Joint Committee on the National Security Strategy

Oral evidence
Cyber Security: Critical National Infrastructure

Monday 23 April 2018

4.15 pm

Members present: Lord Harris of Haringey (The Chair); Lord Brennan; Lord Campbell of Pittenweem; James Gray; Lord Hamilton of Epsom; Baroness Healy of Primrose Hill; Lord King of Bridgwater; Baroness Lane-Fox of Soho; Dr Julian Lewis; Lord Powell of Bayswater; Lord Trimble; Stephen Twigg; Theresa Villiers.

Evidence Session No. 2 Heard in Public Questions 26 – 38

Witnesses

I: Paul Smith, Strategic Security Board, Water UK; Lyndon Nelson, Deputy Chief Executive and Executive Director for Supervisory Risk Specialists and Regulatory Operations, Prudential Regulation Authority; Jonathan Brearley, Executive Director for Systems and Networks, Ofgem; Steve Unger, Chief Technology Officer, Ofcom.

Examination of witnesses

Paul Smith, Lyndon Nelson, Jonathan Brearley and Steve Unger.

Q26 **The Chair:** Can I welcome you to the meeting of the Joint Committee on the National Security Strategy and pass on the apologies of our Chair, Margaret Beckett? You will have to make do with me trying to organise proceedings.

We have a variety of questions that we will want to put to you. I should warn you that there may be Divisions in the House of Lords. There is also some pressing House of Commons business, so there may be interruptions or other difficulties as we go forward.

To start, I will ask each of you to give us, succinctly if you will, an idea of who you see as the key player for driving improvements in cyber resilience in your particular sector. What makes that happen?

Steve Unger: I will explain quickly something about Ofcom's role in relation to cyber. Since 2011, the telecoms operators that we regulate have been required to take appropriate steps to maintain network security. The word "appropriate" is from the statute and is obviously quite broad. We issue guidance as to what we mean by appropriate. Operators report incidents to us and we then investigate. That is the overall framework.

It is worth emphasising that the vast majority of the incidents that are reported to us are what I would call traditional failures. We typically get 600 or so incidents reported to us each year, and over the last three years we have had three incidents that have related to cyber security. Most of the issues by volume that we deal with are still from traditional risks.

As I am sure you are aware, the NIS directive will expand the scope of our responsibility over the next few months to cover certain elements of internet infrastructure, such as internet exchanges. However, the biggest change in approach over the last few years has probably been a shift from looking at incidents reactively to trying to assess risk more proactively, particularly because, given the nature of the risks associated with cyber, you cannot really judge forward-looking risks by looking at history.

To pick up your question, I would identify two main areas of risk for us that we worry about at the moment, both of which have been somewhat in the news recently. The first is broadly supply chain risk: the concern that UK networks may contain components supplied by companies that may not be trusted. That is a long-standing concern, particularly in relation to China, although not exclusively to China.

Historically, the main concern has been in relation to Huawei, and more recently there has been a fair bit of news and a set of statements about ZTE as another potentially untrusted Chinese supplier. That is the supply chain risk, which as I say relates particularly to China.

The other set of concerns that has been in the news recently is the risk that some unfriendly state might use an existing, known vulnerability in networks to attack our infrastructure, with the aim of taking out elements such as critical national infrastructure. In the news, that has been associated particularly with Russia.

Broadly, the risks that we are concerned about in relation to China are mainly to do with the supply chains. The issue that we are concerned about in relation to Russia is mainly to do with cyberattacks using known vulnerabilities.

The Chair: Just to clarify, in relation to the supply chain vulnerability, do you judge whether a particular supplier is dubious, do you take advice from government, or a bit of both?

Steve Unger: We take guidance particularly from the National Cyber Security Centre. We do not directly regulate the different elements of the supply chain, but we judge whether operators are acting in an inappropriate way, and in making that judgment we take account of the advice that we get from the NCSC.

Jonathan Brearley: Just to clarify, is your question about who the key player is in driving protection against cyber risk?

The Chair: I meant: is it government or you as the regulator? Is it the operator, the trade body, or a combination?

Jonathan Brearley: Let me describe the regulatory framework and how it is changing. I want to say up front that ultimately the energy companies themselves and the owners of the national critical infrastructure are the ones that should be driving this. We put in the right regime to make sure that they have access to the right information. We are moving to a world in which we will set clear standards for them to do so.

I will describe two things: the world we have today and the world we are moving to under the network and information systems directive. In the world we have today, BEIS and the National Cyber Security Centre work closely with the companies, usually through guidance, support and advice, to make sure that they understand how to protect the infrastructure that we have. Those companies clearly have a strong incentive to do that and have been doing so successfully to date.

However, we all know, and as Ofgem highlighted last year, that this is a growing and fast-changing risk. We are therefore moving to a more robust framework where Ofgem will play more of a role. In this role, Ofgem will in essence ensure that the standards in the guidance set out by the NCSC are being followed. We are taking on new powers that will allow us to enforce against that, whether it is to direct companies or to fine them if we think they are not behaving in a way that protects consumers appropriately.

That said, at the heart of this, ultimately the companies are the ones that need to take responsibility for making sure that their consumers are protected.

The Chair: Just to be clear, do you see your role as being to pass on the message from the National Cyber Security Centre and then to check that the companies are actually taking that seriously?

Jonathan Brearley: Yes, and to enforce if we think they are not. In the new world we will also have enforcement powers that will make sure that they do that.

The only thing I would say is that when we think about the standards that we set and how we are going to go about this, when we move from a world that is about advice and guidance to one that is about standards, the benefits of the world we are in today are that companies are very transparent about their problems. They are very open about issues, and those issues are shared. When we move to this new world of standard setting we need to do so in a way that avoids two things.

First, we must not make this a prescriptive, tick-box exercise, because the world is moving too fast, and with the best will in the world any regulator will not keep up with that. Equally, that ensures that companies come forward with their problems, because that is the way we will transfer best practice most effectively.

Lyndon Nelson: I have a very similar answer to my colleague's. Firms are responsible and they already have existing regulatory responsibilities. The NCSC is very catalytic here: we definitely run an intelligence and threat-led response. The regulator's role is to make sure that that intelligence and threat are properly understood by the firms.

The other thing, and I do not think I am unique here, is that for firms, of course, the impact of failure is often more than for the individual firm itself. So the problem on the network, the impact on what for the financial system is a highly interconnected, highly international one has to be borne in mind.

The role of the regulator is often to bring those externalities very much to the fore when we are actually supervising and regulating firms. The responsibility with regard to the cyber threat is definitely the NCSC's. When it comes to the resilience of the system, it is definitely down to the regulators to ensure that the regulated take their responsibilities seriously.

The Chair: How do you assess whether they have taken them seriously?

Lyndon Nelson: We carry out quite a lot of testing. I suspect that throughout this afternoon I will use the "testing" word quite frequently. As many of you will be aware, we carry out intelligence and threat-led penetration testing. We also carry out a large number of exercises, and of course we have ongoing supervisory dialogue with the key firms in this picture.

The Chair: Okay. Mr Smith, obviously you are not a regulator.

Paul Smith: No.

The Chair: You are going to tell us how you relate to a regulator.

Paul Smith: Good afternoon. I am here representing Water UK. I am a member of the strategic security board, where I am the lead on cyber. I was also a member of the working group that wrote the good practice guidance for the water sector, and I am the chief security officer at United Utilities. So I am here as an operator and a trade association.

To answer your question, the responsibility for making sure that the right control is in place absolutely sits with us as operators of those critical assets. We work closely with the trade industries to try to understand what that regulation looks like and to understand the threat and the intelligence on that so that we can make a proportionate assessment of the controls that we need to apply.

