Joint Committee on the National Security Strategy

Oral evidence: One-off session with former chief executive of the National Cyber Security Centre

Monday 18 January 2021

4 pm

Watch the meeting

Members present: Margaret Beckett MP (The Chair); Lord Brennan; Lord Campbell of Pittenweem; Richard Graham MP; Lord Harris of Haringey; Baroness Healy of Primrose Hill; Baroness Henig; Baroness Hodgson of Abinger; Darren Jones MP; Lord King of Bridgwater; Baroness Lane-Fox of Soho; Sir Edward Leigh MP; Angus Brendan MacNeil MP; Baroness Neville-Jones; Lord Powell of Bayswater; Tom Tugendhat MP.

Evidence Session No. 1 Virtual Proceeding Questions 1 - 30

Witness

I: Professor Ciaran Martin, former chief executive of the National Cyber Security Centre.

Examination of witness

Professor Ciaran Martin.

Q1 **The Chair:** Welcome, Professor Martin. Thank you very much for meeting us today. A lot of us were on the previous committee when we took evidence from you in 2018 in your role as the head of the National Cyber Security Centre. We were looking then at cybersecurity's role in our critical national infrastructure and at initiatives to improve cyber skills. There seems to be even more attention on these issues now with it appearing that attacks are growing in frequency and, indeed, even as part of the issue with the response to Covid-19. Of course, we are coming up to a period when the first five-year cybersecurity strategy will need renewing. There is an ongoing debate about offensive cyber and, into the bargain, the Prime Minister announced at the end of last year the creation of what he is calling a national cyber force.

There is a lot happening in the field. Having left that role, what is your

assessment of what the NCSC has achieved since its creation and what, if anything, might you have hoped it would have done more—where it might have gone further?

Professor Ciaran Martin: In relative terms to other countries, I think it was a good five or six-year period for the UK because of what the NCSC was able to do, mainly because the UK successfully pivoted on to a more activist strategy. A lot of cybersecurity in the first 15 years of this century was very passive. It was very much, "The market will take care of this problem. The Government only need to take care of the high end of the threat". We underestimated some of the structural problems in the way the internet had grown up; not maliciously, it is just the way it happened—prioritise free connectivity over security.

I remember being very struck by an account given by a senior American industrialist, Art Coviello, who founded RSA—a titan of global cybersecurity. He recounted two strategies of President George W Bush and two strategies of President Obama. They had been based on encouraging information sharing and collaboration among the private sector, and encouraging the private sector to collaborate with the Government—both quite passive, exhortatory things, if you like, and they had not really worked.

By gripping incidents and detecting and communicating them clearly, by trying to work out what we cared about most in critical infrastructure, by trying to look at structural defects in the way the internet worked—business was not going to take care of them because there was no commercial incentive to do so—and by trying to make it easier for human beings to use technology more safely rather than shouting at them for getting it wrong all the time, which was a terrible approach to things, we made good progress and the UK continues to make good progress in all of those areas.

What are the regrets, and what should the focus be now? There is a lot of proof of concept—sorry to be a bit jargonistic—there are a lot of things that we have shown can work, but we have not quite scaled them out into true, national-level defence systems. That is really important. The pace of getting off legacy systems, systems that are 10 to 15 years old, is not quite where it needs to be.

I was quite struck by the fact that the incoming Biden Administration across the pond has a hugely ambitious emphasis on and programme for cybersecurity, it seems, and quite a lot of the money is going into getting the federal Government off antiquated systems because there is only so much you can do to protect antiquated systems; you are into mitigation, not transformational security shifts. There is something in that, and there is also further to go on skills, I would have thought.

Relative to other countries, and certainly judged by the interest in the UK model from across the globe, it is a pretty good story, but there are a whole set of things now that need to be scaled up or turbocharged.

Q2 **The Chair:** As I mentioned, we are coming up no doubt to a renewal of the five-year strategy. Are those the kinds of things that you would want to see if you were still in post? Is that what you want to see in the new strategy?

Professor Ciaran Martin: I am still interested in the new strategy, because I think it is important for good government. Generally, when it comes to the prioritisation of cybersecurity, I would say this, wouldn't I, but we have so many other things to worry about that there will be a natural tendency to pay less attention and there will be proportionately less bandwidth. The Government are the same size as they were five years ago, but they are obviously preoccupied with other things, and I make no criticism of the government machine for that.

The business case for cybersecurity within that context, in so far as we had a salvation in 2020, was that technology was it. It kept some businesses going some of the time. It mitigated the economic damage done by the pandemic, and, frankly, for all of us personally, connectivity with people we care about made a horrible year a little bit easier. Maintaining, and if we can enhancing, public trust in technology is really important.

In terms of a future strategy, I do not think that a radical overhaul is needed, except for the three things I mentioned: scaling the impact of these things, particularly through the private sector—we have done a lot of things in government, but they have not quite migrated out to the private sector in the way I might have hoped; skills—I am sure there will be more on skills, but in the interests of time I will just register it; and critical infrastructure protection, which we will probably come on to.

Finally, if there is any new emphasis—this is more complicated than it sounds—we have to be prepared to make some hard choices to make sure that we have more secure technology. We have been through a technological revolution where, frankly, security was an afterthought, and we are suffering from that. There is hard, technocratic work to do to plug some of those gaps, but there are also hard choices to make.

I will give two examples at opposite ends of the scale. One is the age-old debate about encryption. It is a really hard public policy choice, and in a sense the market has spoken. People want that sort of privacy. There are knock-on effects for all sorts of law enforcement and national security mitigation risks, but unless we want to weaken technology as a whole we will have to find ways of living with that.

The other, which I am sure we will come on to, is that we are learning about the fragility of global tech supply chains—about the difference between not being able to trust pieces of equipment and the trustworthiness of supply chains and so on. There are some complicated economic choices, but I think that we will have to commit to a strategic effort, in conjunction with allies, to try to make sure that the next generation of technology is significantly safer than the one it will replace.

Q3 **The Chair:** Yes, that makes a great deal of sense. Going back a moment,

the issue of skills, which you touched on, is something that we have talked about quite a lot in the past. My horrid feeling is that we shall need to continue to do so in the future.

In the report we just published on biosecurity, we tried to use the Covid pandemic as a bit of a test case to look at how the structure of identifying risks and addressing them and so on was working from the national security point of view: in other words, not doing an inquiry into Covid itself but asking how it plays in terms of national security. How well and how frequently do you feel that the National Security Council engaged in the cyber issues while you were at the NCSC?

Professor Ciaran Martin: I have no cause for complaint on that front. Obviously, you would have to ask my successor how things are at the moment, but as with any bureaucratic set of arrangements there are ways in which it can improve. The National Security Council and associated substructures have proved their worth in a variety of areas over the slightly more than a decade that they have been in place, particularly for an issue like cybersecurity because it is so multidimensional. You can lament the proliferation of departments and Ministers involved, but that reflects the reality of the complexity of the subject. There are international issues. There are crisis management and domestic security issues. There are digital policy and skills issues. There are resilience issues.

Access to individual Ministers was never a problem, and we may not always have liked collective decisions across the NCSC, but pretty much without exception there was a serious process of collectively deciding on the issues. In fact, there is always a negative and positive way of describing the same thing, and the lack of single ownership at ministerial level of cyber issues is the negative way of saying that it was a properly collective cross-government discussion.

I often say that, in so far as the UK has been able to make progress in cybersecurity, three things aligned in the last five years that often do not in public policy. One was a clear and unchanged strategy. You mentioned that the five-year strategy is about to come to its end. I spent nearly a quarter of a century in the Civil Service, and I was witness to a lot of five-year strategies in Governments involving three parties that lasted one or two years before they were substantially revised, even by the same Government.

So there was a clear and consistent strategy. There was decent and, most importantly, stable funding. I also think that the UK has had a decent balance of ministerial support and at the right remove. There is always a trade-off between ministerial sponsorship and direction versus operational discretion to get on and use the experts to do the things that experts can do. By and large, that worked well in the UK system.

Of course, I have no reason to say this anymore, so it is a genuine opinion; I am not here to defend it. I do think that that collective approach brought in in 2010 has stood the test of time. It is not perfect, but I have looked at and dealt with, and continue to deal extensively with, cybersecurity

bureaucracies across the world, and I think it is a pretty good framework for decision taking.

The Chair: That is very helpful. Thank you very much.

Q4 **Lord Harris of Haringey:** It is good to see you again, Professor Martin. The NCSC's recently published annual review, which I assume you had quite a hand in, provides a lot of information on activities that were undertaken but gives us less information on outcomes. Are there metrics that could be used and reported on to demonstrate the success or otherwise of the centre?

