Joint Committee on the National Security Strategy

Oral evidence
Cyber Security: Critical National Infrastructure

Monday 25 June 2018

4.20 pm

Watch the meeting

Members present: Dame Margaret Beckett (Chair); Lord Brennan; Lord Campbell of Pittenweem; James Gray; Lord Hamilton of Epsom; Baroness Healy of Primrose Hill; Baroness Henig; Lord King of Bridgwater; Baroness Lane-Fox of Soho; Dr Julian Lewis; Lord Powell of Bayswater; Lord Trimble; Theresa Villiers.

Evidence Session No. 4 Heard in Public Questions 54 – 63

Witnesses

I: Rt Hon David Lidington MP, Chancellor of the Duchy of Lancaster; Mr Ciaran Martin, Chief Executive Officer, National Cyber Security Centre.

Examination of witnesses

David Lidington MP and Ciaran Martin.

Q54 **The Chair:** Mr Lidington and Mr Martin, thank you very much indeed for coming. You are very welcome to the Committee and we are looking forward to your evidence. I understand that you are willing to go into private session later on for about 20 minutes. I will say when we are going to do that. Let us begin by looking at the National Cyber Security Strategy that was published in 2016. That was a change from the strategy published in 2011. We are now in 2018—how has the threat to CNI changed since that 2016 strategy was published?

David Lidington MP: It continues to increase and the character of the threat continues to evolve. We are seeing a range of cyber threats from both nation states and cybercriminals; a rising level of threat, with more frequent and more complex attacks; and more sectors that we can identify as being at risk. Last year we saw attacks on what we would term CNI in the health, media, telecoms and energy sectors. We have also become more aware in the last two years of the potential vulnerability of CNI supply chains as a target for attack. Inevitably when you are dealing with complex supply chains where, as the WannaCry attack on the NHS last year demonstrated, something as small-scale as the wrong privately owned memory stick being inserted into a workplace computer can infect a significant network, it is important that we get a greater grip on those supply chains. We have also started to become even more aware than we were two years ago of the capacities of certain state actors and their readiness to use that cyber capability. Ciaran will probably be able to say a bit more on that.

Ciaran Martin: I endorse everything that the Minister has said about the threat. In terms of the behaviour of threat actors, in the past two years we have seen a consistent rise in Russia's appetite for attack on critical sectors, as well as a diversification in the sectors that it might attack. So in addition to what you might call more traditional targeting of hard infrastructure such as energy infrastructure, we have seen against the West as a whole the targeting of softer-power democratic institutions, media institutions and things relating to freedom of speech. On other state actors, we have seen a diversification by North Korea away from what might be called political retaliation attacks to, frankly, the theft of money, which was what we believe to have been behind the WannaCry attack.

Not all the trends are going upwards. We have seen an evolution of cybercrime, where some of the most sophisticated attackers are now operating at almost nation-state level. There is also a risk of proliferation. There is now a highly developed market in cyberattack tools and techniques—things such as money-laundering capabilities, data-mining capabilities, and so forth—so states of more modest means can acquire those capabilities; and, providing the cybercrime group is based in an area where western law enforcement arrangements do not apply, organised criminal groups can continue to threaten us.

Finally, in 2017 we learned to watch out for the reckless as well as the deliberate. With two of the most serious attacks of 2017—WannaCry, which affected us here as well as a number of other countries, and NotPetya, which started out as a Russian attack on Ukrainian infrastructure but spread rapidly into large numbers of western companies that do business in that country—the impact went well beyond the intentions of the attacker. So that is something we need to be wary of as we seek to protect our systems.

Q55 **The Chair:** Good point. In that 2016 strategy, a number of objectives were set. How are you measuring progress towards those objectives, and how and when do you intend to report on them?

Ciaran Martin: Interestingly, cybersecurity, despite its grounding in modern technology, has been the subject of relatively small amounts of performance data internationally, so we are seeking to develop those performance measures. The National Cyber Security Centre has committed to publishing an annual review which is fully public and bodies such as the Committee can take evidence on it.

A specific innovation we have made is a pioneering programme that is being looked at internationally called Active Cyber Defence, in which we seek to make the internet automatically safer but also to publish evidence in support of those tests. We do a series of pilots—for example, on anti-spoofing measures—and on 5 February this year we published a detailed 70-page report, *Active Cyber Defence—One Year On*, full of those early metrics, trying to show what worked and what did not work, and therefore what we would like to see further uptake of, both elsewhere in government and in the private sector. There is a range of activity going on.

The National Cyber Security Centre is an organisation that seeks to be transparent as a default. There are some things that we cannot get into, but with the annual report, the Active Cyber Defence reviews and a range of other metrics, we are seeking to move the debate on.

David Lidington MP: On the question of reporting to Parliament, it depends quite a bit on how Parliament itself wants to address these issues. Clearly, there is a place for this Committee to continue to monitor the Government's overall cyber strategy. Every department has its own Select Committee and it seems that it would be perfectly proper for a departmental Select Committee to inquire into the cyber preparedness of an individual department or service. Obviously, the ISC has its own particular role.

Q56 **Lord Powell of Bayswater:** Just before I ask my question, I need to add to my declaration of interests that I am a member of the advisory board of Thales, the French defence company. Minister, one or two witnesses have told us that there should be more transparency about the way in which the £1.9 billion is being spent; in particular, what projects are being undertaken in relation to critical national infrastructure. Obviously, you will want to keep some of it under wraps, and that is quite

understandable, but can you give us a slightly clearer picture of exactly how this money is being spent in relation to CNI?