From our side and the trade bit, it is more a collaborative way of working and making sure, with the new frameworks coming down, that we clearly understand, not just within our sector but across sectors, that we can share that good practice and take that into our respective organisations and apply the appropriate controls to that.

The Chair: Do you see this as being driven, in your case, by Ofwat, or by the Government's guidance to Ofwat, or—?

Paul Smith: We see it as coming, for the water sector, primarily through Defra. Ofwat tends to be more focused on economic regulation. It touches on resilience as part of its PR19 approach. Obviously cyber is part of that, but the actual regulation piece comes from Defra. Defra has very much been looking at the security of our critical assets for a number of years now in guidance, and the cyber part, I guess, is just the next generation of that security threat.

The Chair: We had a description there of Ofwat as primarily an economic regulator. Would those of you who are definitely regulators see your role as being primarily economic? Where does the resilience and long-term sustainability of what you have fit into that?

Jonathan Brearley: From an Ofgem perspective, our role is changing. To date, we have been primarily an economic regulator. Our job has been partly to do with price controls and partly the way we assess the funding the networks need to make sure that they have sufficient funding to manage the cyber risk.

However, as I say, for us that is changing. We are becoming the joint competent authority, with BEIS, and our role will extend further into enforcement and into making sure that the standards that are being set by the NCSC are being followed up by those companies. That is something we are building now as part of that directive.

Steve Unger: From an Ofcom perspective, for a while we have been both an economic regulator and a regulator concerned with security issues, and, actually, as a converged media regulator we have a range of other responsibilities, so we are used to being both an economic regulator and having a range of other duties.

Lyndon Nelson: The Bank of England is firmly not an economic regulator, so it is primarily concerned, in my part of the Bank, with the safety and standards of individual institutions. Obviously the Bank of England has a financial stability responsibility. If there is any economic regulation in that sense it will be carried out by the Financial Conduct Authority.

Q27 **Lord Powell of Bayswater:** I have a couple of linked questions. First, how will the network and information systems directive change your regulatory role in respect of cybersecurity? You have begun to touch on that, but you may have more you wish to add.

Secondly, and linked to it, do you have sufficient technical and financial support from the Government to perform the new responsibilities you are being given? That is really addressed to Mr Unger and Mr Brearley.

Steve Unger: In our case, the main change is in a change in the scope of what we do. We already had a set of responsibilities in relation to telecoms networks. Our scope of work will now also include elements of internet infrastructure—internet exchanges, domain names, service providers and so on. So it is a change of scope.

Although this is not specified in statute, I also mentioned that it is important for cyber that the way one approaches problems is also different. It is important to take a more proactive approach, so the type of testing that my colleagues have already referred to is also an important shift.

In our case, we are working with government and the NCSC to implement a scheme called TBEST, which will involve penetration testing of the companies we regulate to establish whether there are vulnerabilities. Those are the two changes: in scope and in the more proactive approach.

Do we have the resources? Yes. Do we have the money? We have the money that we have asked for at this stage of the process. Probably the bigger issue in cyber is skills; even with the money, recruiting people with the right skills for this sort of issue is challenging.

Lord Powell of Bayswater: We are coming to skills later.

Jonathan Brearley: I absolutely agree. The change in our role has been significant.

I think we will be able to manage financially. Equally, I believe that the technical support that we get from NCSC and others will help us in that role, but I do think there is a skills issue for all of us. It is a big challenge to get the right sorts of skills into the organisation so that we can tackle

this. It links to a more fundamental change in the energy market, in which data, IT and information are becoming more important in the market as a whole.

Lord Powell of Bayswater: Mr Unger, you mentioned Huawei as a risk. I am curious. Is it a risk because it is Chinese, or is there any evidence that it is a risk?

Steve Unger: It is a risk. It is regarded as a risk, particularly by NCSC, because of the potential for Chinese control. Of course, many companies have parts of their supply chain in China, but the specific degree of control that the Chinese Government could control over Huawei is clearly of concern to NCSC. In Huawei's case, mitigations have been put in place in the UK. There is the evaluation centre, which is one such mitigation.

Lord Powell of Bayswater: So you see a difference between Huawei and ZTE. The attitude seems to be that ZTE is seriously a risk because it is a nationalised company; it is a state-owned enterprise.

Steve Unger: ZTE is owned more directly by the Chinese Government. The advice from NCSC also notes that the issues with ZTE are partially about Chinese Government control, but also about their own supply chain. The US has now decided to refuse to allow ZTE to use US components. That creates a concern, quite separate from the Chinese Government control question, of how those systems can be maintained in the medium term.

Lord Powell of Bayswater: Thank you for clarifying that.

Lord King of Bridgwater: Would you add Global Switch to that as well?

Steve Unger: Not at the moment. The high-profile concern is about Huawei and ZTE, partly because of the risk but also because of the extent to which they are used in UK networks. The risks with Global Switch and several other companies, as with the risk associated with any company, should be judged on a case-by-case basis.

Lord King of Bridgwater: I understand that the Australian Government have terminated their contract with Global Switch.

Steve Unger: That is right.

Lord King of Bridgwater: But we welcome Chinese investment in this country from Global Switch.

Steve Unger: Yes.

Lord King of Bridgwater: Does that raise any concern?

Steve Unger: This is an area where we tend to take our steer from the NCSC, and at the moment it is rather more concerned about ZTE.

Lord King of Bridgwater: Do any of your colleagues have a comment on that? Probably not.

Lord Hamilton of Epsom: Can I just tease this out? Surely, the risk is from individuals rather than the ownership of companies. There is a suggestion here that if you hire a British company, everything is all right, but it might be employing Chinese nationals who are not.

Steve Unger: I think the view from NCSC—perhaps you might talk directly to it—is that the risk increases depending on a number of factors. Clearly, any company will deploy a range of people of different nationalities, but a company potentially controlled by a foreign Government is a higher risk than if there are employees from a foreign Government.

In practice, one has to take a pragmatic approach. The risk is never zero for any network or supplier, and a pragmatic judgment should be made in each case about whether the risk is manageable. It is worth emphasising that some of the risks are nothing to do with supply chains. The concern related to Russia at the moment is not so much about Russia supplying equipment into UK networks as about it exploiting known vulnerabilities in equipment supplied by trusted manufacturers, so there are a range of risks.

The Chair: I am conscious that we have strayed into the territory that Mr Gray was going to touch on, so perhaps we could take his questions now.

James Gray: I have a final word on the question of suppliers. You have been frank in naming Huawei, ZTE and others in this meeting. What actual advice do you give? This question is particularly for Mr Brearley and Mr Unger, and perhaps Mr Smith. Do you go to your members and say, "Here is a company about which we have doubts. You ought not to be buying equipment or systems from them"? What do you tell them?

Steve Unger: I mentioned previously that we have issued guidance. The basic legal test that applies to our operators is whether they have taken appropriate steps to protect network security. That means that they can buy equipment from a range of suppliers, but perhaps the most important thing is whether they have carried out an appropriate risk assessment. We have certainly highlighted to them the risk associated with some foreign suppliers, but those risks can be mitigated if they have appropriate controls in place.

James Gray: Sure. But would you go as far as saying to members, "We have doubts about company A, B or C"?

Steve Unger: That advice is out there from the NCSC and, as mentioned earlier, our job is to judge whether the operators are taking appropriate steps to maintain network security. In judging that we would ask the operators, who are clearly aware of the NCSC's advice, whether they have looked at that, taken it seriously and considered what mitigations can be put in place before purchasing.

Jonathan Brearley: All I would add is, similarly, that the advice comes from the NCSC and BEIS, and our role will become one of making sure that it is being implemented.

James Gray: Is there a commercial risk here somewhere? Today you have openly named Huawei, which is often in this building sponsoring all sorts of events. Is there not a risk of it accusing you of commercially undermining a perfectly responsible company?

