HOUSE OF COMMONS

Public Accounts Committee

Oral evidence: Cyber security in the UK, HC 1745

Monday 1 April 2019

Ordered by the House of Commons to be published on 1 April 2019.

Watch the meeting

Members present: Meg Hillier (Chair); Douglas Chapman; Chris Evans; Layla Moran; Stephen Morgan; Anne Marie Morris; Bridget Phillipson; Lee Rowley; Anne-Marie Trevelyan.

Sir Amyas Morse, Comptroller and Auditor General, Adrian Jenner, Director of Parliamentary Relations, National Audit Office, Tom McDonald, Director, NAO, and Richard Brown, Treasury Officer of Accounts, HM Treasury, were in attendance.

Questions 1-134

Witnesses

I: Sir Mark Sedwill, Cabinet Secretary and Head of the UK Civil Service, and UK National Security Advisor, Madeleine Alessandri, Deputy National Security Advisor, Cabinet Office, and Ciaran Martin, Chief Executive, National Cyber Security Centre.

HOUSE OF COMMONS

Reports by the Comptroller and Auditor General

Progress of the 2016-2021 National Cyber Security Programme (HC 1988)

Examination of witnesses

Witnesses: Sir Mark Sedwill, Madeleine Alessandri and Ciaran Martin.

Q1 **Chair:** Good afternoon and welcome to the Public Accounts Committee on Monday 1 April 2019. We are here today to discuss cyber-security, among other things, with the head of the civil service and the National Security Adviser—I will introduce the witnesses in a moment. I think this is the third occasion when we have looked specifically at cyber-security, so we want to get to grips with how money is being spent, what it is achieving, and where things are going on that.

We also have the opportunity to ask the head of the civil service about his time at the Home Office—we will be picking up issues relating to Windrush, the emergency services network and the Disclosure and Barring Service. We told you that we want to ask about those matters, Sir Mark. We appreciate that you are no longer in that role. Obviously we have given you notice of this. We have had a busy time reading your papers, but that is not a free pass from the Public Accounts Committee. From our previous work, it is fairly obvious what we are looking at, and we hope that if we ask tight questions, you will give us quick, short answers that are to the point.

I will introduce our witnesses. From my left to right we have: Madeleine Alessandri, the deputy national security adviser at the Cabinet Office—welcome to you—then Sir Mark Sedwill, the Cabinet Secretary and head of the UK civil service, and the UK National Security Adviser. Sir Mark, you have three jobs. Are you managing them all?

Sir Mark Sedwill: I have one job, Madam Chair, just with a broad portfolio. It is for others to judge.

Q2 **Chair:** It is not always the case that the National Security Adviser is the head of the civil service as well.

Sir Mark Sedwill: No, it hasn't been—although actually it was, really, until about 2010. I have two very able deputies. We have beefed up their roles and we share the responsibilities between us. So Madeleine's role is bigger than that of some of her predecessors.

Q3 **Chair:** Rumour tells us that you were not keen to give up the national security job when you got the top job in the civil service. Is there any truth in that?

Sir Mark Sedwill: Of course, I didn't get the top job in the civil service under circumstances I wanted. I had a job that I felt well qualified to do and for which I had prepared. Essentially, it was only because of the tragic

circumstances that I took this on. The Prime Minister and I agreed that it made sense—at least for now—for me to continue to combine the full set of functions and ensure that Government as a whole is working together as we go through Brexit.

Q4 **Chair:** Of course, the job you have got as head of the civil service wasn't advertised, was it? It wasn't open to all comers.

Sir Mark Sedwill: No, and generally that hasn't been the case, either. It has been done essentially through a process of consultation, but it is an appointment made by the Prime Minister, having consulted others.

Q5 **Chair:** Okay. We will not get into that too much today, but we may say things about it in future.

I am pleased also to welcome Ciaran Martin, the chief executive of the National Cyber Security Centre. We have had colleagues of yours in front of us before. I think this is the first time that two of you have appeared in front of us. Obviously, Sir Mark has been a regular attender at our hearings.

Before I get into the issues relating to Windrush, I want to pick up an investigation that *The Sunday Times* published yesterday. Among many things, at the heart of it were communications with HMRC, which had important data about financial fraud that seemed to be linked to funding very serious terrorism incidents. Could you clarify whether HMRC is able to share data with the security services?

Sir Mark Sedwill: Yes, and indeed they have an obligation to do so. Obviously they have very serious obligations to protect the confidentiality of all our records, business tax records and so on, but that does not prevent them from sharing data that is necessary to support criminal investigations or, indeed, national security investigations. That obligation has existed for many years and would have existed at the time the report refers to. I understand that they are in touch with *The Sunday Times* to identify exactly the detail behind the report that was published. There is some ongoing court action as well. But the short answer to your question is yes.

Q6 **Chair:** Okay. We know that there is ongoing court action, but there have been reporting restrictions on this issue for nearly a decade now, I think. That seems quite a long time for restrictions to be in place, especially given that there were arrests and people have served prison terms and come out of prison. Is that the sort of Government you want to be heading: one where there are reporting restrictions on something, many parts of which are very public?

Sir Mark Sedwill: That is a matter for the courts. Although you just asked me about the breadth of my responsibilities, obviously they do not go beyond the Executive. That was a matter for the courts.

Q7 **Chair:** You have said that there are conversations now between HMRC and *The Sunday Times*. Obviously, as journalists, they might not be able to reveal their sources—where they got that information—which would be

quite proper. They have worked on this for two years; it has not just come from nowhere. Is there anything you think needs to be shared more readily between parts of Government, or anything that currently is not being shared, that would aid our national security?

Sir Mark Sedwill: In general terms, where Government Departments, with all sorts of information, are aware that a particular record or individual might have a national security or indeed a criminal element, they would always have shared that. Of course, this report dates back to before the era of big data and so on. What we have seen more recently is an ability on the law enforcement and national security side to identify where there may be cases of other kinds. They can then actively ask questions about those individuals, whether they have come to the attention of HMRC, or indeed other parts of Government.