David Lidington MP: Not easily within the approach that the Government have collectively determined of not disclosing further details beyond the £1.9 billion. The reason for our reluctance is that, while there would certainly be some elements of that £1.9 billion that, while important, might not merit the highest degree of classification, the more information we give which allows both criminals and hostile state actors to subtract from the £1.9 billion and work out what we might be spending elsewhere and what that sum might be buying us, the more the risk increases. It is really to try to minimise that risk of our enemies finding out more about our plans and preparedness that we are very cautious about the level of information that we divulge.

Lord Powell of Bayswater: It is quite a large sum to keep under wraps.

Ciaran Martin: Your question was about critical national infrastructure protection. There is an issue about the extent to which public spending on that is a meaningful indicator of what is happening. This is not just about a reluctance to disclose for security reasons. I will give one example of a company that I would rather not name, for reasons of commercial sensitivity—it would not want me to name it—but it is a critically important company under any definition that one could think of. After an incident in 2014, this company, based on our advice, spent more than £300 million on a cybersecurity infrastructure modernisation programme. That is completely off the public books because it is necessary private investment by the company for its own means. Whether we can find a way of measuring this I do not yet know, but one of the most important things we need to try to influence and make a success of as a country is increased private sector investment, which is key to protecting most of the critical national infrastructure.

David Lidington MP: The question raises the whole issue of the distinction between the responsibilities of government and the responsibilities of CNI operators themselves. Obviously, while it is our job to tell the operators and our contractors our assessment of the threat, the things they should guard against and the standards that we expect them to maintain, at the end of the day it will be down to the directors and operational management of those companies to ensure that those precautions are implemented. I announced earlier today some ways in which we are intending to make the strategic government suppliers—the main contractors—adhere to higher cybersecurity standards as a matter of course in future and try to police those through their supply chains.

Lord Powell of Bayswater: As a director of many companies, I understand that, but I would have thought there was still scope to give at least some generic examples of the sorts of activities which the Government are conducting under this programme. We need to demonstrate, and have sought, accountability on this. It would be helpful if general descriptions of the activities, where possible, were released.

Ciaran Martin: I am happy to try to do two things. First, I can give you an overview of the National Cyber Security Centre spend and the direction of travel of that; and, secondly, I can give you some examples of the priority critical national infrastructure programmes that we are prepared to do, if that would help the Committee.

In budget terms, we have three main sources of funding: the GCHQ core funding, which is largely staffing and does not count the dual-use capabilities that the wider GCHQ uses for intelligence as well as cybersecurity purposes; the National Cyber Security Programme; and other funding, including a range of funding from the Ministry of Defence. In 2016-17, that all added up to £158 million. Over the course of the spending review period to 2021, that becomes £285 million. That is spending on the centre, which is not the totality, of course, of government cybersecurity spending.

On the critical national infrastructure priority work, there is a sub-committee of the National Security Council that determines the priority programmes. Over the past few years, priority programmes have included, in the public sector, the cyber resilience of universal credit, and, in the private sector, smart meters. The current priority programmes are the Bank of England's real-time gross settlement system; the new social security payments system in Scotland; the civil nuclear investment decisions last year, which were influenced by us and will continue to be on an ongoing basis; and a range of other projects in aviation, finance and telecoms that we can talk about.

Q57 **Lord Powell of Bayswater:** That is a step forward, and I am grateful for that.

One additional question: all our witnesses have talked about the importance of co-operation with Europe in this field. Minister, could you tell us a bit about what negotiations there have been with Europe to co-operate in this field and whether they have revealed the same rather dog-in-the-manger attitude which has come forward on the space programme and one or two other areas, where we would like to be co-operating with Europe?

David Lidington MP: Obviously, as you know, Article 4 of the Treaty on European Union excludes matters affecting national security from the remit of EU-level activity, including the jurisdiction of the court. So there is a set of relationships that sit apart from it. Without going into any detail on the negotiations, we remain very clearly of the view that an ambitious and systemic pattern of intense co-operation between us and the EU 27 is in the national security—including CNI—interests of all of us. I think that view is shared by a number of EU member states. On this general issue—I would not single out the CNI question—there are what I would describe as doctrinal issues with the EU institutions, which we hope we can find a way to overcome; otherwise, it amounts to a deliberate decision by the EU negotiators to put EU citizens at greater risk than they are at the moment. Of course, on the day that we leave the European Union we shall fully conform to European law in respect of data. We have

implemented the GDPR on the protection of data, and we are in the process of implementing the NIS directive. We will continue to do what we regard as the right thing, and we hope very much and believe that at the end of the day our partners will recognise that it is in their interests to work with us on this.

Q58 **Lord Hamilton of Epsom:** I want to ask about responsibility for the overall national security strategy. You have taken responsibility for this only quite recently. There was a two-year lapse when nobody was responsible for it at all. One gets the impression that it is a very low priority for the Government because you did not have a Minister in charge of this, and we feel it is rather a poor orphan when it comes to the Government—nobody seems to want to take responsibility for it at all.