Steve Unger: We have quite a long-standing relationship with Huawei, and I am in many ways an admirer of that company. It innovates in various ways in developing new technology and has delivered a number of benefits to the telco industry, which we respect. At the same time, there is a risk because of the potential for Chinese Government control. We are not anti-Huawei, but there is advice out that there is a risk, and that risk needs to be managed.

James Gray: But if you discovered that it had chips in its equipment that were undermining British critical national infrastructure, presumably you would then become anti-Huawei, would you not?

Steve Unger: In some circumstances, yes, but at the moment that is not the case. On the one hand, it is a company that provides equipment to a number of UK networks. That delivers benefits to UK consumers because of the quality of that equipment, its price and innovation, and so on. On the other hand, there is a risk that needs to be managed. I guess I see it in that reasonably pragmatic way: there is a balance here, as there always is.

The Chair: The others are very silent on all this.

Jonathan Brearley: In terms of where Ofgem is now, this is the sort of thing that the NCSC and BEIS will advise companies on. All I would say is that you need to take care not to be too prescriptive about the things that you ask companies to do or to avoid. This is ultimately about getting them to take on responsibility, examine their own supply chains and then do the work to make sure that what they do is secure. The more you take that decision-making away from them, the more at risk you are that things are moving far faster than we can move to catch up with them.

James Gray: Having strayed from my brief slightly, you said earlier that it is all down to the companies. That is fine if you are dealing with major national companies in water and electricity, but surely there are suppliers in the supply chain that are quite small companies and simply would not have the capability to deal with these things themselves. They would look to you as their regulator for advice and assistance, would they not? To be honest, United Utilities will be fine, but what about the bloke who makes the widgets?

Jonathan Brearley: Again, there is advice out there for all companies in the NCSC and BEIS's guidance, which is being strengthened. Our job, though, is to make sure that when the big companies that own the

networks get their supply chain in place, they are carrying out the appropriate checks.

Similarly, someone mentioned employees as an example. Companies also need to make sure they have the right security checks on employees coming into their own company.

Q28 **Theresa Villiers:** I will start with a factual question. It would be helpful if you could outline the main assets and organisations within your respective remits that are classified as critical national infrastructure. Can you also give a flavour of how distinctly you treat them, as opposed to other organisations and assets with which you deal?

Lyndon Nelson: It is the large banks, the payment systems, and the Bank of England, because it is also a payment system. They are very much subject to a high level of scrutiny. For example, they are the ones where we have carried out the first phase of penetration testing. They are also the companies on whose progress we would report to the Treasury, as well as to the Financial Policy Committee, because of the financial stability implications if they were to fail to deliver some of their critical services.

Jonathan Brearley: From Ofgem's perspective, it is any supplier that has over 250,000 customers—basically, all the medium and large suppliers—and any generator that has over 2 gigawatts of generation. Then all the network companies and interconnector companies come under the CNI definition. The difference in the way we treat them is that those standards get applied but advice and guidance is available across the board.

Steve Unger: In our case, thinking particularly about tier 1 and 2 levels of CNI, most of the public operators that we regulate are not classified as critical national infrastructure. They are generally designed as networks to supply a wide range of customers. That is why I emphasised earlier the role of risk assessments. My sense is that if you think about the level of risk associated with a particular piece of communications infrastructure, a lot depends on what it is actually used for. Having a clear sense of those end-use vulnerabilities means that doing a proper risk assessment that is context-specific is, for me, more important than whether, in that slightly black and white way, it is part of the CNI formally.

Theresa Villiers: This question is again probably more relevant to the three regulators. What approach do you use to prioritise the organisations and assets for which you are responsible, and which you believe have the most urgent need to address cybersecurity issues? You have given a flavour of the distinction between critical national infrastructure and other assets. But looking at it more as a spectrum, how do you focus on the biggest risks that you believe need the greatest attention from the organisations coming within your remit?

Lyndon Nelson: We have essentially a risk-based approach. The CNI determines what you might call impact; it makes sure that we have an eye on the biggest assets.

The other aspect that we bring to it, given our knowledge and supervision of the firms, will be the probability based on how they have managed other operational risks. What is their IT estate like and what is their level of vulnerability, et cetera? That would also determine prioritisation. We have done a variety of interventions with that smaller but let us say higher probability of failure population. That is essentially how we would determine our resource allocation.

Jonathan Brearley: The categories that I have outlined give a relatively limited number of companies to focus on. Again, we would take a risk-based approach to focusing our resources, which is partly about the scale of the problem but also about the degree of risk we think that particular company is under.

Steve Unger: Probably the most important thing for us, to pick up a theme from some of my colleagues, is to make sure that the operators themselves have the systems in place to identify technical risks. For me, that is the highest priority, and there are probably two parts to it. One is making sure that they have a clear sense of board-level accountability on these issues. The second is that those who are accountable are well informed internally. If that is got right, a lot of the rest follows. Our understanding of technical risks is driven by the threat assessments that we get, for example, from the NCSC and elaborated on through the testing programme that I talked about previously.

Theresa Villiers: Within the networks and organisations that you oversee, what vulnerability keeps you awake at night the most? Assuming that there was a successful cyberattack on an organisation or asset that comes within your remit, what sort of case would you see as doing the maximum damage?

Jonathan Brearley: From my perspective, we have already seen a case study from Ukraine of what can happen if this goes wrong. A worst-case scenario is clearly a serious security of supply incident, where you quickly get to the sorts of figures that are very high in their impact on the economy.

As for what specifically keeps me awake, or concerns me, it is more the fast-paced nature of this. When I talk to people in companies about how they are doing today in protecting, they are relatively confident but they always say, "We do not know what that is going to be like in six months' or a year's time". The system we develop has to be agile enough to adapt as the situation around it adapts.

Steve Unger: I do not know what keeps me awake at night, but I echo that comment. Once you understand a risk, you need a chance to deal with it. The big worry is the stuff that we do not know about, and it does exist. In my sector, I suppose there is the risk that a widespread failure

of communications networks could have a knock-on impact on many other areas in the economy, well beyond the communications sector.

Lyndon Nelson: It is dangerous to ask a regulator what keeps them up at night. We could be here all night, but I will stick with the spirit of the question. If a shared piece of infrastructure was vulnerable and attacked, how many other companies are sharing that infrastructure?

In reality, however, basic systems and controls—this came through in our testing—are to a large extent the source of many vulnerabilities. So if firms were to improve their password controls and such things, we would see a large proportion of these vulnerabilities reduce significantly. But what would keep me awake at night is definitely the shared infrastructure, a shared piece of software, or something like that.

The Chair: I think Mr Smith should tell us what keeps him awake as well.

Paul Smith: Going back to the start of the question and the CNI assets, we have a prescribed formula for our definition of assets. It is driven by the population served. The top three categories—that is, anything above 100,000 people—will be in scope from a CNI perspective. We obviously look to the National Cyber Security Centre and our regulators to understand the threats and risks around, and then protect them accordingly. The other aspect is where we serve other CNI sectors. We might have a small asset that is not CNI but serves a CNI sector, so we need to consider that as well.

What keeps me awake at night is a lot of the unknowns. We know of vulnerabilities—as a sector, we do tests to try to verify our vulnerability state and mitigate it—but the unknowns may be in a random network, or external influences at any one time that can change that state. You are probably aware that the cyber threat changes almost daily. It is about trying to make sure that we have appropriate levels of control for those assets.

James Gray: It was a week ago today that the NCSC produced a new technical alert. I think I am right in saying that, for the first time, it was done jointly with the CIA and the national homeland people in America, which was quite significant. I think that for the first time it also mentioned Russia as a particular threat. How does that differ from what you have been told previously? What is new about it?

