration with oppressive regimes. Presumably you operate in China, do you?

***Alex Towers:*** We have some operations in China. Mostly they are about supporting multinational companies who want to operate in China.

Q202 **Stephen Metcalfe:** Fine. I just want to make sure that we are being fair. There are a lot of companies that operate in China in the telecoms market, and we have to be consistent in our approach to how we challenge where companies operate around the world.

Can I ask about the HCSEC? Do you have all the products that you use from Huawei reviewed by the HCSEC?

***Alex Towers:*** Yes, I believe so.

***Scott Petty:*** No.

Q203 **Stephen Metcalfe:** Why not?

***Scott Petty:*** In Vodafone's case we use Huawei in our radio access network. They review the framework and the development frameworks for the development of those products, but it is possible for an individual version of a product or an individual version of software to be deployed in our network that has not been evaluated by HCSEC. The reason for that is that there are constant revisions to products and software, so we rely on NCSC's analysis of the framework, but it is possible for a particular card or business software to be deployed that has not yet been evaluated by NCSC.

Q204 **Stephen Metcalfe:** Do you think that that is a manageable risk? Do you approach it on that basis?

***Scott Petty:*** The security and assurance of our network is our responsibility. We really welcome the work with NCSC. We think it is leading on a world basis. We wish other countries had the same framework and forward-looking security organisation that we have in the UK. They give us an additional level of assurance, but we do not outsource our assurance to NCSC. The security of the products is our job. They give us an additional level of capability and resource. We would also, frankly, like to see that across all vendors that we run within our network. That degree of visibility that NCSC provides through HCSEC is welcome for the industry. It gives us an additional level of assurance.

Q205 **Stephen Metcalfe:** Does anyone else want to add to that? Are the products that you use to maintain your network evaluated by the HCSEC?

***Patrick Binchy:*** Similar to Scott, the software is evaluated but if there are changes there may be some replacements that are not.

Q206 **Stephen Metcalfe:** And O2?

***Brendan O'Reilly:*** It has been judged that part of critical infrastructure has been through, but, similar to Scott's answer, there are—

***Alex Towers:*** I should probably clarify that there may well be a distinction to be made between the critical components and other components.

Q207 **Stephen Metcalfe:** I think you might have touched on this, but how central, in your assessment, is the work that the HCSEC does in mitigation of risk? Do they add to your evaluation of the products? As we have heard, there are three suppliers effectively in the UK supplying some of this core technology, so presumably Huawei is a key supplier of yours.

***Scott Petty:*** Huawei is one of the leading radio manufacturers in mobile. You are right: there are only three major radio manufacturers, along with Ericsson and Nokia. There is a little bit more choice in their core, but five vendors, not three vendors. They are a key supplier to our industry, both in the UK and across the world. They are one of the leading contributors to the development of standards and the development of the industry as a whole. Again, we really welcome the work that we do with NCSC to give us the insight and assurance that we need to place that equipment in the parts of the network that we believe are appropriate.

Q208 **Stephen Metcalfe:** You refer to the NCSC more than to the HCSEC. Is that right?

***Scott Petty:*** NCSC is a much broader framework of risk assessment that we apply to the entire technology set. HCSEC is just related to Huawei equipment and Huawei products in that area, but it derives from the same framework and gives an additional level of assurance. All of the broad work of the NCSC is welcomed by us.

Q209 **Stephen Metcalfe:** And if the HCSEC did not exist, would that change your view of their equipment?

***Patrick Binchy:*** I don't believe so. We think that the equipment is some of the best in the industry. Certainly, the technology is leading.

Q210 **Stephen Metcalfe:** So you don't share the security risks that have been highlighted elsewhere in the run-up to this inquiry?

***Patrick Binchy:*** We haven't had any evidence of security risks as yet. We have evidence of coding practices that need to be improved, and we are working with the NCSC and with Huawei to do that.

***Alex Towers:*** I think if it did not exist we would want something to exist that carried out the sorts of functions that it carries out. Indeed, before it existed, when BT first introduced Huawei into its fixed network, we developed something akin to the HCSEC approach with the Cabinet Office and the relevant bits of Government at the time, because it provides that additional layer of security.