David Lidington MP: I reject the implication of your provocative question, Lord Hamilton, if I can put it that way. The National Security Council has overall responsibility for our national security strategy in all its forms, including the cyber aspects. The point about the NSC is that it brings Ministers together and, in its official configuration, the senior officials with responsibility for each aspect. Ciaran in the National Cyber Security Centre, I with my responsibilities for that, the Home Secretary with his lead on the cybersecurity response and the Defence Secretary in terms of this country's offensive cyber capability all follow the overall strategic remit set by the National Security Council chaired by the Prime Minister.

Lord Hamilton of Epsom: Yes, but of course it is not really chaired by the Prime Minister; it is chaired by the Home Secretary, is it not?

David Lidington MP: No, the National Security Council is chaired by the Prime Minister.

Lord Hamilton of Epsom: Is it? Oh, right. But it does seem to me that all the responsibility is so spread around that nobody is responsible for anything by the time you finish. Why is there no longer a National Security Council sub-committee dedicated to cybersecurity?

David Lidington MP: We put the cybersecurity into a particular National Security Council sub-committee, so there is a responsibility there.

Ciaran Martin: On the general question, the National Security Council, in my experience, has taken cybersecurity extremely seriously, as have the Government as a whole in spending reviews. We have consistently rising funding, strategic stability and the right balance, in my view, between organisational autonomy to get on with what we need to do and ministerial sponsorship. There is a division of responsibilities because the Chancellor of the Duchy of Lancaster is responsible for the strategy; the Home Secretary is responsible for a cyber emergency, as he is for all major domestic security incidents; and of course, there is close alignment with the Department for Digital, Culture, Media and Sport on the wider technological piece.

With regard to ministerial interests, the Chancellor of the Duchy of Lancaster and the Home Secretary are briefed fortnightly—and that always happens—on the latest operational threats. That lasts around an hour, going through everything that we do. It is frequently on the National Security Council agenda and those of its sub-committees, whether as an item in its own right or when we talk about Russia or any area of interest where there is a strong cyber dimension. I feel that there is strong ministerial support for and ownership of the NCSC and the wider cybersecurity agenda more generally.

Lord King of Bridgwater: May I just clarify a point? You said that the offensive capability falls to the Ministry of Defence?

David Lidington MP: Yes, that is right.

Lord King of Bridgwater: Would it not be led by GCHQ? Would that not be answerable to the Foreign Office?

Ciaran Martin: The emerging framework for offensive cyber is still in development because it is a relatively new set of capabilities, and it involves everything from effects that would constitute the use of armed force in international law all the way through to the sorts of operations that you will be familiar with from your time chairing the ISC, Lord King. Given that that involves a mix of effects, there is formal and close joint partnership between the Ministry of Defence and GCHQ, and authorisations will operate and alternate accordingly.

David Lidington MP: The Defence Secretary has overall responsibility for the development of our offensive cyber capability but the Foreign Secretary, as Lord King says, has a statutory responsibility for GCHQ. The two have to work together.

Q59 **Theresa Villiers MP:** Can I ask about the reporting structures for the departments that have responsibility for critical national infrastructure? Obviously, there is a fairly extensive list of government departments that have a remit in relation to security and CNI. Could either of you tell us how often Ministers report to you on cybersecurity resilience in their sectors? What do they report on—what are you judging them on?

David Lidington MP: There are different ways in which this happens. Each lead department has a responsibility to identify the CNI that is within its area of responsibility and to take the appropriate action with regard to the operators or suppliers of CNI and critical services. Departments get Cabinet Office guidance and direct support from Ciaran and the NCSC, as well as from the CPNI. They have a duty to keep the risk to their sectors under review and to report on how they prioritise those risks and their intentions to manage them through an annual formal sector security and resilience plan, and we publish summaries of those on GOV.UK. In doing that work, each department looks to the national risk assessment and to the advice provided by risk owners across government. Basically, it is each department's job to assess the criticality and vulnerability of particular CNI operations.

On how we deal with this collectively, the National Security Council has a sub-committee on threats, hazards, resilience and contingencies. The secretariat to the NSC, working under Mark Sedwill but in conjunction with Ciaran and his team, try to spot if there are particular problems or challenges facing departments. A lot of this will be put right by appropriate action from departmental officials and specialist agencies. We have meetings of the sub-committee every few months, with a fair number of departments represented around the table—I cannot remember the total offhand. We then address issues, usually on the basis that the national risk assessment or our expert advisers have flagged that a particular subject merits ministerial attention. That happens when there is something on the table in which more than one or two departments are involved, where we need to get the whole of government focused and ensure that the planning has been done for a particular contingency.

Theresa Villiers MP: Which department do you think is best prepared and which is least well prepared in terms of those responsibilities?

David Lidington MP: Ah. You give me the impartial view on that. It is a bit difficult.

Ciaran Martin: This is all about risk. One of the most important things is that we are in the process of doing tailored risk profiles for different departments. For example, the Department for Work and Pensions has relatively little to worry about from the big state actors and an awful lot to worry about from cybercriminals in terms of personal data and money. For the Foreign and Commonwealth Office, it is probably the opposite, although with visa databases and that sort of thing you need to watch out for the criminal risk. For the Home Office, it is a combination of the lot. Those different risk profiles lead to different defence needs. As you would probably expect, I am not going to name and shame individual departments.