Steve Unger: I was familiar with the risk, as we have been working with the NCSC and it is not completely new. It has been publicised recently, and clearly the specific concern in relation to Russia and what it might do has increased over recent weeks or months. But the vulnerabilities identified in that threat alert—the technical alert—are not new; we have been aware of some of them in the past and talked to our operators about some of them to mitigate those risks.

James Gray: Why did they produce the alert in that case? If it is a long-term story of the kind that you describe, why did the NCSC, the CIA and

others decide to produce this new alert this time last week? If you were aware of these risks for a long time and working on them, what was the purpose of this new alert or perhaps what triggered it off?

Steve Unger: I suspect you would have to ask them.

Jonathan Brearley: You would have to ask the NCSC that, but it is pretty clear that when you talk to companies about how they manage them, these risks are not unknown but their level has clearly changed. That is why those agencies felt moved to make a public statement, but ultimately that is a matter for them.

James Gray: Okay. Am I therefore right in concluding that none of you would have changed what you advise your companies to do in the light of the new technical alert? If you were already working on it for many months and it was not a great surprise to you, presumably not much has changed as a result.

Steve Unger: The threat level has increased, so the way I see it is the technical vulnerabilities have been there for some time. The capability, particularly in Russia and some other states, to exploit those vulnerabilities has existed for some time. It does not appear from nothing.

The judgment that has presumably been made is that the willingness of some countries to use that capability has increased. The threat is greater in light of recent events, but the technical vulnerability is not new. I assume, though, that they have gone public because the threat looks greater at the moment.

James Gray: This puzzles me, I have to say. Here we have three major organisations producing a significant alert, but you said a moment ago that it was not terribly new because you knew all that already. I presume that your companies have not done much differently in the meanwhile. It strikes me as odd and it leads me to wonder whether there is a connection somewhere with Salisbury or Syria. Is it all part of a national ramping-up of concern about Russia, or is this purely a routine announcement by the NCSC? "There's nothing to worry about. Just get on with it, chaps".

Jonathan Brearley: I am sorry to come back to this, but at the moment that advice from the NCSC goes direct to the companies under the framework, so it is not Ofgem's role now to interpret that for them. I just observe that the public announcement was clearly made in a way that suggests the threat level has gone up, and I suspect that companies are responding to it.

The Chair: Just to be clear, the distinction was that that announcement was made publicly. Am I to take it from what you say that the bulk of the advice you get from the NCSC is not made public?

Jonathan Brearley: Certainly, the companies themselves get advice from the NCSC and from across government that is not made public.

Steve Unger: Exactly. Our companies get advice direct from the NCSC. We also have a close dialogue ourselves with the NCSC to understand what it regards as of concern, and it would not normally make public all the details it gives us.

Paul Smith: From a water perspective, we received some information on the Russian threat that was outside the formal public briefing last week. There was more technical content about what we should be looking for, which is different from previous known events of that type from Russia.

Jonathan Brearley: I would just add that it is imperative that the companies and the security services in general have fast and comprehensive information about a situation when it occurs. So there are bound to be private conversations as part of that. Part of that is the need to move quickly when something happens.

Lord King of Bridgwater: Do you get involved in what I call war-gaming? Do you get involved, with your industries, in worst-case situations and work on those?

Lyndon Nelson: Extensively.

Lord King of Bridgwater: And in analysing what you would do if you were on the other side and trying to see how much damage you could cause, and distinguishing between things that are an inconvenience or an interruption and those that might lead to permanent damage?

Lyndon Nelson: We carry out exercises looking at the worst case. I have not been involved in what you mention in the other half of your question, which is how would I cause permanent damage outside the UK.

Steve Unger: In our case, we have been involved for a number of years in exercises in relation not just to cyber but to other types of resilience issue. More recently, obviously, things have ramped up on the cyber side. We do not do a lot of work trying to understand how you would attack UK networks, because the NCSC is the UK source of expertise on that. We take threat intelligence from it as to the types of vulnerabilities that it has identified.

Lord King of Bridgwater: But are you involved in that sort of exercise, if it is being done by NCSC, and with the companies perhaps involved?

Steve Unger: Yes, we are involved in those types of exercises.

Lyndon Nelson: The Bank co-ordinates the exercises on the financial system. We put on an exercise last year for 30 firms. Essentially, we brought down the payments system, not necessarily as a cyber event; the cause was not really relevant to the exercise. But, yes, we operate those.

Jonathan Brearley: We, as Ofgem, run our own resilience exercises, and we participate, or intend to participate, in those run by BEIS.

Paul Smith: In the water sector, we too undertake collaborative discussions and exercises to understand a cyber event and how you might recover from it. Each organisation will absolutely go through and do those penetration-type testing models to prove where those vulnerabilities could be exposed.

Jonathan Brearley: It is worth adding that as we scope out this new role in enforcement we will have to look hard at whether we war-game more comprehensively with the companies.

The Chair: I know that Baroness Lane-Fox wants to come in on the point about penetration testing. It may be a good moment to take that question, and we will then move on to Ms Villiers.

Q29 **Baroness Lane-Fox of Soho**: Mr Nelson, we know that the Bank of England did some effective penetration testing, and you have all mentioned it from different points of view. Can you comment on why you thought that was effective and how you ran and operated it?

Lyndon Nelson: Of course. It comes back to the Chair's question about how you test these things. In many other parts of our world, we run a stress test to test the financial resilience of firms, and we can test that resilience in some other way. In this area, we did not have that, so we felt the need to have the test. That is what created it.

We carried out 34 of these penetration tests and we will do more. They are intelligence and threat-led, accredited people who provide that intelligence and at the same time validated by the NCSC. We agree the scope of that. The penetration test is then carried out, and in almost all cases there is a mitigation programme from that which the supervisors take forward.

We will probably extend the range of companies with which we carry out this test. We are also advising colleagues with similar structures to ours in the G7 and carrying out a similar test for them. We will carry on refining this testing programme.

Baroness Lane-Fox of Soho: So how can you be sure that what you have learned from the testing is then changed and implemented?

Lyndon Nelson: These firms are the largest firms. They have what you might call a dedicated relationship management team of supervisors. There is a vast programme of things that they have to fix, and supervisors will be on top of that to make sure that firms carry out those changes. Then, of course, we will retest.

Baroness Lane-Fox of Soho: My spies tell me—

Lyndon Nelson: Literally, or—

Baroness Lane-Fox of Soho: No, not literally. They tell me that Sam Woods, chief executive officer of the Prudential Regulation Authority, gave evidence to the Treasury Committee that was slightly contradictory

to what you are saying—or maybe not.

Lyndon Nelson: I hope not. He is my boss.

Baroness Lane-Fox of Soho: He said that there is still a long way to go in operationalising this kind of resilience and testing. What did he mean by that?

Lyndon Nelson: That is absolutely correct: we have a long way to go. The CBEST test itself is not perfect. The penetration test itself is not perfect. Of course, we only ran it for 34 companies, and there are a lot more companies to run it for. So that is where we start.

The test is in its infancy. We have only had one round, and we have learned a lot from it. I think back to Lord King's comments earlier. Were I to think about how I might break one of the banks, perhaps as an insider might be the way I would choose to go. This illustration test does not do that.

It has, however, provided some very useful information, both for the NCSC in terms of how vulnerabilities are managed but also for supervision. So, yes, it has a long way to go, but we were very pleased with the results that we received from the work that we had to do.

Baroness Lane-Fox of Soho: And now to the rest of you. You mentioned TBEST already. Can you add anything about how effective the systems will be in each of your different areas and the challenges of implementing them, or not?