Professor Ciaran Martin: That is a fair cop. The only bit that I have to correct slightly is that the report came out on 3 November. I left on 31 August, and while I was responsible for—

Lord Harris of Haringey: I cannot believe there was not at least one draft knocking about before 31 August.

Professor Ciaran Martin: I cannot remember. Anyway, that is the period in question, but obviously it is for the Government to defend that record.

The point on metrics is a good one. It is a paradox of cybersecurity. Again, to Margaret Beckett's initial question as to whether there are things that it would have been better to have made more progress on in the last five years, I would say that metrics is one of them. The paradox of cybersecurity is that, for such a data-driven technical subject, there are remarkably few metrics. There are a variety of indices by the International Telecommunication Union which the UK is top of, but in one by Harvard's Balfer Center the UK fares badly in cybersecurity by comparison. They tend to be very much about the quality of strategies, the amount of money, not the outcomes that you mention.

There was an attempt—it is nearly a decade old—to quantify the cost of cybercrime to the UK. It was before my time, but it was heavily criticised and, frankly, put people off attempting it again.

The way I would characterise it, looking at the last decade or so of UK cybersecurity strategy, is that we went from pure input—"We will spend this amount"—to starting to get a bit of output. Some of the published numbers from the UK are on things like the volume of takedowns, the share of UK maliciously hosted websites and so forth, which you can measure progress by against other countries. They are outputs, but outcomes are very hard to measure.

Let me give you a specific, if quite nerdy, example, with apologies. When it was initially introduced, the UK Government's automatic takedown service, which a lot of other Governments are copying—I am probably slightly out of date with these figures—brought a dramatic reduction in what you might call the time to die that a malicious website was up. A malicious website was up on average for more than a day before it got taken down. Some of the work of the NCSC, wider government and private sector partners brought that average down to 45 minutes, which is a striking success, and it will have reduced some harm. However, the

problem, when you look in more detail, is that quite a lot of harm happens in the first hour—not all of it, so it was still worth doing, but it is not make for as dramatic a reduction in harm as you might think. That is the sort of thing.

Depending on capacity, it may be something—do not worry, I am not pitching—for think tanks and collaboration with others and so forth. You want to do this internationally, because it would be good to get some benchmarks. If an opportunity came along with partner Governments to fund some genuine objective research that people could work at to do some proper metrics, it would be worth doing. It is a fair criticism of the current state of affairs that it is very hard to look at the actual metrics of outcomes.

Lord Harris of Haringey: I want to pick you up on something that you said a few minutes ago in answer to Margaret Beckett. You said that, in the technological revolution that we all went through, security had been an afterthought. Are you able to point to things that the centre has successfully done to ensure that software standards do build and do require that security be built in, or is it one of those issues where, whenever the centre tries to raise it, it is told, "No, you'll stifle innovation. Let's keep out of that"?

Professor Ciaran Martin: I think there is a difference between legacy and newer IT. With legacy there is obviously not much you can do, because you cannot retrofit it. On newer stuff—I am afraid I have lost track of where this has got to—the internet of things, devices and that whole newish bit of the IT ecosystem are a good example of fresh thinking in the UK and elsewhere that can be built on.

I mentioned that technology was an afterthought. This is a wild, and therefore incorrect, generalisation, but bear with me. In the mid to late 1990s, the noughties and so forth, the economic model was, "Give us personal data in return for free access to web-based services", essentially; it was a large part of the early technological economy. IoT is different. As the T implies, it is often something you can hold or at least see, so there is a hardware dimension to it. It is more often than not something that you pay for; you buy both a product and an ongoing service.

Because of that, particularly the physical aspect of it, there are, in effect, trading standards that you can impose. The UK Government have done some quite useful things, DCMS-led and NCSC-supported. Two or three years ago, the UK was out in the lead with a code of practice for IoT sales, where you could start to make judgments about products: "This will be updateable automatically until 2025. This won't, so it might cost more but it is safer", and things like that that you could not do. The UK and Singapore signed a research and development agreement on this in October 2019. Singapore has now gone on to put that into law. The UK Government, I understand, are planning to put that into law. I would recommend that sort of thing.

That IoT thing is a good example of looking at emerging technology—or emerged, in this case—deciding that you will fix structural problems with it

in a regulatory model or a business incentive model and so forth, and doing it. It is slow and painstaking work, but there is some evidence that we are trying to get ahead of the problem in the UK. That is the sort of approach that we now need to move on from. Whatever new technology we are talking about—5G or AI or even, long term, quantum—we need to be looking at building the security model into the way we manage these technologies and their introduction into society.

Q5 **Lord Harris of Haringey:** Okay, but clearly we take it as a given that, whether it is trying to influence future standards or not, the centre gives high-quality advice to parts of government and parts of the infrastructure, or even to the private sector, on technical matters to do with current cyber threats. How do you actually make sure that the advice you give is properly tested and properly audited? What challenge function is built into the process?

Professor Ciaran Martin: Again, the posture now is something that the Government will have to account for, but basically it is what they call white papers; this is a technical term that does not quite mean the same as it means in policy departments. You publish your thinking on everything from new and emerging technologies. It is very technical stuff, and expert communities look at it and feed back and challenge. You can imagine how this works; there are ferocious arguments about that within highly technical communities that are incomprehensible to most people.

Essentially, in one word, it is transparency, and I think the UK benefits from this. The National Cyber Security Centre, in technical terms at least, is a very transparent organisation by the standards of the globe. It puts it out there and says, "If you don't agree with this, can you please tell us?"

There are many examples of modifications, so that is where it comes from. As I understand it—I do not know if they are still in existence—there are technical advisory panels and all the rest of it, and formal peer reviews. When I was in charge of the NCSC, one of the things we had was the incident management model. An incident might be a slow burner, or it might be really quick, and you need to say to the public, "Do this, don't do that. Worry about this, don't worry about that". We had to establish a 24/7 technical review panel. It was internal, but it meant that somebody would technically assure it and sign it up, and then it would be out there for challenge and all the rest of it.

There were processes, and I am sure that, as with any process, you can challenge them, but technical assurance was built internally into everything in the National Cyber Security Centre, and where possible, which was most if not nearly all of the time, the technical detail was published for criticism and scrutiny in an open-source way.

Q6 **Baroness Healy of Primrose Hill:** Professor Martin, I would like to return to the pandemic, if I may. What particular challenge has Covid-19 thrown up in terms of cybersecurity? How well do you think the NCSC and others have dealt with those challenges?

Professor Ciaran Martin: The pandemic has challenged the technology sector in one way, and the cybersecurity subset of that in probably three ways. One way in which it challenged the technology sector as a whole was capacity; there was this huge increase in demand, for obvious reasons. I think the evidence is there that, while it was not perfect, it was not all despair.

It is unfashionable to praise, for example, the British communication service providers, but they did pretty well last year. When engineers from BT and Vodafone were given awards in the birthday honours list, I remember thinking, "That's fair enough". They climbed up poles in the middle of the night to keep villages and towns connected so that they could go the next day. For the most part, technology stood up to the challenge, and thankfully it did. So it is not all despair.

In cybersecurity, there are probably three issues. Two are consumer facing, and one is statecraft. Of the two that are citizen and corporate facing, the first is the large-scale move to remote working. I think the UK model is largely correct in saying, "Treat cybersecurity as an ordinary business risk". One thing that most ordinary business risk manuals will tell you not to do is have a massive unplanned change in your operating model overnight, but that is what pretty much everybody has had to do: go from 5% home working to 100% home working, or whatever it was.

Organisations did that reasonably responsibly. The Government did a decent job in providing guidance and help in managing that transition. Again, mindful of Lord Harris's point about the absence of metrics, there are none, really. At the same time, if there had been a series of security disasters as a result of the sudden move to home working, there would be something in your briefing papers to say, "Ask him about that". By and large, that migration went reasonably well, although it went reasonably well across the world. So that is one thing.

Secondly, when we talk about cybersecurity we really underestimate the scale, venality and moral turpitude of international cybercrime. We often talk about the big states and all the rest of it, but in terms of harm and how putrid it all is, international cybercrime is pretty disgusting. Within days, people were getting large-scale scams about fake PPE, fake tests, fake cures, fake government schemes and so on. Again, the UK did well on that by international standards. There are output metrics about hundreds of thousands of takedowns of this, that and the other. The world's first suspicious email reporting system came in and very quickly got a million hits, with then over 10,000 takedowns of these scams. No other country in the world is doing that in that national way, so that is all good.