This is an area that has developed a lot over the past decade or so, and it is one of the areas where our security and intelligence services are cutting edge worldwide. But it is that reversal: rather than just other parts of Government being aware of a problem, it is now possible for the security and intelligence agencies to go and seek information because they have a better appreciation of the overall data pull.

Q8 **Chair:** Is there a threshold below which HMRC should not be sharing information? Obviously, taxpayer confidentiality has been a cornerstone of their operation, but I think most of us would agree that where someone is wilfully trying to do harm, they have rather blown their right to confidentiality. Are you content that there is enough freedom for HMRC to share information with those whose job it is to protect us?

Sir Mark Sedwill: Yes, I think so. Madeleine, who is an expert in this—actually, both my colleagues are—might want to add something, but I think the answer is yes. It is not only that they have the freedom; they have the obligation to do so. That is something that has changed through various Acts of Parliament over the last decade and a half, I guess. One would never be complacent in this area, of course, so I would never say that we are absolutely confident that everything is in place—that all the systems, all the legislation and all the powers are necessarily in place—but this is an area where we have made progress.

For example, the operational review that happened after the attacks a couple of years ago identified that the security and intelligence agencies need to break some of their understanding out into a wider community—in that case into social policy Departments—because the terrorist threat has become more diffuse and therefore they need other actors to play a role. This is a continuing process, but there has been no lack of willingness, and I do not think there is any real constraint in the legislative framework to enable it to happen, while—as you say, Chair—of course respecting all the safeguards and protections that we all expect as citizens.

Q9 **Chair:** Ms Alessandri, the story in *The Sunday Times* was based on quite detailed work. If you take their premise, do you think anything has changed significantly that means this could not happen today?

Madeleine Alessandri: Without being aware, as Sir Mark said, of the particular cases they alluded to in their article, I would reinforce that not only is there an obligation on the authorities to share across any information that is relevant for national security purposes, but there are much deeper structural ties now across from the intelligence community with Departments that have capabilities or material that is relevant. There is also a greater, stronger community of understanding of what information is relevant to national security, and therefore a greater willingness and knowledge of what is required to be shared as well.

Q10 **Chair:** Do you think that goes down to a relatively junior level? Would a relatively junior investigating officer at HMRC, or at any other Department, know that something might be of interest to the security agencies?

Madeleine Alessandri: I cannot comment in detail on HMRC processes, but on clarity and the line management of understanding what has to be triggered and what the trigger points are, I would hope that is firmly embedded across that organisation so that even the most junior officers know, through training and induction, at what point they need to escalate if they are not themselves confident that they know whether they should pass it on.

Sir Mark Sedwill: To reinforce the point I was making earlier, given the way that the data is now held, the initiative will often now come from the security and intelligence agencies themselves, because they can identify what the data pulls are and then make inquiries, whereas 20 years ago, when of course we did not have records in quite the same form, it would have had to be the other way around. That ability to pull information into the national security space is probably the biggest improvement.

Q11 **Chair:** We may come back to that in time, but thank you for that. Can I move on to Windrush? I am sure that you have read our Report on Windrush, or someone has read it for you and told you what was in it. We were very concerned that a lot of the warning signs were missed, and of course, Sir Mark, it was on your watch at the Home Office that a lot of this happened. Why did the Home Office not act on information that highlighted the impact on certain groups of compliant environment and hostile environment?

Sir Mark Sedwill: The first thing to say, as I said in my letter to you, is that, like everyone else who has been involved with this, I deeply regret that it happened. Although the number of people who were badly affected is relatively small, one is one too many. I deeply regret that it happened and, had I been aware of it, we would have sought to take action to address it. I should just put that on the record.

If you look back, there were some warning signs. The NAO Report refers in particular to two: the diplomatic telegram that referenced this, and the report from the stakeholder group, "Chasing status: if not British, then what am I?" Those were not brought to our attention—or certainly not to my attention or the attention of senior management teams. There were

individual reports; the Home Office, as you will recall from your own time there, gets a huge amount of this kind of material, but that does not mean it should not have been picked up.

Q12 **Chair:** I suppose the point is not whether it came to your attention, but whether it came to anybody's. Not everything can come to the permanent secretary or the Home Secretary.

Sir Mark Sedwill: No, I agree.

Chair: But surely the whole point of having a well-run immigration system is that, when such issues are flagged and there could be some people very adversely affected, there is a risk mechanism within the system to deal with it. Clearly, in this case these reports were around and somebody would have read them, however junior, but the mechanism did not kick in to make sure that protection was put in. What went wrong?

Sir Mark Sedwill: No, it didn't. That is partly why my successor has commissioned Wendy Williams to look at exactly that. I can probably tell you what I have said to her—I have had a session with her and will have another session with her, and I am happy to cover the points I made to her—but we will need to see her report to see exactly what went wrong in this particular case, how far within the system this particular issue was flagged and so on.

Fundamentally, underlying this—I will be brief, but I can pursue the points if you wish—is, first, the sheer complexity and volume in the immigration system. It is one of the most complex in the world. Case workers and immigration lawyers all struggle with that complexity. That means that sometimes there are unintended consequences. Of course, this was a cohort of people who were not illegal immigrants, but people who were here legally. Therefore, none of the policies were designed to affect them, so it was a problem of unintended consequences, and that is not always as well understood as it should be. The second has been the general shift in law for people to demonstrate status in a country that does not have a national identity scheme.

Q13 **Chair:** That is exactly the point, isn't it? There was a general shift to demonstrating status, very much driven through the Home Office, yet you could ask a number of us around the table, and any MP with a constituency surgery would know that there are people who would find it hard to prove that. It is not rocket science to work that one out.

Sir Mark Sedwill: I agree—I am not defending it, I am just trying to explain it—but that is over a long period and it is not just in immigration. Money laundering legislation is exactly the same; if you want to open a bank account you have to demonstrate status and identity in a way you did not 20 years ago. We have had this more recently with EU citizens who were here but who did not have all the documentation. Some of them felt they were under some kind of pressure to demonstrate a status to which they were entitled but for which they did not have the documentation. That is a feature that, on that occasion, was addressed more quickly.