There is an issue about sectors, given the inquiry into critical national infrastructure. The one sector, regulated by the Government through the Bank of England and the private sector, where it has worked well as a whole and we need to look at more to see how we can replicate it is finance. There are all sorts of reasons for that. One is money: it is a sector that has very large companies with a lot of money. Another is that the competitive dimension to that market does not include security: banks do not compete on security; they tend to look at it as a shared systemic risk. Another is that their business model has meant that things such as controls on insider trading and fat-finger mistakes and so forth mean that they are quite savvy about IT resilience anyway. Added to that, the Treasury takes that seriously as a policy issue. The Bank of England has said this is a core part of operational resilience regulation. That model has worked quite well. In other sectors we are struggling to get that sort of virtuous circle going.

Theresa Villiers MP: I suppose I was not really expecting you to answer the question. I appreciate that with different departments you are not

necessarily comparing like with like, but do you have some kind of ranking system of the departments in terms of preparedness?

Ciaran Martin: We have internal metrics on things such as the uptake of particular new techniques that we have developed for government, such as the automated defence measures on protecting the integrity of your domain name; in other words, this is from HMRC rather than somebody pretending to be HMRC. We know who has taken that up and who has not, so we have data like that.

The Cabinet Office secretariat that the Minister referred to asks in an annual survey for updates on cyber-incident handling plans, and of course we would input into that. We gather data on things such as redundant domains. If an organisation changes its name or is abolished or modified, if you leave the domain identity, that gives more of an attack surface. That should be cleaned up and we know which departments are better than others at doing that. We try to share some of that best practice and to publish some of the data in aggregate. Currently, we are not convinced of the merits of external league tables and so forth.

David Lidington MP: Part of the problem is that, because the nature of the threat keeps evolving, we can never be complacent. I agree with Ciaran that because of what it has had to do anyway the financial sector has a pretty good track record, but I am not going to put my hand on my heart and say that that means it is safe, because there will be organisations right now trying to work out how to get round the security measures that big financial institutions have put in place.

An important point is that this is not just a matter of the Government or big companies setting overall metrics. The challenge is to effect cultural change right the way through an organisation, whether we are talking about junior civil servants—perhaps in offices a long way from London—NHS employees, bank employees or energy company employees. We set up the National Cyber Security Centre—unprecedentedly, with one foot in intelligence but the other in the public-facing arena—precisely so that it could give expert, credible advice on best practice to both private and public sector organisations to try to drive up overall awareness and standards. That is one of the biggest challenges we face.

Theresa Villiers MP: How do you approach the inevitable big knowledge gap among Ministers and senior civil servants who are trying to hold to account the various organisations that are delivering these things in practice? With the best will in the world, cybersecurity is a phenomenally complex technical area and no matter how effective your Ministers and senior civil servants are, they will not have that technical know-how. How are the Government equipping them with the tools to hold to account the agencies for which they are responsible?

Ciaran Martin: The answer is to simplify it. I am deadly serious about that. We tell CEOs this, and we give the same message to Ministers and senior civil servants about government. This is about operational risk in the department. Whether that is managing an actual hazard or a terrorist

risk, cybersecurity should lend itself to the same intellectual and practical approach.

I will give you a specific example relating to bulk data holding. Last year, in the light of some very serious cyberattacks in the US against US government entities, we published 15 principles for departments that handle bulk data. That was aimed at board and ministerial level so that they could ask the questions. This is at the slightly more technical end of things. If you have a bulk data holding, you will have a systems administrator. It is useful for the board or at least somebody on the board to know who that is. But is the account they are using to administer the system for bulk data holding the same account that they use for normal, internet-facing business? That is a question that any competent Minister, senior official, chief executive or non-executive board member should be able to ask and understand the answer to. If the answer is yes, they are using the same account, that is the reddest of red flags and it needs to be taken really seriously. We have given very practical steps such as that. The mantra that we constantly give to leaders of whatever hue is that you do not walk away from the meeting or the discussion if you cannot understand what you have been told because that is a business risk.

Theresa Villiers MP: Thank you. You have said that you take a rigorous approach to Ministers and their responsibilities in relation to CNI. What is the relationship like with Ministers in the devolved Administrations? Are you able to be as exacting in what you ask of them as you are with Whitehall Ministers?

David Lidington MP: Obviously where we are touching on matters that are reserved under the devolution settlements, that is a UK government responsibility. We certainly have had no resistance from any of the devolved Administrations to what we have needed to do there. Where a power is conferred on the devolved Administration, that is a matter for them. But again, there is a very good and effective working relationship between the officials in both the Welsh and Scottish Governments and the National Cyber Security Centre and others in Whitehall involved in this work. It is not a matter on which I have ever had any cross words with any Minister in either of the devolved Governments.

Lord Hamilton of Epsom: On CNI, are you concerned that there may be "sleeper" bugs in computer systems that can be triggered at some later date at the will of some national Government who want to mess everything up at some time of their choosing?

Ciaran Martin: I agree with the first part but will pause on the second part. I agree that we are concerned about lurking hostile presences on networks. Does that mean that they can automatically and immediately turn hostile? That is a bit more complicated. At the end of April, we published a landmark report with the US Government on sustained Russian presence in UK and US internet infrastructure. That is different from an attack; it is more like a campaign—it is a foothold, an intrusion that you can use for ongoing espionage purposes or can develop as the

potential for a hostile, disruptive and destructive act in the future. The purpose of that guidance was to tell our companies and government organisations how to spot that, what the technical indicators were and how to get rid of it. That is an important part.