It showed across the world that one of the biggest threats to the healthcare sector is the scourge of ransomware, where criminals are locking systems and demanding data, and in my judgment the UK is probably lucky rather than immune from this. There was a tragic case in Düsseldorf, Germany, where a patient was being taken to hospital but had to be diverted to a hospital further away, because the hospital to which she was due to be admitted could not receive her as its systems were ransomwared. She died

on the way to a different hospital. There are things like that which just show the scale of that problem. Again, as I understand it—I cannot speak to it anymore—this has continued. The UK has put more active protections across the NHS digital estate than most countries have been able to do in equivalent things, so there is some good work there.

So there is the move to home working, the scale and horrible nature of criminality, and—this is an important point—the national-level risk of cyber criminality to critical infrastructure and how it changes. For years, the whole debate has been about whether a schedule should be drawn up of critical networks, critical companies and so forth. A lot of people in the UK, including me, have always argued against that on the grounds that bureaucracies are not very good at drawing up definitive lists, and even if you get it right the first time, which you probably will not, it will change. Covid is the vindication of that. Five years ago, critical protections meant energy plants, banks and so forth, and that is still the case. After the events of 2016, people who did elections, media and political discourse joined that list—quite rightly, too, because the revealed preference of some attackers was to destabilise politics. In 2020, initially in the pandemic, food distribution logistics became very important for a while, and then, of course, small but incredibly important research institutions specialising in vaccine research became really important and became the target.

The lesson from that—again, the UK has a decent story to tell on this, I believe—is flexible and adaptable adjustment to protect what you care about most, because what you protect and care about most will change, and in 2020 it changed rapidly. In the normal course of human events, it will change over time anyway and you need to be able to adjust to it.

Q7 **Baroness Healy of Primrose Hill:** On that point, one of the criticisms that has been made in our recent biosecurity report was that the Government had not done enough pandemic response exercises. They had undertaken exercises, but they were for a flu pandemic rather than for a Covid-type disease. Do you think that we were perhaps not flexible enough in our planning?

Professor Ciaran Martin: I do not know. It is really hard. I know nothing about virology, I am afraid, so I am not in a position to say whether it was an appropriate or inappropriate judgment to exercise flu pandemic but not respiratory diseases. In fact, I may even have got that bit wrong.

In cybersecurity, I am sympathetic to people juggling that sort of issue, because every time we did a major exercise, the next major crisis bore no resemblance to it. It was just that thing. You only need to look at the sorts of things that were being talked about in 2015 or even 2016, such as the statement by Philip Hammond when he launched the national cybersecurity strategy on 1 December 2016. He started talking about attacks on power plants and so forth, and I have no criticism of that at all. That was very much at the forefront of people's minds. The Russians had taken out the lights in Kiev the year before, and so on. The first major crisis following that strategy was six months later, and it was a North Korean rogue ransomware attack gone wrong. Its problem was that it was so badly

configured that it spread like wildfire throughout systems all over the world. It bore no resemblance to the sort of thing we were thinking about and it was quite hard to anticipate.

Of course exercising is important. Here is an example of something that came out of UK exercising in cyber which is really good. If a major cyberattack is state-backed, it is very much intelligence led, COBRA led and so forth. If it is criminal but in the west, law enforcement can be the appropriate lead. As a result of exercising, the UK systems, as far as I understand them, are very flexible in handing over the principal role of co-ordination between intelligence and law enforcement, and that is a really good thing. It is sometimes better to focus on who, in practice, is doing what and what your procedures are and how adaptable are they, rather than trying to guess what the next crisis will be. Certainly, I would not like you to ask me, "What do you think the next cyber crisis will be?". If you did, I would say, "It could be a ransomware attack on a hospital" but then I would probably get it wrong, because history says that I will probably get it wrong. That is probably the best we can do on exercising.

Q8 **Baroness Neville-Jones:** My couple of questions rather follow on from what you have just been saying. In the annual report of 2020, you described a knowledge base that would allow the Government to manage critical national infrastructure assets and—[*Inaudible.*]

Do you think that is a model that could and should be used in other areas, now that we have had experience of trying to protect pharma or academic research or other sectors? Can we accumulate a similar body of wisdom and knowledge? Can it be done preventively, or is this only something that you can do with the fruits of experience?

Professor Ciaran Martin: It is a really difficult question. In terms of incentivising what you might call classic critical infrastructure, there is something about regulatory models. Personally, as a matter of opinion, I like the way the financial services model has evolved. It has been copied in telecoms, which is that you do not put cyber in a box that says, "This is cybersecurity". You bake it into the regulatory framework—in the case of finance, the Bank of England's role in stress testing of banks. If the telecoms security Bill passes Parliament, it is part of Ofcom's wider role in making sure that we have a thriving telecoms industry. The virtue of that is that the likes of the NCSC can give the expert technical advice about what needs to be done, but the NCSC, unless it has changed dramatically in four months, and in this respect I doubt it, would never and should never have the expertise to try to devise a viable regulatory and profitable economic model for finance and telecoms. I would like to see that model extended into other critical sectors.

In terms of preventive stuff, you might be able to use it as a model for pharma because of the size of the companies, but when you are talking about smaller academic institutions and so forth, it is hard to extend that big regulated business model into them. For things like food distribution it is harder, so what do you do about that? First, the state should have a big protective intelligence sort of shield—here, the NCSC benefits from being

part of GCHQ—that can quite savvily detect threats. If there is a shift from hostile states targeting energy to hostile states targeting academia, you can switch those—

Baroness Neville-Jones: It provides an umbrella.

Professor Ciaran Martin: It provides an umbrella. You can also look at guidance or regulation through things like the Charity Commission. Charities, Universities UK and all of that look at guidelines for best practice. They will not be as good as big energy companies because they do not have the same money and so forth, but you can at least look at incrementally strengthening the basics in a preventive way.

Baroness Neville-Jones: It sounds as though it is partly irrelevant as a technique and has to be adapted to the circumstances of the sector.

Professor Ciaran Martin: Thank you. That is a better answer.

Baroness Neville-Jones: You have talked about the saviour that technology has been in the pandemic. Where do you think we now stand in terms of security? Do you think that we are much more exposed at the moment, or do you think that it has increased the level of cyber awareness in society as a whole, or is it a combination of the two?

Professor Ciaran Martin: Broadly, the pandemic has not strategically shifted the balance that much. Anyway, we are on the cusp of shifting to a bunch of newer technologies. I talked earlier about getting security baked into those, and I think that is the answer. The pandemic has just made it more of an imperative.

Q9 **Baroness Neville-Jones:** You have not talked about quantum and it is not really on our list, but when do you see that becoming a big issue? What is the timescale? I know there is argument about that.

Professor Ciaran Martin: There is argument about that, but I hesitate to put my tuppence worth in, even though you tempt me. I am just quoting genuine experts or people who are taking decisions based on this, the science is there. It has been there for some time. It is all about getting the engineering and the marketability of it right. If you look at the publicly available stuff from government, principally the NCSC, and talk to the venture capital industry—I do some work there—depending on their timeframe, people are looking at a decade at the earliest before there is widespread use in a noticeable way, where it becomes part of everyday commerce.

Baroness Neville-Jones: You think at the earliest. That is reassuring.

Professor Ciaran Martin: That is if you get the likes of Sir Peter Knight and others, who are the genuine experts. I claim no specific expertise in quantum technology and that space.

Q10 **Baroness Lane-Fox of Soho:** Thank you, Professor Martin. You kindly gave evidence to our committee in 2018, and one of the results of that inquiry was that many in the private sector said that they wished they had had more specific guidance from the NCSC. That interrelationship between

the organisation and the private sector is clearly fluid and complicated. I am interested in your views on that and whether you think they understand the role that the NCSC can provide for them.

Professor Ciaran Martin: There is a question, I suppose, of scale and potentially function.

On the question of scale, the NCSC has about 1,000 people. A lot of it certainly was and is the operational umbrella that I just spoke about. A lot is the specific technical expertise and how the Government reach a view on the security implications of quantum and when they will become apparent. There is lots of excellent work going on on that.

The advisory expert function on business will never be huge, and, looking at this in the abstract, there is the question of the extent to which you want it to be huge as opposed to a purveyor of good practice and good advice so that people can make judgments for themselves. It very much links to the point I made to Baroness Neville-Jones. It is not easy to have in-house expertise in government that says, "This is what you should do technologically", but I think the UK has managed to do it reasonably well. It is neither particularly possible nor particularly desirable to say, "Therefore, this bank should do that". There are decisions for regulators to take on balance. Cybersecurity is not an unassailable priority. It is something to be balanced with other things—with commercial profitability, with other risks and so forth. There are things to reflect on there.

Lest that sound too defensive, I do think, for example, that there are things that can be done better. Again, it is a bit like the scaling function, which I mentioned to the Chair at the start. When you look at things like telecoms security and the relationship between the Government and the telecoms sector, most countries are very envious of the closeness of that relationship. By that I do not mean cosy; I just mean the rapidity and depth of exchanges of views and information between the Government and the telecoms sector, which is obviously hugely important in development.