In this particular case, none of those checks and balances, some of which you referred to, flagged this problem up. I think that is what the Williams review will need to understand. Within the system itself you have ministerial review, appeals, judicial reviews and the Borders and Immigration inspectorate, and none of those identified this.

Q14 **Chair:** But even going back to the design of the policy, you are overseeing the team of civil servants who would have been responsible for providing advice to Ministers. If you introduced a policy that changed things so fundamentally, you would expect to have civil servants saying, "Minister, there could be a problem here, there could be a problem there, you need to think about how you are going to deal with this group, but this bit will go well." The advice should have come up to say that there might be an issue here.

When we heard from Philip Rutnam, when we last raised this, Shabana Mahmood asked why it was so inadequate, and he replied: "The basic answer to your question will be that it was because the work was not done to the standard required. It will have been a failing, to be honest, of understanding the context, of not understanding enough about the populations that were affected and not doing enough work on what the effects could be." He was saying this worked when these concerns "are at the heart of the policy-making process and are about real effects." He is saying it was a failure.

Sir Mark Sedwill: I think he was talking about the impact assessments that were done for the 2014 and 2016 Acts, if I recall. I think, as this incident has demonstrated, that is correct. There was a huge amount of work done on that legislation: impact assessments, stakeholder meetings, panels chaired by Ministers, enormous amounts of written evidence; but those impact assessments were largely focused on the groups that either were the target of that legislation or the partners who were expected to help implement it—the private sector and so on.

What we didn't understand—and we didn't have the analytical capability to do so, and obviously we need to learn that lesson; I absolutely accept that—was that this was a group of people who were not designed to be targeted by that legislation and we didn't identify the unintended consequence of it, or indeed of previous legislation, which was that it affected them. This wasn't solely an issue that arose in my time, just to be fair; it was an issue that arose over many years and in many—

Chair: Can I just say, Sir Mark, that this is the sort of issue that was arising in MPs' surgeries, and therefore would have been coming up somewhere through the system? There must have been enough. I should think just MPs' letters alone would have flagged that there was a pattern here. That is the job of Ministers and civil servants—to pick up where one MP thinks it is one bit of casework, and they see there is a pattern. I use MPs as a proxy for, obviously, a number of advice agencies. The thing about MPs' letters, of course, is that they go directly to the Department—very often directly to the Minister. So there was a failure there, was there not, once the system threw up the problem, to tackle it at that point?

Sir Mark Sedwill: Madam Chair, again, let us see whether for example that particular source of information was in fact there. I am not aware that it was. I am not aware there was any MPs' correspondence of this kind. That is what the Williams review will identify. That is exactly the kind of external check that one would expect to have identified this problem. When I was there we put a system in place, in UKVI in particular, essentially to assess the qualitative data we were getting from MPs' correspondence, in order to identify a problem arising. It is why, for example, we identified that the passport service was moving into crisis, whenever it was—I forget, but I think it was halfway through my time there. We saw this early warning sign coming from MPs' correspondence. I am not aware that we saw that in this case, but that is obviously what the Williams review will identify. As far as I am aware—but that is obviously with the health warning that I don't yet know—the only warning signs were in these two specific pieces of information the NAO report flags.

Q15 **Chair:** But if you have quality assurance processes in place—and of course you ran the UK visas system for two or three years—

Sir Mark Sedwill: UK visas, yes, the old operation; the old overseas operation.

Chair: So you had very direct experience of running a large administrative system in which there were lots of people washed through an administrative process, where problems would have been identified. So you knew—you have direct experience of understanding that process. Yet the quality assurance processes were not picking up that there were problems, and some people being thrown up by the system, who were legally, rightfully here but were having immigration problems even though they should not be having immigration problems.

Sir Mark Sedwill: That is correct. There were lots of other quality issues raised during my time there. I got the office to look this up; I think I had 58 or 60 reports by the Chief Inspector of Borders and Immigration, and there were 400-plus recommendations in those. None of those flagged this up either, so there was something in the system that just didn't bring this problem forward to any of the areas where there were checks and balances. I absolutely agree that a quality assurance system, which is multi-layered, should have identified it, but it didn't, and that is what we need to learn from the Williams review.

Q16 **Chair:** This is the same Department that is responsible for passports, and therefore for identity assurance. It is well known in that field, as you and I both know, because of our previous experience—I should explain that I worked with Sir Mark, to a small degree, when I was in the Home Office. We always knew there were groups of people who would find it hard to assure their identity and therefore sometimes that would be about assuring their rights to things. So it wasn't an unknown when the policy was framed. Was it perhaps the case that the focus on these immigration targets was so driving the policy of the Home Office that these nuances, which were pretty important, if you were affected, and these assurances were not kept in play?

Sir Mark Sedwill: Again, Wendy Williams will give us an independent view of that, Madam Chair. It is a possibility, obviously, but we did a great deal of work to try to identify what the impact would be, particularly on the communities that the measures were targeted at. In this case, as I say, it was an unintended consequence; this was not the focus of any of those immigration Acts, because these were people who were entitled to be here.

It should not have happened—I am not suggesting that it should have. All I am trying to do is explain one of the reasons why I think it happened, which is that the checks and balances did not reveal the problem.

Q17 **Chair:** But the check and balance is as simple as spotting one person appearing in the system who had every right to be in the country and accrue all the resulting rights, yet who was thrown up as an illegal migrant when the evidence clearly showed that they were not. One such case might have rung a little bell, and a few should have raised alarm bells that other people would potentially be caught, but you are telling me that it was just not noticed. It seems unbelievable that something as basic as that was not noticed.

Sir Mark Sedwill: I am just trying to explain to you what I understand about the situation. As I say, I think there are some underlying structural causes. You have just described what you would want the quality assurance process to achieve, but clearly it did not reveal this problem—it revealed lots of other problems, which we fixed, but not this one. Obviously I regret that, because it has had an effect on people's lives.

Q18 **Chair:** But it had an effect for a long time. All the while you were there, this was brewing.

Sir Mark Sedwill: That is right but, to be fair, it also had an effect for many years before I was there and for a period afterwards.