Steve Unger: TBEST is somewhat based on the experience of CBEST and is the same sort of idea: penetration testing in controlled circumstances. At the moment, we are engaged in two pilot trials of the process—one with a fixed operator, one with a mobile operator. I think it is the right thing to do, not least because there are clearly risks. Some of the risks we worry about most only become manifest too late, and at that point you will probably kick yourself if you have not done something beforehand. Proactive testing of this kind is essential, but it is difficult, particularly when you are testing a live network, which is what we are doing.

At the moment we run pilots on the fixed and mobile network. The plan is to learn from those pilots this year, and the expectation is that we will take over operational responsibility for running that programme around the end of this year. At the moment it is being run by government with our participation.

Baroness Lane-Fox of Soho: That is quite a long timeframe before you get a serious test, would you not say?

Steve Unger: I am hoping that we will learn quite a lot from the pilots, actually. We will get the learning from the pilots in a few months.

Jonathan Brearley: In Ofgem, we are still scoping up our standard-setting role, and we will look at this as part of that.

Baroness Lane-Fox of Soho: You have not done any penetration testing?

Jonathan Brearley: Ofgem has not done any penetration testing.

Baroness Lane-Fox of Soho: In what kind of timeframe would you imagine that you might?

Jonathan Brearley: I think we will have to look at the details of the implementation of what we have.

Baroness Lane-Fox of Soho: Thank you.

And if I am not talking about penetration testing, I am talking about skills, so I will just segue into the fact that I would imagine that one of the challenges with all this is the skills shortage that you have all alluded to. Is there anything that you want to add? We know there is a problem, but how are you addressing it and how much are you feeling it in what you are trying to do?

Jonathan Brearley: From my perspective, particularly as we are setting up this function, it is probably our principal challenge. There are two issues. One is just a general shortage of people, so you have to be thoughtful about the resource that you need and about the function that you are going to set up. Ofgem trying to learn and do everything is not a model that is going to work.

Secondly, we will have to be flexible about pay, because people can demand a huge amount in the market and we will need to make sure that we get the right skills in place.

Baroness Lane-Fox of Soho: Do you know what percentage of jobs are outstanding—as in, unfilled—in your sector in this area?

Jonathan Brearley: No, except that the market is incredibly tight. We do know that.

Steve Unger: It is a challenge. We are building capability incrementally, looking to recruit a small number of posts—two or three. The point there is not trying to replicate the skills and experience that already exist in the NCSC. Part of the trick here is to leverage that technical know-how. There is no point trying to replicate it. We need enough capability internally, though, so that we can have a sensible dialogue with the NCSC and that, when it comes to regulatory decisions, we can make decisions in an appropriate way.

So we are having to build up somewhat, but we are certainly not trying to duplicate the NCSC. In doing that, yes, there are not enough people in the UK to do what is required for the country as a whole. We face the challenge of competing with the private sector, which can generally pay

more. The way you handle that is by thinking creatively about how you recruit. We might have to develop a pipeline of recent graduates, for example. That is the kind of thing we are looking at. We are getting people who perhaps do not have the same level of experience that you might see in some private sector appointments, but you can help them develop.

There are things you can do, but it is difficult, and of course it is a sector-wide problem.

Baroness Lane-Fox of Soho: Do you feel the same in banking? It is quite a big statement: that we do not have enough people in the UK to keep the UK safe, effectively.

Steve Unger: I think there is common recognition.

Lyndon Nelson: It is always difficult to find skills. This area is not unique. The Bank has to deal with a number of these areas. There are a couple of things I might say, partly about mitigation. Our own cybersecurity person, who looks after the Bank's cybersecurity, would say that about 80% of his role is not technical; it is about behavioural change and staffing. I very much take my colleague's point that we do not necessarily need to fully replicate the technical expertise of the NCSC, but I completely agree that we need to leverage our own skill set.

Also, our CBEST test—this is quite an important element of it—is an accreditation scheme, so in effect it is outsourced through a properly managed channel of accreditation. It has been very successful for UK cyber experts, and that accreditation is now being used. We have been too successful, in a sense, so that other countries that now want to run their own penetration test have a ready-made resource.

It is constantly on my list. Sam Woods is the person you highlighted with regard to my performance metrics, and one of the questions I am constantly asked about is the resource level on the operational resilience team, which is where cyber fits in. We have some mitigation strategies in place to manage the skill set as much as we can.

Paul Smith: I guess it is no different in the water sector. Getting the right skills resource is a challenge, and it is probably slightly different from a regulatory position, because we are after the people who have the technical knowledge and capability to understand the vulnerabilities and the solutions and apply the appropriate controls.

We have tackled that in a number of ways. We have developed a lot of apprenticeship schemes and brought graduates in. We have reskilled engineers from traditional technology backgrounds and given them some cyber experience. Equally, we rely on the National Cyber Security Centre to provide some of the expertise that we might need.

Also, the point was made that we do a lot of education across the sector, so we share a lot of good practice and programmes of training so that our staff become more aware and we lessen the likelihood of an impact. So

you try to tackle it in both ways: by educating the population of employees, not just training the specialist.

Q30 **Lord Campbell of Pittenweem:** Can I take you back to penetration tests—a new concept in my understanding? Can you illustrate for us how one of these works typically? If you are doing pilots, I suspect that you tell the subjects in advance, but if you do not tell the subject in advance I suspect you tell them after a successful system of pilots has been examined. Are they erratic—that is not the right word—or even sporadic? Are they done at random in order to be effective? Can you give some illustration of exactly what the judgment is and how the test is carried out?

Lyndon Nelson: The tests as currently envisaged are not random, in the sense that the firm is aware.

Lord Campbell of Pittenweem: If it is a pilot, it would not make much sense.

Lyndon Nelson: Oh, no. Ours is not a pilot, ours is a live test. Theirs is a pilot. So the firm is aware that the test is being carried out, but clearly they do not know where and they do not know the range. The testers have to employ only legal and ethical means of getting in.

Lord Campbell of Pittenweem: If I may say so, a so-called enemy would not necessary employ legal or ethical means.

Lyndon Nelson: Indeed. We discussed some of the weaknesses of the programme. That is clearly one. But that is really about the external barrier. There are really two aspects of the way we carry out our test. First, if you are on the outside, can you break through the external barrier? The second element of the test is that they are literally let in through the external barrier and we see what they can find once they are in. Clearly, one needs the awareness of the firm to do that. That is how we currently do it.

There are suggestions of running what I think you were suggesting—a random on-the-spot test—but that would be of a different nature. We might, for example, run a test today assuming that you have lost your payment system or access to your clearing member. Can you take us through what would happen? That is how it is currently done. It is very much hidden. The firm is not aware of where the testers will go, but they are aware that they are being tested.

Lord Campbell of Pittenweem: Mr Unger, is your position different?

Steve Unger: It is similar. The firms are aware of the tests, but that does not mean that every individual at the firm is aware, because if they were they would fix the vulnerability. There is no doubt that running these types of penetration tests on a live network is something we need to do quite cautiously. I am aware that some of our European peers are doing similar testing, but not on live networks. They are, if you like, on dummy setups. Doing them on a live network is more challenging.

There is a fair bit that one can do. There are, for example, vulnerabilities that it is possible to scan for. If people are using poor passwords on certain elements of the network, it is possible to scan for certain vulnerabilities in a manner that identifies those vulnerabilities without affecting service. Clearly, as you design tests that affect service you need to be much more cautious about the way you implement them.

Lord Campbell of Pittenweem: In case you are too successful?

Steve Unger: Yes. On the other hand, we need to be successful enough to identify the vulnerability. Therein lies the tension.

Lord Campbell of Pittenweem: That is what is called the exercise of fine judgment.

The Chair: I am conscious that we are moving inexorably towards a vote in the House of Lords, but Ms Villiers, you have a group of questions that you wanted to ask.