You talk to the Americans and they say, "There is this big thing in internet security", and you say, "We can get the telcos together tomorrow and they will all come". They would all come physically before the pandemic. The Americans will tell you, "We can't afford to do that" and so forth. One of the reasons for the telecoms security Bill coming in is that UK telcos said to the Government quite publicly in a very open and constructive dialogue, "We're reaching the limits of what we can be expected to do voluntarily. You need to put this into the regulatory framework". That is good.

It does not exist in other sectors, and maybe it should. Maybe there is a scaling function there. There are things that you can do a bit more, but I would be cautious about going to a the national IT helpdesk type of function, if you like. That is putting it pejoratively, which I do not really mean to do.

Q11 **Baroness Lane-Fox of Soho:** I was struck by your answers to Lord Harris's question about outcomes and how you would measure them. Do

you think that you could ever measure outcomes within the private sector as a result of NCSC work, or would that be inappropriate? Is that dangerously near the IT helpdesk?

Professor Ciaran Martin: No. That is why I said that it would be worth putting some serious effort into this. So much of government success and failure is about quite boring things such as capacity and all the rest of it. I do not think that Governments across the world have quite figured out how to measure the private sector. Take the annual taxpayer-funded DCMS breaches survey, for example, where they survey a representative cross-sample. I may be wrong about this, and forgive me if I am, but I think that it meets the standards of official national statistics, so it is methodologically sound in terms of those standards. It says, "Do you think you have experienced a breach? If so, what was the monetary value of that?" That is worth doing.

The challenge over the last decade or so, and I think this is appreciated in the methodology, is that it has been impossible to tell how much of that is growing awareness of being breached and how much is because this year was worse than last year, or better than last year, for cybersecurity. That does not mean that we should stop the survey. It means that we should try to improve the methodology, and ideally do it over time. That is a perfectly laudable public policy objective and should be pursued. In my tenure in office, I do not think that I did enough to move it along, I completely accept that, and it is a very worthy thing to be getting after. Metrics are important. Taxpayers are entitled to know, for a start.

Baroness Lane-Fox of Soho: I have one last quick question. The pandemic, as you were describing to Baroness Neville-Jones, has changed a great deal. Do you think it should change which organisations are classified as critical national infrastructure in relation to cybersecurity; pharmaceuticals, for instance, or others you may have ideas about?

Professor Ciaran Martin: It is the same answer, really, as I gave to Baroness Neville-Jones. We should be able to flip just like that what we think of as critical national infrastructure. We really should.

Q12 **Lord King of Bridgwater:** You talked about the private sector coming for help and leading against the problems of cyberattack. You have talked about all the telephone companies, as I understand it, but are there some that do not want to be involved with you and think that it might compromise their work or somehow affect their own security?

Professor Ciaran Martin: Again, I am not in government now. The UK has set up the National Cyber Security Centre not to be a regulator but to be a supporting function. This is not recorded metrics, but I think experience shows that, by and large, most organisations have welcomed that. I think it is a matter of record that various people, including me in office at the time, have said that when the general data protection regulation on personal data came in, which was a huge, and in my view mostly beneficial but a bit clunky, addition to the regulatory framework, there was an observable change in all jurisdictions covered by it, which is basically most of the west, whether in or out of the EU. American

companies have to care about GDPR because of doing business with Europe. What were sometimes quite informal relationships between government and the company affected became a bit more formal. The general council started to appear a bit more often. I do think that there were things in that.

Outright refusal to be helped, if you like, is pretty rare in the UK, which is one reason why, while I am not particularly averse when it is appropriate to saying, "This needs the force of law", we would want to be a bit careful about doing anything that would reduce the help function of the National Cyber Security Centre when appropriate, without turning it into the national IT—

Q13 **Lord King of Bridgwater:** You say that 1,000 staff are working there. How many different countries are represented?

Professor Ciaran Martin: I am not the head of it anymore. You would have to ask it.

Lord King of Bridgwater: Or in your time?

Professor Ciaran Martin: As part of GCHQ, I assume, as with all the intelligence services, they are all UK nationals.

Lord King of Bridgwater: I thought that within GCHQ there was some exchange of people with those with whom we had good fraternal relations.

Professor Ciaran Martin: You would have to ask it. There are integrees and so forth. There has been a small number. I do not think it has ever been declared publicly which countries have and have not formal interchange with that part of GCHQ, but yes, there have been integrees with other countries.

Lord King of Bridgwater: I am asking you whether in the NCSC you had a few people from other friendly countries and showed them what we were doing.

Professor Ciaran Martin: There were a handful, yes, a handful.

Lord King of Bridgwater: A handful?

Professor Ciaran Martin: Yes.

Q14 **Lord Powell of Bayswater:** Professor Martin, before we leave the last question, one of the things you did at the NCSC was to set up the Cyber Security Information Sharing Partnership. Were you happy with the take-up of that scheme from business, or were you disappointed?

Professor Ciaran Martin: It is one of a number of areas where good concept has not scaled properly yet, so there is more to do. It is an interesting and challenging problem. As with much of cybersecurity, it is about economics and economic incentives. Clearly, some busy businesses do not quite see what is in this for them. It behoves government and so on to look at why that is, yes.

Q15 **Lord Powell of Bayswater:** Coming on to a more general question, the

number of incidents just seems to grow like Topsy. Every year, there are more and more incidents. Is that a perpetual process, an inevitable trend? Do we just have to get used to it, or is there some way that you think will emerge to get on top of the problem and cap it?

Professor Ciaran Martin: It depends what we mean by incidents, and I do not mean to go all technocratic on you, Lord Powell. As an observer rather than anything else, I would say that the statistics in the NCSC annual reports of 2017 to 2020 on the number of incidents the NCSC dealt with tell you nothing more than the capacity of the organisation. That is at the top. The job of the centre is to triage the most important incidents with which it has the capacity to deal and work accordingly. Of course, one big incident might wipe out your ability to do 100 small ones, and then the overall number in a year comes down. Again, to Lord Harris's point, it is an interesting output or metric, but it may not tell you a great deal more.

There are other metrics, such as metrics on ransomware. When it comes to how much of this we will have to get used to, major state-sponsored espionage and so forth—obviously, a very serious case was exposed in the United States recently—is something we will be living with. The thing that we are living with that I passionately believe we should not be living with is the crazy rise in dangerous ransomware over the last year, because that, in my view, is a fixable problem that requires more international attention.

Why do I say that it is a fixable problem? It is fixable, first, because a lot of the international criminals who do it are well organised but not technically that sophisticated, so there are potential mitigations. For what you might call classic ransomware, which just locks you out of the data so you cannot use it and are stuffed, so you pay a ransom in order to get back online, good deployable back-ups take care of that problem.

There is a new variant of ransomware that means that the ransomware threatens you by leaking your data online or gives you an information security breach. Obviously, good back-ups do not take care of that problem, but at least they mean that you are not locked out of your systems. Margaret Beckett mentioned the potential national cyber force at the start. Potentially, where possible, given that these organisations are not always that sophisticated, when all else fails we can just disrupt these people online.

Bringing together a whole bunch of questions from the committee, I would love to see a recognised international measure of ransomware. There are various academic and industry ones that are all going hugely and rapidly in the wrong direction, and I would like to see a whole suite of activity of defensive back-ups, better protections, and, frankly, some disruptive measures that in two years' time would dramatically reduce it. I do think that is achievable.

Q16 **Lord Powell of Bayswater:** The last aspect is resources. Do you think that a massive increase in resources, by both Governments and business, would make a substantial difference in cutting it back? Or is it rather like the cycle of weaponry: every offensive weapon produces a defensive

answer, which then produces a new offensive weapon?

Professor Ciaran Martin: Quite a lot of the transformative capabilities with regard to ransomware might not need that much value of resource. It might just need smarter public policy. In terms of disruptive capabilities, it is a question of choice, effort and trade-offs, because you may have less to deploy against terrorist groups or whatever.

More importantly, to return to my area of greater expertise on the question of defensive measures, one of the problems with ransomware in particular is the whole economic framework around it. The position on insurance and ransomware in this country and in the United States is crazy. In this country, it is not just allowed but increasingly routine practice to pay out to cover the costs of paying criminals. If you pay the criminals in bitcoin, you can claim it on your insurance policy, unless it is a recognised terrorist organisation. That is because the law on extortion dates from international terrorist kidnappings. The problem there is that, for a variety of reasons, international terrorist groups do not really do cyberattacks, so that prevents nothing.