Q19 **Chair:** The immigration system in the Home Office has pretty much always been under-resourced and has had huge management issues. When I was there, we found that people could not write English, which is why the letters repeatedly had errors in them. Those basic management issues were there on your watch and were very well known, yet in the middle of everything else going on in the Home Office, it did not seem a priority to sort it out.

Sir Mark Sedwill: I don't think that is fair, Madam Chair. We made huge improvements to the immigration system in my time there. We did not fix every single problem, but we fixed many of the problems that were there. We inherited a system with massive backlogs, in which cases simply were not being dealt with at all, let alone well. We improved the quality assurance throughout, and we created special caseworking teams to do so. I do not claim to have fixed every problem, but we fixed an awful lot of them. *[Interruption.]*

Chair: I will bring in Layla Moran very quickly, but it will have to be a short question, because the Division bell is going.

Q20 **Layla Moran:** How much responsibility do you take for the culture under which all of that was operating? Surely if there had been the right culture, the right questions would have been asked by the right people.

Sir Mark Sedwill: I think we improved the culture while I was there, but obviously as head of that organisation I do take responsibility for the culture. I think we were trying to ask all the right questions. If you meet the caseworkers, they are people who often went the extra mile to do the compassionate thing, so I do not think that the underlying culture that affects the individuals who are doing the work is a problem—these are dedicated public servants. My own view, without yet having the proper benefit of the Williams study, is that this was fundamentally related to some of the underlying structural problems with the immigration system that we are continuing to face.

Layla Moran: Okay, that is good to know. You are on the record with that.

Chair: We are going to vote now. We will be back in 10 minutes or so.

Sitting suspended for a Division in the House.

On resuming—

Chair: Welcome back to the Public Accounts Committee. We were interrupted while talking to the head of the civil service about Windrush when he was at the Home Office. I think, Sir Mark, there was a degree of complacency in your answers. You were there in charge of the whole system for six years, and there were problems. We will wait to see what the report says, but certainly you should have been aware of them in the system, and we are disappointed that you weren't. But we will pick that up once the report is out, if not before.

I will now ask Lee Rowley to ask you some questions about the Emergency Services Network and DBS, two major projects on your watch that have left quite a challenge for your successors.

Q21 **Lee Rowley:** With regards to DBS and ESN, whose responsibility is the failure of those projects?

Sir Mark Sedwill: I would not characterise it that way. You know the accounting system: we have the SROs and, overall, as the accounting officer, during my time, I was responsible for them.

Q22 **Lee Rowley:** What personal responsibility do you accept for the projects?

Sir Mark Sedwill: As the accounting officer, I am responsible for all programmes within the—

Q23 **Lee Rowley:** I understand that, but I am asking about your personal responsibility—you were there, you had the documents, the briefings and presumably the PowerPoints, and yet the projects still failed.

Sir Mark Sedwill: I don't accept that characterisation—that they failed. These were ambitious programmes, and very challenging. They had a

series of challenges through their time. We had to take action to deal with that—that is the nature of the role—but I wouldn't describe them that way. But as the accounting officer, I am, or was, accountable for the performance of all the work in the Home Office at that time.

Q24 **Lee Rowley:** So the collective loss of more than £1 billion, the failure to deliver on time and the loss of a large part of the scope in one project are not failures?

Sir Mark Sedwill: I think you will have to be more specific, Mr Rowley, because I am not exactly sure—

Q25 **Lee Rowley:** You were there, and I wasn't, so hopefully you will remember the specificities.

Sir Mark Sedwill: You're just—well, which of the two projects—

Q26 **Lee Rowley:** I am asking a collective question about them both. I will get to—

Sir Mark Sedwill: Okay, it is two years since I have been there, but let me just deal with the DBS then. I know that you asked my successor about the original business case—there is a gap between the original 2012 business case and what was delivered of £300-and-something million. We reset that business case and the entire programme when I was there, in the summer of 2014, and the gap between that and the delivery was significantly less. So that is the kind of action I took as the accounting officer, because that programme, which I inherited, was off track and needed action taking. That is the responsibility that one takes.

Q27 **Lee Rowley:** And then it went off track again, on your watch.

Sir Mark Sedwill: Some elements were off track, but nothing was significant in that. Programmes of this complexity sometimes go on and off track. They are subject to events. In the earlier period of that time, we had a judgment in the Court of Appeal that we weren't expecting, which required us to reconfigure; we had to introduce the online upgrade to a tighter deadline set by Ministers; and there were some genuinely commercial problems with the handover between the two providers, some of which, as you will be aware, are subject to continuing dispute. Those kinds of issues arise, and the role of the programme director, the SRO, and ultimately the accounting officer is to try to address those problems in complex programmes of this kind.

Q28 **Lee Rowley:** But they weren't addressed; otherwise it wouldn't have ended up in the place it was.

Sir Mark Sedwill: I don't think, Mr Rowley, it is reasonable to suggest that any complex programme that does not absolutely stay on track the entire time is a failure; otherwise we would never deliver anything.

Q29 **Lee Rowley:** I wasn't asking you to stay on track the entire time; I was asking it to stay on track after the revisions that you put into it, after having already gone off track once.

Sir Mark Sedwill: It went seriously off track; we put the revisions in and—

Lee Rowley: Then it went off track again.

Sir Mark Sedwill: Not as seriously, and then it was revised again. That is what happens.

Q30 **Lee Rowley:** Is it all relative then? It is okay if the relativity of the going off track is slightly less than before.

Sir Mark Sedwill: You are trying to put words into my mouth. All I am telling you—

Q31 **Lee Rowley:** I am just trying to understand who is responsible for a £1 billion loss. You tell me. You were the person in charge—

Sir Mark Sedwill: It wasn't a £1 billion loss; that programme was not a £1 billion loss—

Q32 **Lee Rowley:** Collective loss across both of the projects—when I want to talk about an individual project, I will talk about one—was over £1 billion.

Sir Mark Sedwill: You are making an assertion. I don't recognise that number. You might be right, but I have not put those numbers together in my head—

Q33 **Lee Rowley:** If we do talk about DBS, then, do you accept that the timescales were over-ambitious?