It is more complicated than saying that that presence can automatically be used to cause serious harm. It could in relatively short order be used to cause nuisance disruption to services. It is not as easy to turn off the power station supply as Hollywood movies sometimes make out. However, for a serious destructive attack of that nature, it is a necessary but not sufficient condition to have that landing point. That is why we would worry about lurking presences and that is why we publish lots of technical data about how to spot them and get rid of them. I do not want to be overly alarmist about how quickly and how clandestinely those can be turned into the most devastating of cyber capabilities, but it is very much an area of concern, yes.

Lord Campbell of Pittenweem: I am trying to get my head round this. As I understand it, your responsibility is to advise on best practice. Government departments are perhaps in a different category—you can have sanctions within government—but what sanctions do you have if a company declines to accept your advice, or accepts it but then does not fulfil it?

David Lidington MP: When it comes to government contractors, we have announced today that from now on we will write into all contracts a requirement for certain minimum cybersecurity standards, not only to be observed but to be implemented. It will be for the main contractor to provide assurance that it knows enough about its supply chain and the risks in its supply chain to make sure that CNI for which that contractor is responsible is not put at risk in a way that is preventable. We are also implementing what I would describe as the cybersecurity equivalent of a credit rating, so we try to assess each of our main suppliers against those standards. This all involves co-operation by suppliers. But what they stand to lose is their ability to succeed in tendering for government business in the future.

Lord Campbell of Pittenweem: So the obligation is a contractual one; it is not statutory.

Ciaran Martin: Some of it is.

Lord Campbell of Pittenweem: Could you explain which?

Ciaran Martin: In the area of personal data holding, which is obviously a huge area of cyberattack, data protection law applies—both domestic law and, since last month, the GDPR. That is mandatory and statutory regulation of a whole swathe of at-risk activity and there is no need for a new cybersecurity-specific regulation on top of that. As already mentioned, in the financial sector it is woven into the statutory regulatory framework overseen by the Bank of England. The same is also true of civil nuclear.

The corollary of the GDPR for critical national infrastructure is something called the network information systems—NIS—directive. It came in simultaneously from Europe and has been applied in the UK. That mandates a certain amount of minimum standards in cybersecurity, including in governance, with statutory enforcement mechanisms. So in addition to the existing and newly announced contractual measures that the Minister mentioned, there is a whole tapestry of other regulatory and enforcement mechanisms.

Some of this also depends on voluntary co-operation. If I ever felt that there was a systemic problem with critically important companies not co-operating, I would go to the National Security Council and to the Minister and make appropriate recommendations, but I have not had cause to do that yet.

Lord Campbell of Pittenweem: You have not had any experience of that so far?

Ciaran Martin: No.

David Lidington MP: We are applying the NIS directive in our own legislation to five key sectors: water, energy, transport, health and digital infrastructure. We are trying to make the requirements under the directive outcome based, rather than simply ticking a set of boxes. But the penalties for breach are pretty severe. If an operator of essential services or its digital service providers do not put in place adequate measures to protect systems, enforcement action could lead to potential financial penalties of up to £17 million. We are expecting around 500 organisations that operate essential services and about 200 digital service providers to be in scope for this. We are going to have another look at our approach to implementing the directive in two years' time to see whether we need to take any further steps. Obviously, we want not to be in the situation where we are trying to impose penalties but to drive changes in behaviour and alertness among the operators and digital service providers, just as the new measures we are putting in place in respect of contractors are intended to drive a change of alertness and behaviour, not just in the main contractors but by them in relation to their subcontracting supply chain, which is absolutely critical.

Q60 **Baroness Lane-Fox of Soho:** I need to start by restating my interest: I am a director of Twitter. Pretty much everybody has congratulated the work of the NCSC, but I think it would be fair to say that people have also said there were tensions at the beginning between industry and the role of government and where those boundaries lay. Building on some earlier questions, I am also interested in your strategic versus operational focus. Who in government is setting the strategy and how do you have impact on the strategy? Which is the more operational bit of the chain?

David Lidington MP: In terms of strategy, the National Cyber Security Centre operates to a remit that has been set by the National Security Council chaired by the PM. So that is a collective Cabinet-level decision to

say, "This is what we want the National Cyber Security Centre to be doing". It is probably better for Ciaran to explain the remit.

Baroness Lane-Fox of Soho: But how would the NCSC have input into the policy that would impact the strategy?

Ciaran Martin: Through the National Security Council deliberations. That is how the strategy came about. Although it was published in November 2016, its parameters were largely set a year earlier, both the organisation of the NCSC but also the strategic posture of the Government, in the 2015 national security strategy. In a sense, the 2016 strategy is just a longer version of the subset of that.

We put our position papers, ideas and analyses of cyber threats to the National Security Council. To give you a specific example, the Active Cyber Defence programme that we place so much store on was something that we asked specifically to be included in considerations for funding and strategic prioritisation. With regard to the balance between strategy and operations, the Government have given us a clear message that they care about cybersecurity for two reasons: one is national security and the other is economic prosperity and the well-being of the citizen.

Working towards meeting those two objectives involves quite different things. The first is quite an operational aspect. It uses the best of GCHQ's intelligence capabilities: our incident management procedures, and so forth. The second is much more about behavioural change, as the Minister said earlier, and using technological innovation to scale up defences. Ultimately I would like to get the second bucket of priorities—economic prosperity and the well-being of the citizen—on a much more self-sustaining basis, with organisations doing more for themselves, with us pitching in with targeted, innovative interventions, doing what only the Government can do, leaving the experts to do the high-quality operations against the very best. That is the journey we are on and that is the strategy that has been set.