Most people pay, and they can claim it on their insurance. However, if you get a fine under the GDPR—the general data protection regulation—you cannot claim that on your insurance. How you contrive a system where both of those things hold true I just do not know. It is the same in the US: you can routinely claim on your insurance policy for paying the criminals, and if you pay a ransom it is fine unless it is on the US Treasury sanctions list. So, again, there are people who are in the middle of a ransomware crisis looking up the US sanctions list and guessing whether their criminal of choice is on it. Why? What public policy benefit does that have?

A lot of experts say that if you criminalised payments of ransomware it would not solve the problem, and maybe that is right, but it is worth a serious piece of analysis, in my judgment. I do think that a situation where you can insure against paying criminals but not against regulatory fining makes no sense. There are measures that you can take. Then again, if you do not have a back-up and you suffer a classic ransomware attack, if it is personal data you will get a regulatory penalty; if it is not, you will not. What is that about? There are things that we can do with public policy to change the incentive structure that do not require much resources but do require quite deft thinking.

Lord Powell of Bayswater: I am very glad that you brought that point out, because it is very important and business needs to learn from it. Thank you.

Q17 **Lord Brennan:** Professor Martin, in reply to Baroness Healy's question about the pandemic, you said that one of the challenges was capacity. If we think for a moment about the vaccination exercise that is going on at the moment and that will have to be repeated if there is to be a second injection, it is probably one of the most gigantic public service projects in peacetime that we have ever had, involving a number of ministries, GP practices, individuals' private records and so on. How do you think we

ought to assess this element of risk for the future: namely, the enormous size of the problem that cybercrime could attract?

Professor Ciaran Martin: The privacy and confidentiality of health records is something that Governments across the world take incredibly seriously. The NHS is interesting in this context. It is a good example of the need to strike a very difficult balance between practicality and security. Everybody wants the vaccine to be injected into people's arms as quickly as possible. That requires an enormous amount of logistics. Technology helps with those logistics, but, of course, what you do not want is a massive data breach.

The UK in some respects was fortunate in its most serious cyber crisis, which by fluke affected the health sector back in 2017. That led to some really sustained work, which was already happening but was accelerated massively with the NHS Digital part of the NHS, to look at that issue. One of the structural challenges with the NHS is that, in totality, it is a massive organisation but, as we all know, a very disaggregated one, with tens of thousands of smaller organisations, including the small rural surgery across the road from where I am sitting, with a handful of desktops that need to be able to access the same systems.

I honestly do not think that it changes the model of cybersecurity, though. You need to think about the sort of data you are capturing and when you need it centralised. You can say what you like about some of the things about the app or the way data flows, but quite careful attention is paid to where data is at any one time in aggregate. That is the sort of thing that we need to be looking at quite carefully.

What you want to do is try to work out, quite literally, the worst that can happen and try to design and build the system to make sure that it cannot. Then it is just impossible to have the single congregation of data in one place at any given time where you can just lose it all. However, in something of this complexity, you will never have 100% security, so it is about trying to cauterise the worst potential outcome.

Q18 **Tom Tugendhat:** It is very nice to see you, Professor. Thank you very much for joining us. Many of us have had questions about another aspect of your advice over recent years, which is of course the Huawei question, which came up in a debate that shaped quite a lot of actions of last year. Could you please tell us a little bit about the origins of that debate and how you see the change in the Government's position and the advice that went into it?

Professor Ciaran Martin: Sure. In some respects, the different aspects of the policy choices for a democracy to take are becoming clearer now and easier to explain. I hope you will forgive me for putting it this way, but if you take three pending votes in Parliament—probably in this year—one, as I understand it, is your amendment on slave labour and so forth, another is the telecoms security Bill, and another is the National Security and Investment Bill.

Those show three different aspects of what we are dealing with. There is the ethical problem of business with China, given the horrendous repression—on which I am not expert, but which any well-meaning private citizen would be extremely concerned about—which is being voted on. I mention that because, as I understand it—please correct me if I am misinterpreting this—the substance of that discussion is essentially that you are talking about forced labour, slave labour, camps, and that it is completely wrong to have any commercial transaction on products there, even though those products would not cause a strategic national security risk to the UK should the UK choose to buy them. That is one aspect of the problem.

The Huawei advice was not about that. It was about whether, if you were to buy some equipment from a Chinese provider that has been in the UK, with a risk mitigation model, for more than 15 years, that would constitute not an ethical risk but two risks, one being a national security specific risk. In other words, would it give China a button with which it could do harm to the UK? That is a question of technical judgment. There was disagreement at the time between the UK and much of the rest of the European continent and much of the rest of the world. Other countries, principally the US and Australia, and to some extent Japan, have said that if we involved Huawei to a certain level, it would not give that button.

This takes you to the telecoms security requirements. There is a series of structural problems in telecoms security that need to be fixed regardless of who the provider is. The so-called SolarWinds event, the huge Russian compromise of the American private and public sectors, vindicated that approach quite dramatically, because it showed that it was not just about the country of origin.

Russia does not sell to the West in technology terms. There are one or two anti-virus companies, but it does not try to do what China does. Yet by compromising a company based in the wonderful city of Austin, Texas, one of the friendliest places in the world, where of course we trust the intentions of the corporations, the Russians have gained a huge foothold. In a sense, the challenge for the advice was whether you can mitigate Huawei at a technical level. It is for democracies to judge the ethics of it. Can you mitigate it at a technical level? Yes. How do you stop the remaining providers, Nokia and Ericsson, becoming our SolarWinds, if you like? That is the second thing.

The third thing is not so much national security risk but national security dependence. Does this create dependence over the long run? Again, the original 35% judgment was that it did not. However, as you know, because I gave evidence to the committee that you chair, there are other technologies where that could be the case—where you would not want to get in particularly deeply with Chinese or indeed other authoritarian-country providers and that the Government are right to take powers to prevent that happening.

For those reasons, given the intrinsic vulnerability of the UK telecoms sector, including what you might call the SolarWinds-type risk, the 35%

judgment was viable based on the model we already had. Then it changed. We have had this discussion before, and the vote, if you like, on what you might call China policy. The desirability, morality and ethics of doing business with China might have won the day—it was never fully tested—but because of US sanctions it blew the mitigation model apart for Huawei. It was no longer possible to assure its products technically, so the advice changed. That is the best I can do on a very, very complicated story.

Q19 **Tom Tugendhat:** You will know very well that I disagreed with the Government's assessment at the time, but your own professional input was something I never questioned and was extremely grateful to have, and not only yours but Dr Ian Levy's, who I cannot fault for his openness and frankness in addressing questions.

Can I ask a procedural question perhaps rather than a factual one? In a question like that, clearly the NCSC is put under enormous pressure, and many different people are trying to get a political answer out of what, frankly, is a technical body. How do you structure your conversations to make sure that you are responding to the technical requirements put before you and not to the politics? How do you also make sure that the Government's politics do not influence your technical assessments?

Professor Ciaran Martin: It is an excellent question. The one thing I would never say is that our technical assessment should carry the day. It is an input into a democratic judgment by parliamentarians, which is absolutely right. That is why, in the opposite direction, if you do not mind me saying so, your broader strategic view of the challenge was entirely right. It is right that Parliament judges and that elected politicians, Ministers, if they can carry the House with them, or the House as a whole, take the decision.

In one sense, the answer was relatively simple. Our job was to tell the National Security Council how the 5G network works—what the options are based on the market we have now and what the security trade-offs are, because they were trade-offs. The fact that Huawei is now excluded and you are left with two providers is shaky in resilience terms. That is pretty self-evident, so it is a different challenge. There was never going to be a very easy answer. Our job was to make that technical assessment and then other people's to bring the ethical arguments, the foreign policy arguments, the commercial arguments, the diplomatic arguments—China and the US, and so forth. The Government took a balanced decision.

I do not honestly think I ever felt under any real pressure to change the judgment. If I have a reflection on the process—and this is why I think we are in a better place now, as per in answers to other members of the committee—it is that the UK Government, through the National Cyber Security Centre, put an enormous amount of technical detail out there for scrutiny. You could agree with it; you could disagree with it. I think it is better now that we are having a debate about the overall ethics and efficacy of China posture rather than doing it as a proxy—"Oh, I think the NCSC was wrong about the compromisability of a base station". It is a better

discussion to have, I would have thought, based on the balance of expertise in the relative areas, if you know what I mean.

Tom Tugendhat: That answers the question. Thank you very much, Professor Martin. I am extremely grateful.

Q20 **Lord Campbell of Pittenweem:** It is very nice to see you, albeit in your new role. You have begun to sound very philosophical about a period in your professional life that must have been pretty stressful, and unusually so. For someone like me, who does not have much, if any, technical knowledge, I would begin with the presumption that because my side of the argument was technical, that should prevail. What was your sense of disappointment, if any, once these other considerations were made, considerations which you are perhaps not relaxed about—perhaps relaxed is not the right way to put it—but which you now accord some weight to? What was your reaction when that happened?