There is absolutely, as Patrick says, no evidence of any direct security threat that has ever been posed by Huawei—certainly not to our network nor, I believe, to any of them—but there is clearly a different profile of risk involved. That is the reason why HCSEC is a good thing to have.

Q211 **Stephen Metcalfe:** And you feel the same way?

***Brendan O'Reilly:*** Yes. I think it is worth saying that we take all the vendors through a similar security framework. We have a security framework that we make them all work to, and we welcome any additional insight that allows us to make our networks more secure on a day-to-day basis.

Q212 **Stephen Metcalfe:** On that basis, do you think that there could be an argument to set up similar centres to review other manufacturers' products?

***Brendan O'Reilly:*** I think there is huge validity in the fact that we take one vendor through a framework and testing. Actually, for something this critical it would be good to take more vendors through it and give more certainty in the security that we are putting into our network. It is something that would be welcomed.

***Scott Petty:*** Vodafone's position is the same. The oversight board highlighted software engineering deficiencies in Huawei that were found because of the HCSEC model. They would be difficult to find in other vendors' products through testing, so we would like to see that regime deployed more widely to give us further assurance and trust for all the technologies that we use for 5G.

Q213 **Chair:** How concerned are you about the conclusions of the oversight board about Huawei's apparent slow progress in sorting out the technical issues that might undermine national security?

***Alex Towers:*** Both BT and Vodafone sit on the oversight board and we were part of that process, so we share the concern about the technical issues. It is really important to pick it apart a little bit, because the technical issues could create a vulnerability, not necessarily through Huawei or China but to any third party potentially to cause an issue in the network.

They also, through the process that we go through, allow all the companies to know what those issues are and to go away and fix them, so it is not a real and live pressing set of issues, but we do expect to see them fixed. It would be a major concern for us if Huawei do not respond positively to that report, both on the technical software issues and on the question of access to the source code for 5G.

***Scott Petty:*** I fully agree with Alex. We fully expect them to meet the commitments that they are making to the board. If they do not, we will apply normal commercial pressure and hope that they take that step forward.

Q214 **Chair:** Is it you two in the middle that contract with Huawei and use Huawei equipment, or do you all?

***Brendan O'Reilly:*** We all use Huawei, but to different extents.

Q215 **Chair:** Do you all reach the conclusion that the risk can be managed and

that they should not be excluded from the UK, or do you have a different view?

***Scott Petty:*** Our view is that the risk can be managed in certain elements of the network, and we choose not to use them in other elements of the network.

***Alex Towers:*** Yes, the same.

***Brendan O'Reilly:*** We will work to the guidelines that are set out, as Scott said, through the NCSC, and we will work to deliver the best service that we can for our customers based on those guidelines.

Q216 **Darren Jones:** I want to understand the exposure that your organisations have to Huawei equipment, so that we can get a feel for what it would mean if the Government took a particular decision. I will go to each of you. Could you illustrate for us what exposure you have from Huawei technology in your network?

***Patrick Binchy:*** We have recently signed a contract for a 5G RAN with Huawei. We are currently rolling that out and setting that up. Beyond that, we have some very small components in some aspects of our existing network.

Q217 **Darren Jones:** As a percentage—edge versus core?

***Patrick Binchy:*** I am not sure a percentage would give an accurate answer, because of the different commercial values associated with them. At the moment, we are just putting it in the edge—in the RAN. We do not have Huawei—

Q218 **Chair:** You say "at the moment". Is that all you will do? Are you clear that you will exclude them from the core?

***Patrick Binchy:*** Yes. We have signed a contract with Nokia for the core.

Q219 **Darren Jones:** Have you worked out how much it would cost if you had to take out the Huawei kit from your network?

***Patrick Binchy:*** Yes, and we have sent some figures through to the NCSC, but obviously they are confidential.

Q220 **Darren Jones:** Subject to the review. Alex?