Q31 **Theresa Villiers:** Yes. I have a question for you, Mr Brearley, concerning the incentives available to you as an economic regulator to encourage companies to improve their cyber resilience. Do you have sufficient flexibility to be able to take cybersecurity properly into account in your broader remit of setting prices and economic regulation?

Jonathan Brearley: There are two components to that. One is the existing price assessment—we call it the price control—where we allocate the money to network companies. To explain how this works, you end up with an overall agreement with a company that covers several things. There are many areas where companies do economically better than forecast and therefore make savings, so in this price control we are confident that companies have sufficient funding to be able to meet their cyber requirements.

With the next set of price controls, when you start this agreement again, which is from 2021 onwards, in effect you are in a slightly different world. This is an example of a number of areas in the energy market that are changing quite fast and will be in the 2020s. Therefore, I suspect that when we design the next set we will make them more flexible and allow more adaptability in the sorts of things that need to be done. That has still to be decided.

Theresa Villiers: Yes. We have certainly had evidence previously from industry players who felt that there was not sufficient flexibility for the investment they needed to make in cybersecurity to be reflected in their regulatory settlement.

Jonathan Brearley: I need to emphasise to this Committee that companies have sufficient funding with this price control. With this price control you do not agree what is spent where, but you have an overall agreement on funding. I come back to the point that there is plenty of flexibility in the current agreements for them to fund the investments they need.

Theresa Villiers: Mr Smith, what is your perception of the regulator that covers your industry? Is the system of economic regulation flexible enough to incentivise the investment in cybersecurity that you need?

Paul Smith: Historically, it has been quite prescribed around security, but from a more physical perspective you may have heard of the security and emergency measures direction, which is a framework for how we protect our critical assets. That has allowed price controls to have money put aside to protect those assets and build the appropriate security solutions.

As we move into price review, the changes are more to do with resilience. An element within that says that we need to look at organisational and operational resilience. Implicit in that is an element of, "Cyber is a risk to your business and you need to consider it from a resilience perspective". So there is a route through to providing funding for that.

Similarly, the regulation coming from the directive will also give a perspective on how we are to treat those assets, which may give another opportunity for some change in the regulatory position to allow for extra funding for anything that is outside the current scope of critical infrastructure.

Theresa Villiers: Mr Brearley, to come back to your point about looking to the future, how economic regulation interacts with cybersecurity may well need to change. Are you looking ahead at particular things so that in the future you might do things somewhat differently to reflect increased risk from cyberattack?

Jonathan Brearley: This is more generic in the energy system, where we are seeing very different ways of producing and transporting energy across our networks. Five or 10 years ago, there was a generator wired to a customer, but we now have a world in which we have batteries and customers are playing a much more interactive role in the market, which means that overall it is harder to predict. The cyber risk and the scale of funding that is needed for it is one of those uncertainties.

I suspect, although it is still to be decided in this next set of agreements, that we will have to have more things that look like reopeners, where we say, "We're not going to fix the level of funding for you at the start. We're going to allow you to come back in year 2 or year 5 of a price control and say what the need was". In that world, we do a sort of check to make sure that that is economic and efficient; we make sure that we are not funding something that is not sensible. Overall, it allows the price control to adapt more to the need as it comes along.

Theresa Villiers: One area of risk for cyberattacks is smart gadgets. Increasingly, more of those will be communicating with the energy networks. Do you get into this level of detail? Are you in dialogue with the firms that you regulate about minimising risk?

Jonathan Brearley: Absolutely. We have been involved in the smart meter programme, which looks at how we control our energy more interactively. The good news is that that system was built from the start with security in mind. The system that underpins it is separate from other networks and therefore only accessible by the suppliers.

The Data Communications Company does all the administration underneath that system. Therefore, we have a set of security protocols that the suppliers have to follow, which is set out in our legal licence requirements. We are already checking and monitoring what they are doing. A set of detailed codes sits underneath that describes what they are doing. We will be thinking about how that system works and overall how we adapt to the smart system as part of the next set of price controls.

Q32 **Theresa Villiers:** I would be happy to hear from any of the panellists on my last question. How confident are you that companies are prepared to come clean about when they have a problem with cybersecurity, talk to you about what has happened and enable lessons to be learned?

Jonathan Brearley: My view is that right now, given that we are in a world where we are moving to standards, companies are quite open. There are many different fora where they share best practice. We have a forum with National Grid and BEIS. There is an industry forum. There is a cybersecurity sub-committee, and the regulators have a forum in which they talk about cyber risks. At the moment, it is shared. The trick is to design an enforcement regime that does not curtail that. That is what we are trying to do.

Steve Unger: It varies by company. I echo the point that has just been made. We face a difficult balance between being an enforcement agency and wanting to collaborate. Generally, this works much better if operators feel that they are able to share information with us and to learn from that information. They will always be slightly hesitant to share information of certain types with an organisation that might enforce against them and potentially apply punitive fines.

At the moment, there are a few different mechanisms. There are information-sharing mechanisms within government, which in some ways are easier for operators to participate in than sharing information with regulators that might take enforcement action against them. We try to get that balance right, but they will always be slightly more nervous about what we as a regulator might do.

Lyndon Nelson: It is always important that these things are reported, both by people within the firms and by the firms themselves. I would say that there has been a significant improvement in the last couple of years. There was certainly an aspect of the market in which firms would not admit that they had been caught out. The fact that this is now so prevalent means that that is no longer the case.

One thing that I welcome is that the firms in the industry have made a step change not only in wanting to collaborate among themselves but in including the regulator and the NCSC. The large UK banks are considering an important initiative, which echoes what they see in the US, where banks share intelligence and vulnerabilities and the regulator and the security services are part of that conversation. I think it is getting better all the time.

Theresa Villiers: Mr Smith, any thoughts on how the water industry is in sharing its problems with cybersecurity?

Paul Smith: It is very good. From a sector point of view, we are very collaborative. There are lots of security forums and groups that will share best practice, events of note and understanding. We also make use of the government cyber information-sharing portal. We are close to NCSC and, through our strategic group, close with Defra and the DWI in understanding the threats and risks that we all face.

Lyndon Nelson: It is often difficult to know when a cyber event is actually a cyber event. Systems may break down because some change programme is going on. Sometimes the firms themselves genuinely do not know, so it may take a while. I think they are tending to over-report, but better that than the alternative.

Theresa Villiers: Yes. Thank you.

Q33 **Stephen Twigg:** I would like to ask about a non-regulatory incentive, which is cybersecurity insurance, on which we have taken some written evidence. What potential do you see for cyber insurance to change industry behaviour on cybersecurity? That question is for any of you.

Lyndon Nelson: We regulate some of these entities. We are now talking about insurance companies consciously taking on that risk. There is the possibility that companies have drawn a contract where they are vulnerable to cyber risk but they are not aware of it. Clearly, that is a concern for safety and standards. Where this is conscious, the evidence that we see is that that makes a difference to how the incident is managed.

The insurance company has an incentive to assist its customer in dealing with incidents, which often reduces the impact of the incident. In the US, for example, in relation to data privacy, one of the insurance companies that we regulate offers a service to its customers who may have lost data, advising them on how to manage that properly. That certainly reduces the reparatory impact to those customers in the US.

At the moment, this is a relatively positive issue. How it is priced is a major issue. You would expect a safety and standards regulator to want firms truly to be rewarded for the risk, but I think that this could have a very positive influence on this sector.

Steve Unger: I would prefer the companies that I regulate to take direct responsibility. I can understand that in some circumstances having a

third party vetting what you are doing means that there is a cost for getting it wrong. I get that, but I would rather that the major telcos that I regulate felt responsible for making sure that the networks are secured.

I have a concern about the extent to which some of those operators already outsource some operations. It is important that these companies retain a sufficient sense internally of the importance of this issue and their accountability for it. I can see circumstances in which these mechanisms help, but it is important that they do not undermine the sense of accountability within the companies themselves.