Professor Ciaran Martin: First, I am not sure that it matters, but you asked, Lord Campbell, so I will answer.

Lord Campbell of Pittenweem: No, it is very important to this, because this is not the first clash, if you like, between politics and the technical. In an increasingly technical world, the likelihood of that kind of tension arising seems to me to be something that we have to take more account of.

Professor Ciaran Martin: There are three things there. One is that the technical facts changed, so the American sanctions made an ongoing risk mitigation model impossible. There are many people, and I think Mr Tugendhat, quite possibly correctly, is one of them, who would say that had that not been the case and it had been pressed to a parliamentary vote, the Government would not have won support for their original recommendation. We will never know that, because the technical facts on the ground changed.

Secondly, as a democrat, I am relaxed about elected parliamentarians and indeed Ministers taking judgments on the balance of risk, because, first, telecoms and internet infrastructure are not just about security. Security is not the absolute. I know it is facile to say this, so forgive me—it is just to illustrate the point—but the way to have 100% security is not to build something that is useable.

Lord Campbell of Pittenweem: Of course, yes.

Professor Ciaran Martin: You are always making trade-offs, so even without the very contentious politics of China policy there would have been judgments. In plenty of other sectors in the last 30 or 40 years, there has been a very domestic argument about whether the excessive regulation was strangling innovation in the name of security and whether the Government were getting too heavy-handed. There is always that dimension where a security-minded person might say, "You must do this", and the Government say, "No, because that will kill the market". There are always other factors anyway, and it is right that elected Ministers, ratified by the House of Commons and the House of Lords and so on, make those judgments.

Finally, you asked me to reflect on the personal aspect of it, so I will answer honestly in the spirit of the question. I have no complaints, apart from the fact that I am a democrat who respects democratic judgment, because, as I was saying to Mr Tugendhat, if there are much bigger issues of global policy, of foreign policy, of ethics and so on, they should be put on the table. That what was happening, but it is really happening now.

It would have been damaging to the NCSC if some people just said, because it suited their particular argument, "The NCSC has this wrong. Its technical stuff about being able to mitigate risk is all rubbish". Mr Tugendhat never said that, but others did because they heard it from somebody in some think tank somewhere. Dozens of pages of highly professional technical analysis had been published for scrutiny, and somebody said, "Oh, that's just wrong. 5G is just a big bubble of risk, and if you do one attack it blows the whole thing up".

If the NCSC had been overruled by Ministers or by Parliament on that basis, that would have been hugely damaging because it would have been a rejection of its technical expertise. The NCSC's technical expertise was never rejected, which is hugely important. Had the issue proceeded on the original basis and been changed because of wider China-policy grounds, that would be fine. As it turned out, the technical facts changed, so the technical recommendation changed. Of course it was stressful. I am not going to pretend that it was anything other than stressful, but in its own sort of idiosyncratic way the process of British democracy worked quite well.

Q21 **Lord Campbell of Pittenweem:** I am aware of some of that, because I served on the intelligence committee and I well remember you coming to give evidence. One last question. Do you think the NCSC is stronger as a result of these events?

Professor Ciaran Martin: Yes, because relevance to public policy decisions is everything, is it not? If you look at the problem that we have been banging on about—forgive the phrase—all through this hearing, which is that we have not put security inputs properly into the framing of our digital policy, that is no longer true. That is great. Ministers took the technical recommendations very seriously, and the initial set of technical recommendations based on the pre-US sanctions basis gave them a choice. They made a contentious choice and it was properly debated in Parliament. The interesting part was that when the NCSC said, "Look, the facts have changed. We can longer assure this model", the Government did not press ahead with something that their security experts said would not work anymore.

In a sense, that shows that the National Cyber Security Centre continues to be a highly relevant body in public policy decision-taking on digital. I do not think that my successor, GCHQ or anybody ever says that they should have sole authority to direct what public policy should be in a democracy, but the NCSC has a very strong voice and I think the country is better off for that.

Lord Campbell of Pittenweem: I was fascinated by what you said about ransomware, but that is a topic perhaps for another occasion. Thank you very much.

Q22 **Richard Graham:** Professor, it is very good to see you again. I have two questions. The first is a relatively straightforward technical one. Do you think the telecoms Bill will now resolve the issues of 5G, or do you have any lingering concerns that taking out Huawei boxes and replacing them with Ericsson or Nokia boxes, which clearly say, "Made in Shanghai" does not necessarily resolve the problem as some people thought it would?

Professor Ciaran Martin: I get the point, definitely. This is what I referred to, in answer to Mr Tugendhat, as the SolarWinds problem. In technical terms, not in political terms, the position of Huawei 5G with regard to the recommendations for the Telecommunications (Security) Bill was a secondary issue. The primary issue was the security of the framework as a whole, which goes precisely to the point that you mentioned: what standards are Nokia and Ericsson adhering to, and what are their protocols for third-party access? I know that is a techie phrase, but it is very, very important for precisely the reasons you mentioned in your question.

Encouragingly, my answer to your question is yes. Now that the Huawei issue is resolved, for better or worse, essentially by the change in US sanctions, the important issue is now the regulation of standard providers, which come from trustworthy backgrounds, such as rule-of-law democracies in this continent et cetera, but you cannot automatically trust their equipment or their practices because it is a very complicated business with a history of poor security. The telecoms security Bill will have its imperfections, because all pieces of legislation do, but by and large it is, in my view, the right framework for regulating security in 5G and telecoms more generally.

Q23 **Richard Graham:** Thank you. My second question is almost the reverse of Tom's earlier question. Clearly in an era where two superpowers dominate the world, there will be increasing pressure and demand on the NCSC on what you might refer to as China issues. In the Minister's foreword to this year's report, he credits you strongly with striking the right balance between economic opportunity and security. How easy will it be for the NCSC to continue to do that when issues like TikTok are raised, where video films and video-sharing services form no part of the 13 identified CNI sectors but there may be concerns about data? How easy will it be for the NCSC effectively to represent the view of the agencies so that parliamentarians are sure about the technical assessment?

Professor Ciaran Martin: It is an interesting point. Most of the TikTok stuff has happened recently, so I will comment as an observer rather than from anything I know a great deal about from the inside. First, this is all observation. The NCSC, to my knowledge, has not put out any erroneous or inflated view of the risks of this particular social media app. Something is conspicuous here by its absence. I do not think that in the NCSC's history, pre and post me, there is any evidence of politically pressured assessments. I am not deflecting. I just think this is the bigger problem.

TikTok is a very specific example of a not terribly strategically important service, in my judgment. Others may disagree, but in my judgment it is not terribly significant.

There are all sorts of other dimensions—you mentioned the 13 areas. There is a really hard bit of government coming up, for two reasons. One is that you are broadening out the definition of cybersecurity to a really strategic level. It is no longer just about whether the networks are safe from keyboard warriors in other countries; it is about security of supply, where you buy things from, what you need to be completely sovereign and what you need some allied stuff in, how you control a European or a North American supplier's supply chain—all of that. To give all that to a cybersecurity body when it is a huge issue of economics, trade and so forth is a very, very difficult problem. It gives rise to a challenge which democracies, including this one, are historically quite bad at, which is doing economics and security at the same time in the right balance. That is the bigger problem.

Richard Graham: Sorry to interrupt, Professor. Do you think it should be more with the NSC then than the NCSC once it gets raised above the purely cybersecurity issue?

Professor Ciaran Martin: Yes, definitely. I understand that that is the way it is going. It is a huge role-of-government issue. I am not downplaying the UK's role in the world—it is a significant player—but at the same time it does not make the global market all by itself. Sometimes it is a bit lazy. We heard this a lot in the 5G debate: "Oh, let's build a Five Eyes alternative to Huawei". The Five Eyes is an intelligence-sharing alliance. It does not build telecoms companies. There is no economic, commercial and industrial sub-committee of the Five Eyes. The US and the UK are not common markets, whatever else they are, so we cannot just assert our way out of this problem.

You could easily convene a global meeting where everybody signed up to say, "We're going to build plural technology to get away from Chinese dependence". How you build that reality across like-minded countries is a very, very hard problem. I am not saying it is unsolvable, but you do not want to just—[*Inaudible.*] The solution at a global level is not security ministries but economics, industrial ministries, trade ministries, and that sort of thing, so we need to broaden it. That is a very hard problem.

Richard Graham: Thank you very much indeed.

Q24 **Darren Jones:** Thank you, Chair. Professor Martin, I have a quick supplementary question about a comment you made earlier, before two substantive questions. You raised the importance of investing in the replacement of legacy IT systems. In the last Parliament, when I was on the Science and Technology Committee, we asked Oliver Dowden, who was then the responsible Minister in the Cabinet Office, whether the Government had a funded plan to replace legacy IT systems. There was no strategy in place for that. Do you happen to know whether there is a strategy now or whether we still do not have a cross-departmental strategy

to replace old IT systems?