***Alex Towers:*** In the fixed broadband network, there is no Huawei equipment anywhere in the core of that network, but it is in the access networks. For superfast broadband—fibre to those green cabinets you see on the streets—many of those have Huawei equipment in. We always operate a multi-vendor approach in every part of the network, so there is never purely one vendor, but they are present there. They are also part of the roll-out of the next generation of fibre broadband to premises that is just taking off now. We are aiming to get to 4 million households with that by March 2021.

For mobile, when BT bought EE, Huawei were part of the core of that for the 4G mobile network. They are still there now, but we are in the process

of moving them out of the core, so that when we come to the new 5G core, it will not have any Huawei equipment in it. Huawei are present in the mobile access network—the transmitter sites—for 4G as it stands and, indeed, now for 5G, which launched just a couple of weeks ago, they would also be in that deployment.

Q221 **Darren Jones:** EE runs the emergency services network for our police forces. Is there any difference in the approach to the ESN and your general offer?

***Alex Towers:*** No, that is part of the 4G network and it is the same sort of mix.

***Scott Petty:*** One third of our 4G base stations use Huawei radio access equipment. As we are deploying 5G in non-standalone mode, any site that we want to deploy 5G in, about one third of our network, requires Huawei 5G equipment. We do not use Huawei in the core network.

Q222 **Chair:** On 4 or 5G?

***Scott Petty:*** On 4G, 5G or 3G.

***Brendan O'Reilly:*** It is about 5% of our network overall, mainly microwave equipment. There is nothing in the core, so we do not have Huawei in the core now. It is 5%—there or thereabouts.

Q223 **Chair:** Is it only EE that had Huawei equipment in the core?

***Alex Towers:*** For 4G, we do. I do not know about Three.

***Patrick Binchy:*** Our core is Samsung at the moment and our future core will be Nokia.

Q224 **Chair:** So it is only EE that has Huawei in the core. Is that right?

***Alex Towers:*** Yes, and we are taking that out for 5G.

Q225 **Darren Jones:** Do any of you, with your current Huawei equipment, pay for the service or maintenance services, where they are able to remotely access your current kit?

***Patrick Binchy:*** Similar to the answer earlier, you have the production network and your testing network, so not in live production, no.

Q226 **Darren Jones:** So you do not have them providing remote access maintenance to kit that is being used in the Three network.

***Patrick Binchy:*** Monitoring they will do, going forward, but not access.

Q227 **Darren Jones:** What does monitoring mean?

***Patrick Binchy:*** They will get the alarms, so they can tell us that we have a problem or we have an issue.

**Darren Jones:** And then you deal with it yourselves, or with other suppliers.

***Patrick Binchy:*** Yes.

Q228 **Darren Jones:** Okay. BT?

***Alex Towers:*** No, that would be under our management.

***Scott Petty:*** We run our own network operation centres.

***Brendan O'Reilly:*** Same.

Q229 **Darren Jones:** It has been clear today that the distinction between core and edge is merging and becoming a bit greyer, certainly in the run up to 5G. Will you be taking any different approaches from your organisation's current position as that trend continues?

***Scott Petty:*** Can I take the chance to clarify that? I think physically it is true that the core network of cloud-based infrastructure can be more distributed. The logical construct of the network does not change. There is a separation between the radio base station and any core network element, including mobile edge computing via an IP security gateway, and that gateway maintains the security separation between the core network and the edge network. That does not change—in our design, would never change—in versions of 5G. While it would be technically possible to remove that IPsec gateway, that would be removing an important layer of security that we would never do.

***Alex Towers:*** That is a really important point. In the way we are designing 5G, we will put the firewall around all the edge computing so that when we talk about edge or access, we really just mean that outer layer of base stations that can only perform very simple functions and do not have any of the sensitive information going through them.

***Patrick Binchy:*** It is the same for Three.

Q230 **Darren Jones:** In line with Stephen's request, can each of you tell me whether you have an ethical policy about customers you will not work with and whether you have declined to work with certain customers, whether they be countries, organisations or Government Departments?

***Patrick Binchy:*** We operate within the UK on an autonomous basis. We operate with UK policy, UK rules, and we've got our own governance across that.