Baroness Lane-Fox of Soho: So we are waiting with bated breath for the new version of the national cyber security strategy. When will that be published?

Ciaran Martin: The current one runs to 2021. As I said earlier, I think in response to Lord Hamilton, I very much welcome the strategic stability that we have at the moment in terms of the funding figures for the centre that I read out, and the goals. We have a clear set of priorities and we are working to them. This is year two, going into year three, of the programme.

Baroness Lane-Fox of Soho: Sorry, it is the national cybersecurity skills strategy that we are still waiting for.

Ciaran Martin: Oh, the skills strategy. I do not know precisely when that is going to be published. This is the first time that I have had to say this

today, but the organisational lead for cyber skills is with the Department for Digital, Culture, Media and Sport. We support it through our CyberFirst programmes and so on. I am very happy to try to update you on that as and when I can.

David Lidington MP: We can check with DCMS and perhaps write to the Committee on that. The original remit of the National Cyber Security Centre was looked at again more recently when the Government had a national security capability review. Our conclusion was that the overarching strategic objectives still stand. We took a look at it and thought the 2016 strategy was still valid so we continue working to that.

Baroness Lane-Fox of Soho: I apologise if I was unclear. It would be good to understand the detail of the national cybersecurity skills strategy. I will come back to that in a minute, if you will bear with me. It is interesting hearing from the CNI operators where the responsibility might lie between you and them. Do you perceive conflicts of interest with those operators? Are there moments when they are arguing for protection of data that you might feel you need access to, or any other areas where there are vulnerabilities or tensions?

Ciaran Martin: On the whole, the relationships are pretty positive. For example, when we tell a critically important company about a sensitive intrusion, of course that is a difficult scenario for it and it can take time to reach a shared understanding of what has happened. But we do not routinely end up in tense situations where there is some sort of fight about what we can disclose or what remedial action needs to be taken. As I think I said in answer to Lord Campbell, the voluntary and co-operative arrangements tend to work quite well and our help tends to be not just accepted but welcomed. When the case arises within the company itself rather than, say, us telling it that we have noticed something, our help tends to be sought.

Baroness Lane-Fox of Soho: With health data, for example, which is arguably where people get the most anxious—understandably—do you perceive that there might be a difference of opinion about how critical health infrastructure or other players might need to work with you?

Ciaran Martin: I do not necessarily see why that should be the case.

Baroness Lane-Fox of Soho: You have never had an issue with a tense piece of negotiation with the CNI health operator?

Ciaran Martin: I imagine you are referring to a specific incident, which I am happy to—

Baroness Lane-Fox of Soho: No, I am just interested. Health feels as though it is one of the areas which causes most public concern on one level about the nature and protection of a data and vulnerabilities to it, and I just wondered whether there had ever been tension around that.

Ciaran Martin: Since NHS Digital was established, given the fragmentation, we learned a lot from the protection of health service

interests from WannaCry. Of course, that was not about sensitive patient data by and large, but, as you will know, the NHS is a huge organisation with thousands of small parts, and that was one of the strategic issues. The establishment of NHS Digital some years ago—long before the WannaCry attack—has given us an organisation with which we can partner. There are no tense discussions with it; there is a real commonality of interest about the protection of the infrastructure of the health service and patient data. Because of the way it is for the lead authorities in government—in this case, the Department of Health and the NHS—to supervise the sector as a whole, drawing on our advice as and when necessary, we would not routinely talk with some of the private health or data companies or have the sorts of conversations that you envisage, and we share the NHS's commitment to confidentiality of patient data.

David Lidington MP: I think Baroness Lane-Fox is right to say that people worry about a risk of disclosure of very intimate information about their health condition and treatment. But at the same time, my own experience as a Member of Parliament is that people like the fact that doctors and clinics contact them by text and email. The younger the patient, the more ready they are to accept those means of digital communication. It is really a matter for the Department of Health and the NHS, but we probably need to do more to get the argument over to people that the use of anonymised big data can make it more likely that we can establish the effectiveness or otherwise of different treatments and improve the quality of the health service that is offered.

Baroness Lane-Fox of Soho: I would agree. It sounds as though you would characterise your relationship with the CNI operators in particular as extremely effective. Can you point to anything that might make it more effective?

Ciaran Martin: There is plenty. On the characterisation of the relationship, it is not hostile but there are lots of things we need to aspire to. I gave the finance model earlier. Elements of that, such as getting the same balance of effectiveness between us, the lead government department, any regulatory authority and the sector as a whole can be quite tricky, given the wider complexities of any sector and, where relevant, the fast-changing pace of technology. We need to do more work to understand where the state's interests as the protector of the public versus a critically important company's commercial interests align, as they mostly do—but occasionally they will not. We have done some very useful pilots with companies, where we have taken the top 50 risks we have seen, and for the most part 90% of them will be the same. We will worry about this, but they will have a commercial imperative with regard to a particular service that from a strategic national security point of view we will not care about. So how do we deal with that sort of situation?

The great disappointment of global or certainly western cybersecurity over the last 10 years has been information sharing. People keep saying that it is the solution to each sector, but again, outside finance, it has

largely underperformed. We need to work out why that is and either fix it or get out of that. So there is a whole series of improvements we could make.

To link to the previous questions you asked, Baroness Lane-Fox, we are not in need of a culture change in terms of hostile attitudes. That is not my everyday experience or that of my team.