Professor Ciaran Martin: I do not honestly know. You would have to ask the Government. I suspect that, understandably, because so many of the multiyear decisions were delayed in 2020 because of the pandemic, the answer is no, but please do not take my word for it.

Q25 **Darren Jones:** Maybe we will write to the Minister to try to follow up, but thank you for that.

My substantive question is about the debate between defensive and offensive cyber capability. The NCSC is often described as a defensive capability, trying to stop cyber threats from causing damage to the UK, but you will know that the Prime Minister has announced a new national cyber force as part of an offensive strategy to use cyber capabilities. You have spoken about this before and raised some warnings about being too gung-ho about offensive cyber capabilities. Do you think that is the wrong strategic decision, or do you think we just have to do this because of what other countries about the world might be gearing up to do?

Professor Ciaran Martin: I am not saying it is the wrong decision. A lot of my thinking on this has evolved since I left government, and I have been able to inquire into it more deeply because I have never worked on the offensive side; I was always on the defensive side. Part of the problem is almost that they both have the word "cyber" in them.

Take the declared publicly explained mandate of the national cyber force. Mr Fleming and General Sir Patrick Sanders gave a public account of this at Chatham House in December, and they talked about how it will counter international terrorism and transnational paedophile rings and so forth, and how it will support war fighting. That is laudable and may well prove highly effective.

However, the one thing it does not do is do anything about cybersecurity. It is the pursuit of national security goals through cyber means. The first, and I think only, British offensive cyber operation that has ever been properly declared—it was declared by Sir Michael Fallon way back in October 2016—was an operation against the so-called Islamic State's propaganda machine, which, as we remember, was, sadly, horribly effective in all sorts of ways.

Ahead of the Mosul offensive, a huge allied offensive cyber campaign was publicly declared. In my view, that campaign, which it is understood was successful, would have achieved three different objectives. It would have reduced the risk of international terrorism by degrading ISIL's online capability to organise. It may well have reduced the threat from domestic terrorism, because people who could be radicalised by it in this country would not have seen the material. It would have aided the military allies who were engaged in that offensive.

It was absolutely nothing to do with augmenting UK cybersecurity, because ISIL was a horrible threat in many ways but it was not a cybersecurity threat. It did not have cyber offensive capabilities. There is a popular

misunderstanding about what offensive cyber is for. It is not primarily to promote cybersecurity; it is about using cyber capabilities. I try to steer people away from what I have started calling the "boxing ring" mentality of cyber—an enclosed domain where you have an offensive and a defence, and that is the only sort of thing you are allowed to use.

There are specific warnings to give. One is about the things that we have to get better at managing. One is information security. We hold these tools and there is a history of them leaking from our allies. That can be dangerous. It is much easier for a cyber weapon to leak, to be stolen or to be lost than it is for a physical weapon, certainly a seriously damaging physical weapon.

Then there is the point about safer technology, going way back to my answer to Dame Margaret right at the start. Offensive cyber relies on the exploitation of technological weaknesses. That is how it works. This goes all the way back to the arguments that were expressed after the Snowden leaks and all that, reprehensible though they were. There were issues of trust and questions about whether we are in favour of safer technology or not.

There are difficult trade-offs. Encryption is the classic example. Encryption allows you and I to communicate freely. It secures business information. It enables dissidents in repressive regimes to communicate with each other and so forth, but at the same time it sometimes makes the job of intelligence services and law enforcement harder. We need to get that balance right, and a very gung-ho approach to offensive capabilities does not quite work in that respect.

Those were the two areas where I sounded a note of caution, but most of all we just need to understand what this is for. It is not primarily about promoting cybersecurity; it is about making us safe through cyber means.

Q26 **Darren Jones:** Thank you for that. My last question on this issue is about Britain's role in providing leadership in the world, and about capability for our own country but perhaps also for our allies. The Prime Minister has talked about a global Britain and looked at how we might contribute in a post-Brexit world. Do you think we are credible as a country, whether through the United Nations or NATO, in trying to lead the discussions globally about the ethical use of cyber capabilities and about how multilateral organisations like NATO might respond if a cyber threat triggers the types of concerns that we have, where we are kind of committed to supporting allies? Do you think that is something that Britain should be leading, or do you think that other countries are better than we are at it and that we should look to them?

Professor Ciaran Martin: I think the UK is in a decent position when it comes to credibility as a competent country on cybersecurity and the responsible use of offensive cyber. Overall across the globe, if you take the 10-year view, I think that if people were told 10 years ago about the situation now, they would be quite surprised at just how little progress there has been towards agreeing a set of rules for cyber conduct and so

on. When I first came across cybersecurity, about 10 or 15 years ago, everybody showed this picture of Piccadilly Circus in 1911, with all these motorcars pointing in the wrong direction and everybody piled up. The whole thing was: "Eventually we sorted out rules of the road, and that's what will happen in the cyber space". There has always been that assumption.

This has been much slower and nobody is leading. I think the UK has been a bit reluctant for precisely the reasons I have just explained. There has always been this sense of, "We'll obey the rules, but Russia and China will not if we exercise restraint". I think there is scope to be a bit more forward leaning, and UK leadership may well be welcomed, but I do not know. We will see.

Q27 **Baroness Neville-Jones:** What you have just said is a lead-in to the question I wanted to ask you, which is about international rules of the road. I have for some time thought that we needed closer integration between the domestic side and the military side in cyber. When I heard that GCHQ and the MoD were going to co-operate more closely, I thought that this was a good start. I have to say that I am not at all clear what that relationship is intended to lead to. You clearly have reservations about it being something that gets GCHQ involved in the cyber side of things, which is a power issue, not a security issue, it seems to me.

Do you agree that there is use in greater integration? If so, where do you think it should lead? It seems to me that some of the most useful work that has so far been done on rules of the road, for instance, had been done in the NATO and the military context in places like Tallinn. That is a strong point for the West and somewhere where western NATO allies can rally.

Could you spell out to me what you think the fruitful route might be, if you agree that integration is useful, and how that complex of expertise might be used?

Professor Ciaran Martin: I am broadly sympathetic to your points, Baroness Neville-Jones. Where does integration work? Look at the 102-year history of GCHQ; its original purpose was supporting military operations.

Baroness Neville-Jones: That is right, absolutely.

Professor Ciaran Martin: Clearly I am no expert on military strategy or war fighting, but I think that I know enough and it is uncontentious enough to say that, in future, military conflict will involve a very significant technology dimension and therefore it is absolutely right that there should be embedded and joint arrangements for that sort of thing. That is very much where it is.

I mentioned that a declared purpose of the UK's new arrangements is to do with international online child sexual exploitation, which is where it gets a bit complicated. I do think there is a case for intervention there, because so much of that horrific trade takes place in non-western countries, where it is effectively out of reach of law enforcement, I have to say. So

intelligence-led disruption is very justified, but doing it through a part-military organisation is a little curious, because there are historical differentials between military intelligence and law enforcement functions in democracies, for very good reason. So there is something there. Looking at definitions of cyberattacks in Article 5, the Tallinn Manual and so forth, I do think that there is a real opportunity for the UK to bring that thinking forward.

If I have one criticism of the current posture, it is about the process. We are having a very interesting and fruitful discussion about this. In answer to Lord Harris, I have talked about transparency in cyber defence, how you get assurance and how you challenge and so forth. The answer is: just put the stuff out there. I do think the Government have been more reluctant that they need to be to just put stuff out there about these precise issues. You are not compromising national security capabilities by having this discussion in public. There is absolutely no question in my mind about that. There is a whole ream of academic scholarship of global diplomatic publications and so forth, like the Tallinn manual.

These debates should be had in public, because there is potentially a very significant offer in the expertise of people on these screens and lots of people in the UK. If you have that broader conversation, it could amount to a very powerful offer from the UK of global leadership in the cyber domain. We have been remarkably reticent about putting it out there for reasons I do not quite understand.

Baroness Neville-Jones: That is very interesting. There is a model, I think, from my nuclear experience, of putting out doctrine. The doctrine provides stabilising points, so that people understand.

Professor Ciaran Martin: You know 100 times more about this than I do, but I think it is a very good example of how you can talk about the operational environment about capabilities, the legal/ethical doctrinal framework about them, without saying anything about how they work and that would compromise the effectiveness of their ultimate use.

Baroness Neville-Jones: So you do think that there is something fruitful to be done there. My impression is that you are not quite sure that we are moving in the right direction at the moment.