Sir Mark Sedwill: At the beginning, yes.

Q34 **Lee Rowley:** And in your reset?

Sir Mark Sedwill: I think they became—again, I would have to go back over the detail of this. I think that the reset was a reasonable set of interventions to try to bring that programme in on time, but then there were some further problems that took it off track. I don't think that it was necessarily that the timescales were over-ambitious—they certainly were at the beginning.

Q35 **Lee Rowley:** Do you think that there was a lack of realism in the programme?

Sir Mark Sedwill: I think at the beginning there was—I think that is what the NAO Report says. The original business case was highly ambitious and, together with the creation at the same time of the new service—the DBS being created out of the previous two institutions—the institutional capabilities of the agency were overstretched.

Q36 **Lee Rowley:** And after the reset?

Sir Mark Sedwill: After the reset, the programme was much closer to trajectory throughout, but as I said, we had some further issues, including, in particular, that as the commercial provider changed from

Capita to TCS there were delays in that handover. That was partly because of capacity in those two organisations. That pushed the programme back.

Q37 **Lee Rowley:** I must just pick you up on this point about how it tracked closer to trajectory. The programme did not deliver; large parts of the scope were cut out—that is what your successor and the head of the DBS came to tell us a number of weeks ago. You cannot debate the trajectory being closer if you are not actually delivering the end product, which you didn't.

Sir Mark Sedwill: We changed the scope in the summer of 2014 as well, for exactly the same reasons.

Q38 **Lee Rowley:** My question was not about the summer of 2014; my question was about the subsequent part of it.

Sir Mark Sedwill: We took what we thought was a reasonable set of actions then. You have to make a judgment, and cannot predict exactly what the trajectory ahead is. We took the judgment then to make the changes to the scope and timing of the programme, we ran the procurement which brought TCS in to take over from Capita, there were some significant issues in the handover between those two, and there were some external changes including the judicial review. That forced us to continue to reconfigure the programme. That programme was run by its SRO and the DBS. We had all the usual scrutiny and gateways, and we made the judgments as we went.

Q39 **Lee Rowley:** So you think we had a governance issue in the Home Office between 2013 and 2017.

Sir Mark Sedwill: No, I am not suggesting that. These programmes do not always go entirely according to—

Q40 **Lee Rowley:** I am well aware of that. I used to be a programme director—

Sir Mark Sedwill: I know you did.

Lee Rowley: I completely understand. That is why I am quite keen to understand where the responsibility lies for a project going off track not once but several times, not delivering its scope, costing us a lot more money, still not delivering and still with no clarity about what we will get at the end stage—and we haven't even come on to ESN yet. It is a total mess. Somebody needs to own this.

Sir Mark Sedwill: In the end, as the accounting officer during that period, the ultimate responsibility is mine. But, as you know, you are running a very big and complex organisation and you are scrutinising programmes through their SROs. You have all the governance in place—you will be more familiar with that than me—and you make the best judgments you can make as you go along, as do the SROs and the programme directors. That is what we did through this programme.

Q41 **Chair:** You just said that we are more familiar with the governance than

you are. I know Mr Rowley is a formidable member of this Committee, but as the accounting officer at the time I would have thought you would be fairly au fait with—

Sir Mark Sedwill: Sorry, I am not talking about the specific programme; I was simply referring to Mr Rowley's expertise in the governance of programmes, as somebody who has got a background in this area.

Chair: There you go—you got a compliment from Sir Mark.

Q42 **Lee Rowley:** I am grateful for it.

Given we have both been involved in this, let's pretend we are in a lessons learned exercise. Where was the flaw: the judgment you exercised or the governance which gave you the information to exercise that judgment? It must be one of them.

Sir Mark Sedwill: I suppose I don't really know is the short answer to that. I would have to look back at exactly whether the judgments were reasonable on the basis of the information we had at the time. They always sought to be. They were certainly done very thoroughly on the basis of the information we had. I don't have anything to suggest we were not given the right information by that programme. There were judgments made and there were some subsequent problems which were not foreseen. I do not know whether it would be reasonable to suggest we could have foreseen them.

Q43 **Lee Rowley:** Perhaps you could ponder that and write to us.

Sir Mark Sedwill: I'd be happy to.

Q44 **Chair:** One area we picked up on was the idea that continuous checking would be very popular.

Sir Mark Sedwill: Yes.

Q45 **Chair:** But that required a lot of organisations that had systems in place—for instance, for three-yearly checks to see physical paper documents—to change their procedures and systems. Wasn't part of it that the design was not in tune with the reality of how organisations and individuals operated, and there wasn't really any attempt to change the processes to match the two? So you had one system going one way and the real system on the ground going a very different way.

Sir Mark Sedwill: I think a set of assumptions were made about the likelihood of digital take-up. The assumption was that because it was more convenient—it was online—

Q46 **Chair:** We know those assumptions were made. You don't need to repeat that bit. Who tested those assumptions? Did anyone say, "Oh, actually maybe this won't work"? Who made the real-world check?

Sir Mark Sedwill: Those assumptions are tested through the processes of the business cases by the programme team and the various gateway processes.

Q47 **Chair:** But those are the processes for delivering a programme. Surely one of the benefits of being the permanent secretary, and indeed of being a Minister, is that you see the real-world impact. You have got, if you like, that wider political—with a small "p"—view of how this will play out, what will happen if it goes wrong and what the impacts are out there in the world. It is a question not just of taking all the business cases through but of stepping back for a moment and seeing the big picture. Did you do that at any point with this project?

Sir Mark Sedwill: I don't recall stepping back and considering that digital take-up was going to be significantly less than the programme expected. I did not have any real evidence to suggest that was likely to be the case—certainly not that I recall. One is trying to make a judgment about these programmes dealing with the evidence that exists. As an accounting officer, you cannot just act on instinct and hunch; you have to act on the basis of the hard material you have. You challenge and scrutinise, but if the programme, through the gateway processes and all the rest of it, is able to bring to you that the answers to those questions are a reasonable judgment, you approve the programme to go ahead with whatever checks and balances are required.