Baroness Lane-Fox of Soho: To be clear, that was not what was pointed to, but it felt as though there could be some interesting boundaries and bits which need to improve.

Ciaran Martin: I accept that.

Q61 **Baroness Lane-Fox of Soho:** Moving on to the technical expertise you have, a lot falls on your shoulders, quite apart from when you start to see it through the lens of the deep experience of, say, aviation technology or deep health technology. How do you manage to keep up with those deep technical expertises, and do you have enough resources to be able to do that effectively across all the sectors you need to?

Ciaran Martin: It is a constant and difficult challenge. As I think you said earlier, there is the very top end of the skills spectrum and then the mass market of basic skills, and we need to do our best on both. At the top end, successive Ministers have very helpfully sponsored a specialist pay framework for the best technical experts. It does not compete with Silicon Valley salaries, but it is certainly enough to motivate and incentivise people who like the mission of national security to stay, and it gives them a career and a skills framework to aspire to. There are four levels of skills, level 4 being the highest. We have over 20 level 4s, which is a very demanding standard. We are talking world-class sought expertise, and that has to be updated on a two or three-yearly basis.

Baroness Lane-Fox of Soho: Forgive my ignorance, but if someone had very specific bespoke legacy system or, say, aviation expertise, would that fall into that category?

Ciaran Martin: It could do. Another initiative we have done—the Chancellor announced the launch in February 2017—is a formal programme of secondments from industry, which industry pays for, called Industry 100. The aim of that is to get people who have the deep sectoral expertise we want. The last thing we want is a bunch of people going out saying that they have deep technical knowledge of an energy or aviation company, only to be told that what they have just said is wholly impractical in that business. We now have 80 people, not all of them full-time, going towards the Industry 100 target, who are drawn from across all manner of different industries.

Baroness Lane-Fox of Soho: And that is out of the total staff of how many?

Ciaran Martin: Excluding Industry 100, because they are not counted as paid-for staff, we are on 740 or so.

Baroness Lane-Fox of Soho: So would you say that about 10% of staff have that industry-specific, deep technical expertise?

Ciaran Martin: Yes, but in a sense, out of the 740, there are broadly speaking three chunks of 250, so to speak. The first lot is deeply operational—the core GCHQ, often with signals intelligence experience but using that for cybersecurity. Relatively few of them are at level 4; quite a lot of them are at levels 1, 2 and 3. In the second bunch, most of them will work around understanding technology and how to protect it, with research and analysis and so on. The third bracket are the outward-facing advisers, communications specialists and so on. So there is a range of deep technical expertise all the way through, combined with some sectoral knowledge. We have a couple of dozen public communications specialists, who understand how to do campaigns which will influence human behaviour, but it just happens to be about cybersecurity.

Baroness Lane-Fox of Soho: Is it hard to recruit?

Ciaran Martin: Recruiting deep technical expertise is challenging. It is not at crisis levels for us as an organisation. We are taking steps to try to foster the elite pipeline through interventions at schools and universities. As of this coming academic year, we will be sponsoring 500 people, paying £4,000 of their tuition fees, who are undertaking to work on cybersecurity either for us or for related organisations, including in the private sector CNI, for example, as part of the conditions of that. Those tend to be oversubscribed at that sort of training level. But when it comes to getting, for example, a deep specialist in 5G architecture as we look to formulate a strategy by the end of this year, that sort of existing expertise can be hard to come by.

Baroness Lane-Fox of Soho: Yes, I will give you that. That is a bit of a crisis in the broader economy, too. I am interested—from you too, Minister—in whether you map the broader cybersecurity skills gaps across the economy, not just within the NSC—apologies, the NCSC; I got it wrong again. I am interested in how you benchmark it and see what actions might need to be taken to address it.

David Lidington MP: Baroness Lane-Fox is right: this is a challenge right across the economy. We are trying both to take action on the pipeline—schools, colleges, universities and apprenticeships—and to upskill the existing government workforce. Although longer-term solutions have to be found in terms of increasing the supply, clearly there is not an overnight solution. We are taking action in schools and colleges, such as reform of the computer science GCSE and A-level. T-levels, as they start to come in, will cover cybersecurity and digital skills. The National College for Digital Skills will train up to 5,000 students over the next five years for a variety of digital careers, not just cybersecurity. The Institute of Coding is bringing together more than 60 universities, business and industry experts to help graduates to build the right level of skills. The NCSC is helping to promote apprenticeships in cybersecurity with GCHQ and the private sector CNI providers.

In government, we established a designated government security profession—in the same way that we have a government legal service, commercial service and financial cadre—so that we can plan for and promote the career development of people who are specialists in security aspects, particularly cybersecurity. The Government's cyber apprenticeships scheme will play into that work of developing the profession. Looking at key departments, the Defence Cyber School will deliver cyber training across the MoD and wider government. In local government, MHCLG has developed a mentoring initiative that has so far trained more than 2,000 senior local public sector staff in core cybersecurity programmes.

I will be the first to acknowledge that there is more that could be done, but a lot of work is going on. The effort is to try to drive up the quality of cybersecurity professionals that we already have and enhance the pipeline for the future.

Baroness Lane-Fox of Soho: Two questions come out of that for me. First, have you looked specifically at the CNI operators, the regulators and the supply chains from the view of their skills and the gaps in either their recruitment or their internal skills? Secondly, how are you measuring the success of all those initiatives?