Professor Ciaran Martin: That is probably a little too strong. Offensive cyber is not new, and there have been disruptive operations under law for many years organising them. Some of them are military, some of them intelligence, and customers will potentially include law enforcement cyber defence, the NCSC and so forth, depending on the operation. There is much to be said for it.

Probably three things could do with further illumination, which are slight concerns. One is clarity of mandate; the relationship between organised crime and law enforcement is a good example.

The second is risk management. I said in a public lecture that, as far as I can tell from the outside, western organisations operate on the premise of

100% security of capabilities 100% of the time, and clearly history says that you should not do that. So, yes, I think we could do with a bit more discussion and elucidation of how we manage those risks.

The third is where we are going with this. First, I would like to see an unambiguous commitment to safer technology. That really does matter in this space, because when you talk about how we are going to use increasing offensive cyber, many people—I am one, but there are much stronger voices—say, "Okay, are you serious about the primacy of safer technology for everybody?" because there are trade-offs there, so we need to make that absolutely clear. Secondly, what is your end game? What you are trying to achieve at a global level in bringing order to this newly created, human-created domain?

Baroness Neville-Jones: That is a lot of food for thought. Many thanks.

Q28 **Baroness Henig:** Professor Martin, can we turn to skills now? You said right at the beginning, I think, that we have further to go on skills. Our predecessor committee looked at cyber issues in 2018 and was very concerned about the level of cyber skills and the delay in government producing a cyber skills strategy. Eventually, an initial strategy was published in December 2018 and there was more consultation. Did the non-appearance of a final skills strategy harm the NCSC's work in any way or the country's ability to fill our cyber skills gap more generally?

Professor Ciaran Martin: I do not think it harmed the NCSC's ability, for better or worse because of the size of the organisation and the elite nature of the skills you need. In that respect, the delay to the strategy by a year or two is neither here nor there. You are trying to grow your own skills. You are trying to incentivise a small number of people either to come in or to stay, and then you train them with the existing expertise. At the NCSC level, I could not hand on heart say that I thought the country's national authority for cybersecurity was harmed.

More generally, I do not have a hugely strong view on this. When the NCSC was first set up, I very much did not want its mandate to be too broad, because I just thought that was undoable. Taking charge of a digital skills strategy for a nation of 66 million people and the fifth largest economy in the world while fixing cybersecurity was going to be a pretty tall order.

It is easy just to complain about skills shortages, but it is better to be forensic about what we mean. We are probably talking about broadly three levels of skill. The first are the elite skills that you need for a small number of organisations, principally the NCSC and a few others. The second are the skills that are good enough for big important organisations like major government departments, private companies and so forth. The third set of skills is just basic digital and security literacy for the whole population.

I would like to see a strategy for skills that gets that into the long term. I think we are doing okay in the first. It is not just getting people into the NCSC, but things like accelerators and skills competitions for elite people. The NCSC started doing this with people at PhD level and has ended up

going back right back into the early years of secondary school, which is a really good thing. You are already seeing the fruits of that, but you are talking dozens, hundreds, low thousands and so on, and it is creating that ecosystem.

What that does not do is take care of the other two problems. I think the second problem is getting better. I keep going on about getting good ideas to scale. The accreditation framework, where you can say, "This meets a particular standard", works quite well on skills. It does not work that well on other areas such as product assurance. It is not perfect and is probably not quite where it needs to be, in my judgment, but it is getting there in terms of a pipeline of people who are good enough to do the other jobs that I mentioned—in big government departments and so forth.

Then you get into the long term. Baroness Lane-Fox knows much more about this than me and is deeply passionate about it. This is where a delay of one or two years does not matter that much, as long as it is only one or two years. But you have a choice about the whole education system and how much you are going to re-pivot it for the long term for a generation—for kids entering primary school now, who will not be in the labour market for 20 years—and how much you are going to just reposition the whole education system around STEM, digital skills and so forth. There is a very strong case for doing that. You will not see the results of that any time soon, but it is a worthwhile investment, in my judgment, although a big, hard choice.

Again, delivery of that sort of scale of change is rightly for the Department for Education. Of course organisations like the NCSC should be saying, "Look, these are the sorts of things that we anticipate that we will need as a country", but at the end of the day it would be disastrous to sort of tack this on as NCSC responsibility, because it has to be in the bloodstream of the education system, not some sort of add-on from a specialist body.

Q29 **Baroness Henig:** You may not be able to answer this question. How do we rate in terms of skills compared with, say, the United States or China, or other major cyber powers?

Professor Ciaran Martin: I honestly do not know. Proportionately, given the various rankings, we tend to come at or near the top in elite skills at governmental level, so are okay. On general digital skills, I honestly do not know. STEM graduates are way behind the big Asian giants. But I do not want to busk on areas that I do not really understand, I am afraid, so I will leave it there.

Baroness Henig: Sure. Thank you.

Q30 **Lord King of Bridgwater:** Professor Martin, I congratulate you on a real endurance feat in our gathering today.

I want to ask you a question about Brexit. I understand that various initiatives that we have on cybersecurity, which had been previously going on, will now continue on a voluntary basis. That is confirmed by the communications Act that we have just passed. What do you think about

that? Will it cause problems, or will things go on much as before?

Professor Ciaran Martin: Honestly, no. Given the obviously very heated political arguments, I will try to be as analytical and objective as possible. My experience and expertise are of an intelligence-led organisation, and obviously the challenges of issues of law enforcement and Brexit—the Schengen database, co-operation on the prosecution of digital crime, and so on—will arise, as they do for non-digital law enforcement, and we will see where they end up.

On the question of the sort of cybersecurity that the National Cyber Security Centre gets involved in, and the Government's national cyber security strategy more generally, most of those functions were under the auspices of national security and therefore exempt from the treaties of the European Union.

In the last six or seven years of UK-France cybersecurity co-operation, for example, there was seamless improvement, even though half of the period was pre-referendum and the other half was post-referendum. That is not say that people did not talk about it; of course they did. But basically the UK did not have to stop doing anything with France as a result of Brexit, and most cybersecurity alliances in Europe are bilateral or voluntarily multilateral ad hoc alliances based on competence—competence as in quality, if you like—rather than legal competence.

Then you get to the agreement signed on Christmas Eve. Voluntary arrangements are not the same as binding arrangements, but the UK is well regarded in this area, so I would expect its technical expertise to be sought. Having said all that, the principal body here is a standards body called ENISA. Again, in office, I never sat waiting for the ENISA diktat; it was not that sort of job. I do not think it makes a great deal of difference.

There are two areas to watch out for, which are bigger than cybersecurity. One is the data adequacy point, which is well known and is one of the big issues that is essentially parked in the arrangement. It is very important for the UK's digital economy. When you are trading in anything that involves personal data with the EU, will it conform to EU standards? There are negotiations ongoing as per the agreement. That has ramifications for cybersecurity, but that is not its primary purpose.

Secondly, the UK has to act differently in a 5G-type technological diversification debate, because, as I said, it is about markets, trade and all that. Clearly, negotiation is very different outside the EU than within it.

Lord King of Bridgwater: Will you say anything about NATO? Are cyber initiatives in the NATO field a more important area?

Professor Ciaran Martin: Certainly, and, pursuant to the exchange with Baroness Neville-Jones, NATO is hugely important. The UK is well regarded, as you will know. I hesitate to put this in an answer to someone like you, but NATO—

Lord King of Bridgwater: Where you have that wrong is that none of this

stuff existed when I was Secretary of State for Defence.

Professor Ciaran Martin: But one of the things that still holds true, as I understand it from the likes of Lord Ricketts and so forth, is that NATO operates in a fundamentally different way to the EU. It is much more voluntary and consensual and obviously does not have its own body of law that is of great importance. The UK's influence in NATO on cybersecurity is well sought after. In 2019, Secretary-General Stoltenberg brought the NATO ambassadors to the National Cyber Security Centre with the then Foreign Secretary Hunt. UK leadership is recognised, and NATO, as you know, works by agreement, by consensus, on a voluntary basis.

I do not know if this constitutes a declaration of interest, but to give you an example, because the Secretary-General and his deputy are taking cybersecurity very seriously I was asked to be an adviser to them after leaving office, so I do that as well. I think that the UK influence in NATO is strong. Some of the big changes in NATO, such as the NATO industry cyber partnership and the cyber pledge—I will not go into detail on all of them, given the time—have had a lot of UK leadership, thought leadership and delivery leadership involved in them.

Lord King of Bridgwater: Thank you very much indeed. You have done very well. Over to the Chair.

The Chair: Thank you very much. Yes, I think we are all very grateful to you, Professor Martin. For an individual to give evidence for a long session like this is quite taxing, so we very much appreciate it. It is a pleasure to see you again. Thank you very much for your attendance today.