Stephen Twigg: Anything from the water industry point of view?

Paul Smith: We have been keeping a watching brief over the insurance piece for a couple of years now. Today, it is probably still a bit immature from an operational point of view as to how you might associate an assurance to an event on a network and try to link the two together. We will still keep a watching brief on that and will always look to see where we can add value. But it is not one of the tools in our protective control at the moment, because we would rather secure the asset than have an insurance policy to try to recover from that.

Q34 **Lord Brennan:** Will the NIS directive be enough, properly applied, to avoid inconsistent regulatory approaches? That is a general question reflecting two subsidiary ones.

For you gentlemen from Ofcom and Ofgem, Annexe 2 of the Government's response to the consultation on the NIS sets out the proposed competent authorities. It looks like a complete mishmash of England, Wales, Scotland, Northern Ireland, Ofcom, Ofgem, the water authority and so on. Can you reassure us that something coherent will come out of this?

Lastly, in the light of that mishmash, where are you with the Government and the devolved Administrations in seeking to ensure that you have a consistent and not fragmented approach? That question is for all of you.

Steve Unger: For me, it is very clear that we are the competent authority for internet infrastructure of the defined types. Clearly, different approaches have been taken in different sectors, but the most important thing is that in any given sector it is clear who is responsible.

In our case, we are clear that we are the responsible and competent authority. You would probably have to ask someone else how decisions have been reached in other sectors, but, as I say, the important thing is that we are clear about our responsibility.

Jonathan Brearley: The challenge for the Government has been that they are adapting this directive to a series of existing organisations. That perhaps leads them to take a variegated approach in different sectors. We, with BEIS, decided jointly to become the joint competent authority, because we felt that there was an existing role for BEIS in interpreting some of the guidance from the NCSC and being able to translate that to

the companies themselves. Equally, Ofgem has the powers and capacities to ensure that we do the enforcement.

Overall, there will be a varied approach across different sectors. Through the UK regulatory network, the regulators are working together on cyber risk and how to manage it, so what I would say on behalf of the three of us today is that that you are getting a set of common themes in understanding the problem and how we should generically address it.

Steve Unger: I would echo the importance of the UKRN, the UK Regulators Network, which was set up to ensure collaboration between different sectoral regulators. I think it may have been more active over the past year or so and that there is a working group looking at cyber issues, particularly around the implementation of NIS in a consistent way across sectors.

Lord Brennan: Anything to add from money and drink?

Paul Smith: From a water perspective, we have Defra and DWI as our competent authorities. That is quite a good position. In respect of Defra, we have been the regulatory controller in relation to our security measures for a long time now, while DWI understands our water business from a quality perspective. We are trying to safeguard against disruption to that. From a competence piece, they understand that it is good, but there is quite an education piece to go through to give them some understanding of the way cyber plays a part in the technology around operational networks.

When it comes to the high-level frameworks, the opportunity that we have along with other regulatory bodies is to make sure that the frameworks by which we assess each sector are similar, so that we can get some of that cross-sector collaboration and sharing going on. It should not be that different, but it can vary slightly if people look implicitly within their own sector for the controls they want to apply, because we are all linked at many levels.

The Chair: In at least two examples, you have talked about the government department and the regulator both being competent authorities. How will that be managed? I appreciate that it still has to happen, but it seems to me that there is a danger that one will assume that the other is doing it.

Jonathan Brearley: We are working closely to make sure that we have one integrated function between the two organisations. In a sense, we work with BEIS in a similar way where we are concerned about the physical security, for example, of these assets. It requires co-ordination and being joined up, but it allows us to play our respective roles more effectively.

In particular, BEIS can do its role of talking to the industry and translating some of this guidance, while we make sure that we can

enforce the sorts of things we need to when we think that companies are going off track.

The Chair: Is it clear how it will work with two competent authorities for water?

Paul Smith: Yes, the DWI will take the lead as the competent authority. There is also a day-to-day regulatory piece around that and we are obviously working with Defra on the outputs from it.

The Chair: Have any of you had any guidance as to what happens following Brexit with the network and information systems directive?

Jonathan Brearley: The Government's own publications set out an expectation that the UK would continue to have the NIS directive. Clearly, some elements of it might be subject to negotiation but I think there was a clear statement in their publications that they expect to continue with these arrangements.

The Chair: On that note, there is a Division in the Lords so we stand adjourned for about 10 to 15 minutes. My apologies to you.

The Committee suspended for a Division in the House of Lords.

The Chair: I think we can go back in session, although there are one or two Members still making their way back. We had neatly finished one round of questioning, so I can call on Lord Trimble.

Q35 **Lord Trimble:** Gentlemen, a couple of minutes ago you referred to the UK Regulators Network. We have been briefed to the effect that the UKRN undertook a review of cross-sector resilience, including cybersecurity, starting in 2015.

My question is quite simple. Can you talk to us about that review and maybe broaden it into the question of the exchange of information and best practice and so on?

Steve Unger: I can touch on that briefly. It was a rather broad review, which I think we led. We looked at a range of issues to do with cross-sector dependency. Our focus at that time was on the interdependence of communications networks on power, which is rather outside of this discussion. It touched on cyber and the risk that comms networks might be compromised in a way that impacted on other infrastructure. Some of that learning is what has been subsequently taken forward through NIS, but I do not think cyber was the main focus of that review.

Jonathan Brearley: That is the forum in which we will try to help form the standards that we apply and make sure that we have the same sort of auditing and checking processes that others have. That is the place you go to make sure that what you are doing is consistent with others and is best practice. It is the place you go to make sure that you are doing the best you can in this area. As I say, in setting up a new function, that is going to be a great resource.

Steve Unger: It is worth distinguishing between that and the general role of the UK. Over the last year, UKRN has been doing a lot of work on cyber. It has been playing a key role in making sure we are ready for NIS. I think the 2015 review you referred to was rather broader.

Lord Trimble: Do you think that more should be done to share best practice and information? In particular, is there anything the Government could do to ensure better information sharing?

Jonathan Brearley: To be honest, I think it is a job for the regulators to get on and do. Frankly, I think we would all agree across the board that there is more that we can do to work together. I do not think this is necessarily something that we need government to help us with.

Paul Smith: As an operator and a trade industry body we would certainly welcome more information and more collaboration across different sectors to bring into our thinking and make sure that we can apply the right controls.

Steve Unger: I might add that information sharing is important, both within the UK but also for understanding internationally what else is going on. EASA, for example, is a European agency that allows different regulators across Europe to share best practice. There are similar exchanges of information with other countries, notably the US. I think that type of sharing of expertise is also important.

Lyndon Nelson: The biggest request on the financial services side, because of the international nature of the market, is for co-ordination among the biggest regulators across the planet. That is really why we try to put as much effort into the G7 Cyber Expert Group as we can, to make sure that people face off against a similar range of criteria and regulations across their businesses.

The Chair: Do you think that the UK Regulators Network has the resources it needs, both financially and in skills, to carry out the co-ordinating function between the regulators in this area?

Jonathan Brearley: From a personal perspective, I think the UKRN is the organisation that pulls us together to exchange our best practice. Again, we have to be thoughtful about where we are putting the expertise that sits underneath that. I see them more as facilitators than trying to drive the analysis themselves.

Steve Unger: I echo that. The resources come from us. The UKRN's role is to bring us together. The expertise, the detail, has to be rooted in our knowledge and understanding, brought together by the UKRN.

Q36 **Lord Powell of Bayswater:** This last section is about relations with government. In a sense, we have covered some of it already.