***Alex Towers:*** We operate to a pretty clear set of UK base ethics. We have a human rights policy in place that we publish and abide by.

***Scott Petty:*** Yes, we do have programmes run by our general counsel, and we publish a report every year.

***Brendan O'Reilly:*** A similar answer: we also have a global business principles policy, which we will happily send to you afterwards, just as part of the Telefónica global piece.

**Darren Jones:** Full house—very good.

Q231 **Carol Monaghan:** The Secretary of State for DCMS has said that there are essentially only three players in terms of future supply of 5G equipment. Do you agree with that statement?

***Scott Petty:*** For the radio access part of 5G, yes, I agree with that statement. For the core network, no; there are some additional suppliers as well.

Q232 **Carol Monaghan:** Who would they be?

***Scott Petty:*** Namely Cisco Systems, Affirmed Networks, Mavenir—smaller vendors that make components of the 5G network. For the radio access components, there are only three: Huawei, Ericsson and Nokia.

Q233 **Carol Monaghan:** So Samsung wouldn't figure in that.

***Scott Petty:*** Samsung are attempting to move into that market. They are fairly weak in 3G capability and 4G capability, which makes it difficult for us to swap our existing equipment for Samsung, because we still maintain 3G networks.

Q234 **Carol Monaghan:** Samsung have written to us, saying that they have provided commercial 5G solutions in the USA. Would that not make them a player here?

***Alex Towers:*** There may be an evolution, as Scott is saying. I suppose different markets have different characteristics. In the way that we are launching 5G in the UK, in its very first phase which has already begun, this is really about much greater capacity and speed for consumers to start with. We are effectively attaching 5G equipment on to 4G equipment that we already have, so we can really only use the suppliers we've already got to make that happen.

That is why it would be very difficult to impose something like a ban on Huawei in 5G, because it would require us to take out all of the 4G equipment as well. It is not simple to introduce a whole new supplier from this point. As the market evolves, I guess that might change, but not at the minute.

Q235 **Carol Monaghan:** If there were to be a ban on Huawei here in the UK, what impact might that have on future 5G?

***Scott Petty:*** It would slow down our 5G deployments.

Q236 **Chair:** By how long?

***Scott Petty:*** A number of years. It depends on how many base stations you have today, but in our case, everywhere we wanted to deploy 5G in the part of the country that runs Huawei equipment, we would first have to replace the existing base stations with new 4G base stations and then deploy 5G on top of that. Deploying a base station takes many months; it requires us to remove equipment and would consume capital that we would have otherwise spent on building more 5G nodes.

Q237 **Chair:** So we are talking about a delay in some parts of the country of,

what, two or three years?

***Scott Petty:*** Yes, potentially.

Q238 **Carol Monaghan:** How many base stations would there be? How many times would you need to do this?

***Scott Petty:*** In the UK, 18,200, of which 6,000 use Huawei equipment.

Q239 **Carol Monaghan:** When you talk about putting the 5G equipment on to a 4G station, physically, what does that mean?

***Scott Petty:*** We deploy a new antenna panel; it is a square box, this big. We may deploy two or four or six, depending on the particular site, and then we leverage the rest of the equipment that is already in that base station—the power, the transmission, the space that we have in that environment—and we make an update to a baseband unit that is in the box. It is an update to the network that we already have.

Q240 **Carol Monaghan:** So if it was a Huawei base station, it would have to be—

***Scott Petty:*** We would have to remove all the equipment.

Q241 **Carol Monaghan:** Yes, but if we were keeping that base station, would it still need to be Huawei's updated equipment?

***Scott Petty:*** If we were keeping it as a Huawei 4G base station to deploy 5G, yes, we would keep the Huawei equipment. You can't have a Huawei 4G base station with someone else's 5G technology on top. That hasn't been tested at scale or in the field to find out whether we could ever get it to work.

Q242 **Carol Monaghan:** Would a ban on certain suppliers actually reduce our security or have an adverse effect on our security?