Q48 **Lee Rowley:** I take your point about scrutinising the information and evidence base in front of you, but, to my recollection, the problem was that there was no evidence that DBS—the model put forward, with this transfer of assumption, from the employer asking for a check to the employee getting a check—would actually work. There was no evidence, because when we asked your successor and the chief executive, they told us no information had been pulled together to verify whether that was correct. You could not have had the evidence base in the first place.

Sir Mark Sedwill: As I say, that was several years ago, and I do not have all that information completely in my head.

Q49 **Lee Rowley:** You don't have it in your head because it was not collected—that is my point.

Sir Mark Sedwill: That may be right. As I say, I do not have all the detail you are asking me about in my head. There was a general drive towards digitising Government services throughout that period. This was part of that. There was a sound policy reason for moving the request for the DBS check, because people were finding it highly burdensome, as I recall, when moving between employers to keep having to get the same check time and again. There were certain sectors where that was a significant friction on individuals being able to be employed within a reasonable time— in particular in areas where people were working on low salaries. There was a good basis for shifting that at the time. Whether it would have been possible to generate in advance evidence of exactly how that would work, I do not know.

Lee Rowley: You could have done a user-demands assessment to work out what your customer base actually wanted.

Sir Mark Sedwill: The programme produced those assumptions about take-up on the basis of the evidence they had.

Q50 **Lee Rowley:** The Government should have assessed and identified that there was nothing underneath—there was no evidence to suggest that this model would work. Then we would not have lost £300 million trying it out and realising we only got a third of the user base that was expected.

Sir Mark Sedwill: That may be right, but let us not forget that there are lots of checks for these programmes, including gateway processes and all the rest of it. There is a whole range of governance. I am part of it, so I accept my responsibility in the end. But there is a whole range of checks and gateways and so on that you rely upon to tell you where to look and where the risks are, and you make the best judgment you can on the basis of that.

Q51 **Lee Rowley:** So an even more systematic failure than I thought.

Sir Mark Sedwill: I don't know for sure, because I have not audited the programme, but my point is that the kind of questions you are asking would have been reasonable questions not only for the programme to ask or for me to ask in an informal way as the accounting officer, but for the gateway reviews and the business case process to have identified as it went. If there are failures, as with most programmes if they go off track, multiple problems will have arisen—usually in combination.

Q52 **Lee Rowley:** I am slightly concerned by your choice of semantics. It is not "if there are failures"—there are failures. There is a large failure, with a large cheque associated with it. I am trying to understand the responsibility that should have applied to the period while you were in the Home Office. We are talking in a very theoretical manner about an actual loss of money. Who has the responsibility? Please don't tell me that, technically, you have it. I want somebody actually to have it. Or, we can talk more widely and systemically about how the civil service has no accountability for the delivery of these kinds of projects, which I am happy to do with you in your new role.

Sir Mark Sedwill: The civil service does have accountability of these projects, but I am not sure exactly what you are asking me to say. What I am telling you is that you are familiar with the roles of the individuals; you are familiar with the accountability. We reset the programme because the initial programme was too ambitious. That is where that £300 million-plus number that you are talking about comes from.

If I can answer with a rhetorical question, what else should I have done? What else should I have done in the summer of 2014 other than look at a programme that was over-ambitious and commission the action to reset it, in order still to deliver a significant Government policy? It turns out that there were later delivery problems, but I believe that was the right action to have taken, and the people who work for me and I took that action on the basis of the best judgments they had at the time.

Q53 **Lee Rowley:** And yet it went off track again. The question that I am not

clear on is about accountability. In the private sector, if I had lost £300 million on a project, or costs had increased by £300 million, I would not have a job. Why should civil servants still have a job?

Sir Mark Sedwill: That is a much broader question. Civil servants do not get rewarded like people do in the private sector.

Q54 **Lee Rowley:** So that's the answer, is it?

Sir Mark Sedwill: No. Stop trying to put words into my mouth.

Q55 **Lee Rowley:** I am not trying to put words into your mouth; I am trying to understand where the accountability is, and you are not giving me an answer.

Sir Mark Sedwill: You made the comparison with the private sector. The private sector structure of programme delivery is different to the public service structure of programme delivery, but we bring quite a lot of people in. This is not specifically in the case that you mention, but where we believe that a programme is off track or significantly off track, and that is down to failures of the management, or we need to make a change to the team, we make a change to the teams. In that sense, the accountability is the same, but it is not quite the same as in the private sector because of the different structure of the careers.

Q56 **Lee Rowley:** I still struggle with how we have lost, either by cost overruns, or the like, about a billion and a half pounds, and I can't find anybody who will take personal accountability for that. Do you think, as the head of the civil service, that we have the wrong people in the wrong jobs? Do we have a lot of very senior civil servants who are interested in policy and not at all interested in project management?

Sir Mark Sedwill: I think that probably would have been the case a decade or more ago. I think if you actually look at the shift in the senior civil service, there are many more people who have actually had experience of programme and project management. It is one of the areas that, under my predecessor, we focused on seeking to improve—as we did our commercial capability and others. So there are now permanent secretaries—which would never have been the case when I joined the civil service—who actually have a great deal of experience of programme and project management as part of their career.

Q57 **Lee Rowley:** So the Home Office between 2013 and 2017 was the exception rather than the rule.

Sir Mark Sedwill: Well, my background is not in programme and project management. I would not say every permanent secretary has that. I had run some significant programmes when I ran UK Visas, and, by the way, they delivered—and delivered on time and under budget. So I had some experience of programme and project management. It wasn't my specialisation, though.

Q58 **Lee Rowley:** The NAO previously said that the ESN timeline was very ambitious. Do you agree with that, in hindsight?

Sir Mark Sedwill: Yes.

Q59 **Lee Rowley:** How could you have made it less ambitious, as the accountable officer?

Sir Mark Sedwill: We could have had a longer implementation period earlier on in the programme. Certainly at the beginning of it, we would have then projected very significant additional costs because of the nature of the Airwave contract at the time, and the nature of the extensions. That was a significant factor in seeking to deliver this programme to the original deadline, so we were constantly trying to trade those costs and benefits and values off.