Ciaran Martin: On the first, we have worked with, on request, some of the regulators to improve their cybersecurity skills. We have given them referrals of individuals, sat on panels to help them with skills strategies and so on. We have seconded people to them to lead government departments.

On the effectiveness of the cross-government measures as a whole, quite a lot of them are relatively recent, so the data is not quite there yet. We are building this up. Unfortunately, I cannot say it off the tip of my tongue. If it would help, I can give the Committee a memorandum on some of the early indicators of our CyberFirst programmes, such as the conversion rates from some of the competitions, apprenticeship schemes and summer schools that we run, and so forth. Thus far, the rates have been quite high. We would have to consult other departments on the data on the other schemes that the Minister mentioned outside the NCSC.

David Lidington MP: Another point, which I think is of interest, is that the National Crime Agency has been working on a scheme of intervention to try to identify young people who might be tempted into cybercrime, and instead divert them by encouraging them to use those skills in a career in cybersecurity instead.

Q62 **Baroness Lane-Fox of Soho:** I appreciate the focus on education, but education is one very long funnel. It takes a long time. There are 600,000 empty jobs in the tech sector right now; there will be a million by 2020. A large percentage of those will be dedicated to cybersecurity, so this requires urgent intervention, to my mind.

I have a final question and then I promise I will be quiet. Information

sharing was mentioned earlier. Do you information share about how some of these interventions in skills have been internationally successful? Do you feel as though you understand the best practice around the world and where we sit in terms of our cyber skills and resilience?

Ciaran Martin: With some of the international comparators, I think we hold up rather well. I do not know of a definitive index of the skills picture. We have a global network of voluntary allies that we talk to about skills. Everyone in the sector like yourself, Baroness Lane-Fox, will know of the Israeli ecosystem of venture capital. Of course, a lot of that is based on military service and so forth, so some bits are not replicable, but we talk to them. In fact, some of the incentives, without the compulsory element of the Israeli system, that exist in the CyberFirst scheme were borrowed from them.

So we try to take the best ideas. However, I cannot say—perhaps you might help us out—I cannot find an international model that has completely cracked the problem, which is why the global figure for the vacancies that you mentioned in the UK is as high as it is.

Baroness Lane-Fox of Soho: It feels as though a couple of countries, Russia and China, have sorted another problem, but that is a separate conversation.

Ciaran Martin: That is a separate conversation, yes.

Q63 **Lord Hamilton of Epsom:** My question is about the interdependence of one CNI with another. The obvious point concerns power supplies, which of course have an enormous impact on other areas. Have you given a lot of thought to how this all works and how you stop power supplies killing a lot of people in hospitals if they suddenly get shut off?

Ciaran Martin: We have. We were talking about regulation; one model that is popular in some continental European countries specifies companies and say that a particularly onerous regulatory framework must apply to them. We have not gone down that road, precisely because of interdependencies—there are things in supply chains and so forth that would make that impossible to do.

Our strategic approach is about understanding impact. The structural problem we have is legacy systems. The great strategic opportunity in critical infrastructure protection over the next decade or so will come as you move from legacy systems that are perhaps 10, 20 or sometimes 30 years old to a new generation of systems. You build in that resilience. We have published detail on this for Smart meters, which we can certainly give to you because it is already in the public domain.

Smart meters are a classic early example of that, where we develop a doctrine that asks, "Are these things impervious to cyberattack?". No, of course they are not, because that is impossible. But what would you need to do to do national-level damage? You would need to do what we would classify as three state-level simultaneous high-grade cyberattacks—in other words, an act of such hostility that it would have wider

ramifications. What you will not find with smart meters is a single off button that will take out the entire network, precisely by design. That gives you a sense of the sort of model and the approach that we are trying to take to other sectors. However, it is only viable to build in those protections as the new generation of systems come in.

David Lidington MP: BEIS has the lead on this. It is working with Ofgem and industry to ensure recovery plans in case of a major power outage. It has to be said that, last year, the national electricity transmission system did prove itself highly resilient. It had a 99.9999% level of reliability of supply during 2016-17. Having said that, threats are real and we cannot be complacent about this. BEIS is working with the industry and the regulator to ensure that recovery plans are good and tested. It has been talking to local responders to make possible some exercises so that we can understand better the likely implications of a power disruption over a wide area. There is also a cross-government work programme looking at what a major power outage would mean in terms of its impact on other sectors. That will report back to BEIS, the National Security Secretariat and ultimately to the NSC sub-committee that I chair.

Lord Hamilton of Epsom: Do many hospitals have stand-by generators?

David Lidington MP: I will write to the Committee on that, but my recollection is that a very large number of hospitals do have emergency generators.

The Chair: Have they been tested and do they work? Having them is one thing.

David Lidington MP: They are certainly supposed to test them and ensure that they work. We would expect that to be a natural part of emergency planning on the part of the NHS and local trusts.

Ciaran Martin: I want to stress that it is a natural part of emergency planning across a range of things. This should be happening anyway, regardless of cyberattack threats. Part of our guidance on crisis management in cybersecurity is where the nature of the attack is irrelevant. If there is a failure of supply, the normal contingencies of an organisation subject to a power failure for whatever reason need to kick in.

The Chair: You have been very gracious with your time. We would like to go into private session so that we can ask you one or two things that you might not want to say at quite such length in public. I ask the rest of the audience to leave.