***Scott Petty:*** I think it would create challenges for the ecosystem of vendors, and potentially that could reduce security because vendors need competition. Security is a difficult topic for everyone in the industry. It costs money to make your product secure, but you can rarely charge more money for making those products secure. The smaller the ecosystem is, the less commercial leverage we have to make sure they are doing the things we would like to see them do in security. Generally, the bigger the ecosystem, the better it is for us to be able to maintain security.

Q243 **Carol Monaghan:** What is the likely impact on the UK's 5G network of the US Executive order that has added Huawei to the export administration regulations list?

***Alex Towers:*** The short answer is that it remains to be seen, because we are still trying to understand the intent, the implications and the long-term policy position that will be reached on that. They have been listed and a temporary licence has been provided. We are talking a lot to the UK Government to try to understand better where that process will end up. Importantly, it has quite significant implications, if unamended, for

existing networks with Huawei equipment in them, including the fixed broadband network, as well as for any future deployment.

Q244 **Carol Monaghan:** How does it have implications here in the UK?

***Alex Towers:*** Let's see where the position ends up, but Huawei may be prevented from interacting with any US companies as they go about their business. Mostly, we need them to be able to do that, because we are using equipment that may be supplied by Huawei but will have a lot of US IP involved in it. The ongoing patching and updating of networks that have already been built requires, to some extent, the interaction of companies across the world.

***Scott Petty:*** A simple example is that the software code itself may have been written by Huawei, but the compiler that they used to compile that code is a US product. If they were no longer able to use that compiler, they would no longer be able to update their software, and that vulnerability would take much longer to be fixed than would otherwise be the case.

Q245 **Carol Monaghan:** Finally, how urgently do you need a decision from the Government's telecoms supply chain review? What is the impact of the current delay?

***Alex Towers:*** We would like some clarity as soon as we can have it. In the meantime, we have taken the decision—as others have—that we need to press ahead and launch 5G for the benefit of our customers, in the knowledge that we may have to come back and adjust how we do that if the Government come to a different view and want to impose new rules or restrictions. Clearly it would be good to have some certainty about what their position is as soon as we can manage that. Equally, we respect that it is their right to manage the process in the way that they see fit. They have to make the judgments about national security, and they are best placed to do that.

Q246 **Carol Monaghan:** Everyone happy? Does anyone want to add anything to that?

***Scott Petty:*** It is important that it is a fact-based, risk-based discussion, using the guidance from NCSC to come to that decision. If that takes longer, so be it. It is important that it is based on those facts.

Q247 **Graham Stringer:** I think understand Scott's answer to Carol: you are saying that if there are three competitors, you are likely to get a better product because the competition will help them afford security. Do you believe that the competition from Huawei is fair?

***Scott Petty:*** Yes, I do. Even though we don't have Huawei in the core, we have invited them to bid on pieces of business and they haven't been successful for a broad range of reasons—sometimes because of technical capability, sometimes for not meeting the security requirements, and sometimes for the commercial offer not being valid. It is a very competitive industry, and both Nokia and Ericsson win significant pieces of business in a fair commercial RFP, so I do think it is fair.

Q248 **Graham Stringer:** Do you think they are operating on the same financing basis as Ericsson and Nokia?

***Scott Petty:*** Clearly they are based in China, so they have access to resources and talent at a scale that is very difficult for western countries to mimic. If you ever have the chance to go to their R&D centre, you will see tens of thousands of incredibly well-educated employees with incredible skills who enable them to develop products quickly and effectively. In that sense, yes, they have an advantage over any other individual country. However, they still lose business and are still out-competed by leading vendors in the industry. It is our job as operators to make sure the ecosystem is balanced and fair. It is in nobody's interest for any vendor, regardless of country of origin, to have a significant market share over any other vendor. We would then have lost our commercial leverage and our ability to ensure that the industry moves forward together.

***Alex Towers:*** It wouldn't be fair to say that they have an advantage based on the price point. If there is a distinction, it is probably in the extent of R&D spending that they put in, which is probably more than their nearest rivals combined. That is what makes them stand out and gives them scale and readiness in a different sort of way in different parts of the market.

**Chair:** We have reached the end of the session. We are really grateful to you all for coming in this afternoon. Thank you for your time.