Q60 **Lee Rowley:** So we just got those additional costs later? It was just about loading them on afterwards.

Sir Mark Sedwill: No, we didn't, Mr Rowley, because—

Q61 **Lee Rowley:** We did. We put £1.1 billion costs on the Airwave contract, which has come subsequently, plus the £375 million which has been incurred by an additional project management cost.

Sir Mark Sedwill: Well, if you look back at the history of that programme, it was, I think, about 18 months before I left the Home Office—anyway, well into my time there—that we renegotiated with Motorola, who had taken on the Airwave contract, the on-costs beyond if there was a delay and the continuing provision of Airwave, and got significantly better commercial terms than would have been the case beforehand. When we started that programme, because of the structure of the PFI contract that Airwave had, Airwave would essentially, because at the end of the PFI contract they would have owned all of the infrastructure, have been in a position to charge us anything they wished. That was part of the original business case—to avoid those prohibitive charges. So that was the reason that there was that essentially hard stop in the original business case. We did actually reschedule it during my time, though—by nine months. Subsequently there was a software release that did not prove to be effective, and that was part of the reason my successor decided to reschedule the programme further. But the commercial arrangement changed in my time there because, as Motorola took on the PFI contract, we negotiated a better commercial arrangement.

Q62 **Lee Rowley:** Final question. I have read some of the transcripts of when you came here to talk about ESN. Do you accept in retrospect you were overly optimistic about what could be achieved in the timescales and the programme that had been set?

Sir Mark Sedwill: Yes.

Lee Rowley: Thank you.

Sir Amyas Morse: Just going back to ESN, you rightly say, Sir Mark, that the ESN project has been reset again—we have a Report coming out very shortly. There is a huge increase in cost and a substantial amount more time involved in it, sadly. I wonder if I can get the benefit of your

experience. Do you think one of the things that happens is that teams get so committed to projects that they get almost to the point that they really think if they just want it enough they can somehow make it work? I remember the ESN team being enormously enthusiastic about just about everything that they told us. I think they have probably changed now. I think they were selling a pretty big old bit of goods that they believed themselves. Do you think that that level of almost over-commitment—believing you can fly—is actually a hazard?

Sir Mark Sedwill: I think it can be. Many years ago, I was running UK Visas and Immigration when we were taking the biometric visas programme through the various Home Office checks. It was a big ministerial priority and we had a strong sense of conviction in the programme. You go into those investment committees determined to secure agreement, and you are of course straightforward and answer all the questions, but you have put a great deal of personal energy and commitment into a programme and you therefore want to push it through. That is partly what all the gateway checks and audits and so on are designed to try to flush out.

As I may have said last time I was here, I was always uneasy about the level of ambition and the pace of the ESN programme. I sought, as well as the formal scrutiny—the gateways, the Major Projects Authority and so on—a whole load of informal challenge sessions, because I just wanted to test it. However, the programme passed those. As the accounting officer, you cannot act without hard information, particularly if you are going to delay a programme and incur additional cost. We always knew that it was a high-risk programme, but as you and I have talked about privately, I think there is something quite significant in what you say.

Sir Amyas Morse: I am listening to what you are saying, and I know you are sincere. However, I think that the quality of financial information that you all used for these assessments was simply not good enough in many cases. There has to be an explanation for the extraordinary number of resets or failures—it does not matter what you call them; let's just call them things that involve a great deal of time extension and a lot of extra money. That is happening a startling amount. I accept that the skills in the civil service are going up, so there must be an explanation. Looking at the objective evidence of repeated problems, what do you think the answer to that is?

Sir Mark Sedwill: First, I hope it is improving. If you look at project and programme management skills across the civil service, they are significantly greater than they were before, and we have much more professional and commercial capability. Let me just register that point.

I think there is something about truth to power and about the aim to deliver to very ambitious timescales. This Committee has looked many times at universal credit, for example, which is a bigger version of what you might describe as the same phenomenon.

Sir Amyas Morse: Okay. "Truth to power" is probably your answer to the question. Thank you very much for that. I think we all know what that means.

Chair: It is interesting how open civil servants are being about these things currently.

We will now move on to issues around cyber-security, so Ms Alessandri and Mr Martin can speak up on this point. However, you do not all need to answer the question if you agree with the previous witness.

Q63 **Bridget Phillipson:** Sir Mark, starting more broadly, how confident are you that the strategy is helping the UK stay ahead of what is a growing and emerging cyber-threat?

Sir Mark Sedwill: The real expert is to my left. However, I think we should be confident. You always have to be a bit careful about international comparisons because the data is still developing. However, most other countries who face a similar kind of threat regard the UK as being at the cutting edge, so I think we are in pretty good shape.

Q64 **Bridget Phillipson:** But we are more exposed, in some ways, than other countries, aren't we?

Sir Mark Sedwill: We are, because we have one of the most open economies and of course one of the most digital economies. Levels of understanding are high here, so none of us is complacent for a moment, because this is a very fast-evolving threat. That is part of the nature of this portfolio of work. However, I think that, compared with most other advanced western economies, we are in reasonably good shape. Ciaran may give you a slightly harder-edged answer, if that is helpful.

Q65 **Bridget Phillipson:** Yes, and I am also keen to hear how well prepared you think the Government are.

Ciaran Martin: We are not complacent about any aspect of the threat. As you say, it is growing and evolving. We are making some specific interventions, which are helpfully included in the NAO Report, on changing the way the internet works. You asked how well prepared the Government are. For example, thanks to national cyber-security programme funding, more than 1.3 million public sector workers now have automatic blocking technology on their devices. That allows us to check more than 4 billion queries to the internet every week, and to block more than 1 million that are malicious. There are specific interventions like that that we can use.

Very briefly, because I am sure we can elaborate in further questioning, we are looking broadly at two types of threat: the big, strategic, malevolent state actor threats and ubiquitous, not terribly sophisticated, but high-volume cyber-crime. The sort of interventions that I just talked about aim to raise the bar on the latter.