On the whole, our impression from an earlier evidence session and from the written evidence is that you are pretty satisfied generally with relations with the NCSC and it is working out pretty well. One or two

people have mentioned in evidence possible tensions between conflicting priorities—for instance, between intelligence gathering and continuity of energy supply or safe operation of services, as in the NHS. Have you encountered any of those tensions? Would you expect to encounter them? That is an open question for anyone.

Jonathan Brearley: So far, I do not think we have. The industry is heavily reliant on the NCSC. We talked about the next price control, the next financial agreement. Inevitably, there is always a debate about what consumers should be bearing and how much they should be paying towards that. I suspect that will be an area of debate between us, but overall I think the relationship between the NCSC, BEIS and us can work quite well.

Steve Unger: I think that is right. The tension that exists is the obvious one. It is that there is a set of judgment calls about how much of the UK's resources go into protecting ourselves against this threat. That is the type of judgment that people have to make all the time across all sorts of different risks. The important thing is that the companies we regulate do that in an appropriate way and that we are aware of the types of decisions they are making in those risk assessments.

Lyndon Nelson: I think the relationship is very good. In all the years I have done regulation, it is possibly one of the better co-ordinated matters. You are quite right, though, that the responsibilities are different. The existing regulatory structure is largely established by dealing with consequences—the conduct authority, consumers, me, safety and standards—whereas the NCSC is more about the causes: the cyber event or maybe a criminal case that involves the NCA.

We have definitely brought them into existing structures. There were some tensions but very early on in the existence of the organisation, almost first out of the gate, but I would say that the relationship is very good. We have secondees now with the NCSC trying to share information and our reaction function, so I am very positive about the relationship.

Paul Smith: Likewise, the water sector sees it as a collaborative approach with the NCSC. Initially, there was probably a bit of a set-up along the way when it was trying to get itself established and a bit more formalised and structured in dealing with the different sectors. That has definitely changed, and we are now very much on the same page trying to understand the threats that we all face.

I guess as we go forward we would like more meaningful detail on the real threats that we face in each sector. The water sector is still classified as a low threat, but the rest of the UK tends to be on a high level of threat, so we need to understand the nuances as to why it is different, but by and large it is quite good.

Q37 **Lord Powell of Bayswater:** Lastly, to give you a free shot, what would be your wish list from government? What more would you like to see them do to help you establish cyber resilience across your industries? Do

not hold back.

Paul Smith: I think from a sector point of view, as I have just explained, we would like a bit more meaningful information about the true source of this threat. Perhaps they could offer more protective controls as a service—to stop those things coming towards us rather than telling us to deal with them when they arrive. If these are coming through national interfaces and through our networks, should they arrive at the operator? Can we do something to prevent them getting that far before we have to deal with them?

Beyond that, it is more a case of working with us closely to understand the challenges that each of us faces in our business day to day and look at policies and regulation to help us improve those areas we need to improve.

Lyndon Nelson: One of the emerging issues for us is third parties. A number of firms are outsourcing the control that they can exhibit there. In some of these markets there are very few suppliers, so I suspect that with government—we are doing this at the G7 point as well—by buying power we can influence some of these providers to make sure that we understand the cyber vulnerabilities as well as the advantages that they bring through outsourcing.

Jonathan Brearley: From my perspective, a lot of it is about emphasising what is being done, such as fast, comprehensive information to the companies and their working closely with us so that, where we start facing issues in enforcement cases, we work jointly to make sure that those are addressed quickly.

It is more about the shared challenge, actually: how do we deal with this fast-moving change and risk, and how do we create a framework that does not leave the companies just ticking a set of boxes and then standing back and that is also not too rigid to adjust to something that is moving so fast?

Steve Unger: I echo the other comments. I think we all recognise that all this goes in only one direction. The concern about cyber is increasing across all sectors. We are all on a journey, and it is important that we are pragmatic on that journey about what can be achieved given the constraints on resourcing and on the international supply chains, and so on.

Together with government we need to find a way of upping our game in this area in what is ultimately an arms race, but doing so in a way that is still deliverable and not kidding ourselves that there is a silver bullet in any of this.

Q38 **Lord King of Bridgwater:** Following up Lord Powell's question, we all know what a growing and potentially very serious situation we could face. Have each of you attended meetings held by your relevant Secretaries of State?

Jonathan Brearley: As Ofgem, we have regular meetings on the security of supply, as part of a tripartite relationship that involves my chief executive and the Secretary of State, but most of our interactions frankly are with the officials who are running this.

Steve Unger: In the past, I have attended various meetings with various Secretaries of State on this matter.

Lord King of Bridgwater: I am talking about the current situation. Have you had meetings in the last year?

Steve Unger: Not in the last year.

Lyndon Nelson: It is an important issue on the Governor's agenda. He has a regular bilateral with the Secretary of the Treasury in the US, as well as with the Chancellor, obviously. So I am pretty comfortable that we have the right access and that communication is happening now.

Paul Smith: On water, I guess most of our interaction comes through Defra rather than the Secretary of State, although that is on behalf of the Secretary of State, I guess, in that respect.

Lord Campbell of Pittenweem: What about the devolved Administrations? Is it similar, or better, or worse?

Jonathan Brearley: We talk to the Administrations about security of supply and the risks, but it is most at official level. I need to check that.

Steve Unger: We have certainly spoken to the devolved authorities, particularly on physical resilience issues. The cyber issues tend to be similar across the UK. Some of the physical resilience issues in the north of Scotland, for example, are more severe than here, and we engage with the relevant authorities on those.

Lyndon Nelson: I am not aware of anything, but I can obviously write if there is.

Paul Smith: From a Water UK perspective and security group, yes, we very much talk with them, but I am not aware of there being any high-level ministerial engagement.

Lord Campbell of Pittenweem: Do you go to them and do they come to you?

Steve Unger: If there is a major incident, they certainly all come to us.

Lord Campbell of Pittenweem: Point taken. Thank you.

The Chair: Finally, you were asked earlier what kept you awake. Do any of you see anything that we have not referred to as being a looming challenge? It does not yet keep you awake because it has not arrived, but you see it there. I am talking obviously about the cyber resilience field. Is any looming challenge out there that we need to start thinking about soon?

Jonathan Brearley: For energy, I come back to the changes that are going on inside the market. We are potentially seeing worlds in which in five or 10 years' time there will be much more local peer-to-peer trading, potentially between households. You may have seen some of the offers that some of the energy companies are offering, such as using car batteries and selling car-battery solutions back into the grid with electric vehicles.

In that world, where you have a much more disaggregated system, over time we have to make sure that the resilience of that system is also there. That means thinking hard about what a more devolved energy system looks like and therefore how you make sure that is secure.

Lyndon Nelson: I have mentioned the role of third parties. One of the challenges is how we deal with that. The other is that disruption has many causes, and firms changing systems is one of the major vulnerabilities. We are, of course, importing quite a lot of change into the financial system through structural reform and other matters. How much change we are imposing on the sector is one issue that I take a lot of notice of.

Steve Unger: A trend that we have not touched on so much is the internet of things. There were a couple of comments on it. So far, security has been very much about protecting communications between people and traditional business communications. With the internet of things we can expect to see billions of devices. How many depends on how much you buy into the hype, but there is no doubt that there will be a very large number of connected devices embedded in all sorts of other systems in other sectors. Making sure that those systems are designed from the start to be appropriately secure and dealing appropriately with privacy issues will be a big challenge. It is one that people are aware of, but it is certainly one that I worry about.

Paul Smith: From a water perspective, similarly, there are elements of competition. Last year there was an opening up of the business retail market to competition, and there is talk of future domestic competition, even in the wholesale operation—the upstream/downstream-type aspects of the production of water and the removal of waste water. There is a challenge there in making sure that consistency of controls are applied across whatever framework of partners that brings into the equation.

The Chair: Thank you very much indeed. You have all been very helpful. That concludes our session.