Organisations up to and including the Government have to spend too much time dealing with high-volume, low-sophistication threats that too often get through in western economies. We are making structural

improvements on that, which then allows the experts in my organisation, the rest of GCHQ and the rest of the national security organisations to get after the very specific, top-end threats.

It is in classified space, but we measure the sort of aperture of the threat that we can see, so we can tell what accesses we have got and what threats we are capturing and what we are not. Across a range of indicators, we are making good progress.

Q66 **Bridget Phillipson:** Which would you regard as more important—the state actors, as you set out, or the impact that one might see on businesses or individuals? Or do you not view it in those terms?

Ciaran Martin: When I say both, I am not ducking the question. I will answer it very specifically. From the strategic national security point of view, it is the big state threat, which has the potential for large-scale espionage and the disruption of critical services. There is the potential, frankly, for national emergencies or, short of that, significant disruption.

For the longer-term economic health of the country, it is the latter. As Sir Mark said, we are one of the most heavily digitised economies in the world. I often use a local example from near where I live of a four-person hairdressing salon that had to write to all its customers and had to close for three days. While very difficult for that business, that is not a nationally significant incident. However, how many of those add up to a strategic structural threat to the economy? How many letters does every citizen have to get notifying them, under law, that their data has been breached before they start to wonder whether they will input their data and shop online and so forth. They are two different types of threat, and we need to treat both seriously.

Q67 **Bridget Phillipson:** More specifically, to take an example, how well prepared do you think the different and separate NHS bodies are? They have had difficulties in previous years. Have they responded?

Ciaran Martin: Yes, and colleagues in NHS Digital are doing a good job in raising the overall bar. As you know, and as I think is implicit in your question, the NHS is—parliamentarians know better than me—a confederation of lots of small bodies, so that sort of at-scale security that sometimes makes it easier to make improvements can be more difficult.

One lesson, not just from bodies like the NHS, but local government as well, is that, if you look at cyber-security in the UK Government and elsewhere in western economies five to 10 years ago, we were telling everybody that they needed levels of defences equivalent to, frankly, the Government or a major global bank. Of course, most people can neither afford nor have the skills to do that. There is a sufficient bar to be raised, including the basics of patching and so forth, where our role is educative. However, there are also automatic defences that we can make.

Basic vulnerabilities of the type that failed TalkTalk in 2014 are the sort of ubiquitous threats that are not sophisticated and should be defendable against. However, local authorities and NHS bodies, by and large, cannot

afford the commercial technology to scan for those sorts of vulnerabilities, so we built a free service—it does not compete with the market; it is very basic—that most NHS bodies and virtually all local authorities, including all in England, now use. It allows them to scan for those vulnerabilities, tells them what is wrong and shows them how to make those basic protections.

Since we started two years ago, for local government—I do not have the figures for the NHS; we could probably get them for you—we have fixed just short of 4,000 of those urgent findings. That is the sort of incremental, step-by-step approach that we are taking.

Q68 **Bridget Phillipson:** That all sounds very positive. My question for Sir Mark is, why didn't we seek to learn any lessons from the first national programme around cyber before moving on from that?

Sir Mark Sedwill: I think we did. The first programme was essentially fairly groundbreaking. We took evidence from that at the time, and then we did a reset as we went into the second phase of the national security capability review. I would not say that we did not learn any lessons from it.

Q69 **Bridget Phillipson:** But there wasn't a full lessons learned exercise, was there?

Madeleine Alessandri: There was a lessons learned exercise, which, looking back on it, could have been perhaps more robust than it was. But we learned a lot from that first programme, and what we learned was that we need to be more interventionist. I think there was an aim in the first programme to let market forces lead the way. When we reflected at the end of that programme, it was quite clear that was not going to get us to where we needed to be to stay ahead, as Ciaran has outlined, of a very complex landscape, with an evolving threat and of course evolving technology as well. So we needed to do something fundamentally different and groundbreaking.

What we sought and have been seeking to do is to put in place the capabilities and the structures that will enable the UK to continue to adapt and stay ahead of the threatened technology, as it evolves. So there was quite a lot of structural stuff that needed to be done right at the beginning. One of the highlights, of course, was the establishment of the National Cyber Security Centre. For the first time we had—I think that we were the first country in the world to have—a national technical authority on this, which brought together myriad other organisations that were not always communicating in the most effective way beforehand.

Q70 **Chair:** Mr Martin just talked about the new software. What else, practically, are you doing to ensure businesses and other organisations comply? You can produce what I think the industry sees as quite useful guidance, documents and White Papers, but how do you know that anyone is actually using them? How do you get that assurance?

Ciaran Martin: For example, under the European Union's network information security directive—the NIS directive on critical national

infrastructure, which encompasses about 600 bodies—we have issued guidance. We measure the uptake of that—250,000 downloads. It's hard to get comparators—

Q71 **Chair:** I see. So you measure by download?

Ciaran Martin: We measure in part by some downloads, we measure by industry engagement, we look at actions. There are breaches surveys, other surveys and so forth. There is something going back to the NAO's interim Report on the last programme in 2014 about the inherent difficulty of measuring how safe the UK is in cyber-space, so we are developing a range of metrics.

I am sure that we will come on to this, but the easiest place to develop those metrics is in our automated interventions and direct interventions—the stuff we built and the impact it can have. For example, what is the UK's share of hosting malicious websites in the world? We know that figure, and we can talk about that a little later, if you like.

Unlike Sir Mark and Ms Alessandri, I straddle both periods: I was in post at the end of the first period and throughout this programme. As I read the NAO Report, it accurately says there was no formal lessons learned exercise on the management of the programme, but I think that's different from what happened in 2015. Sir Mark alluded briefly to the national security capability reviews, but 2015, in policy terms, was not an evolution; it was a fundamental overhaul.

If I can characterise the objectives of the main strands of work of the first national cyber-security programme, there were two. They were developed through GCHQ: a state-of-the-art cyber-defence and detection system, using the full weight of the state's secret capabilities, and then also promoting information-sharing and awareness among business.

The first one was quite successful. I think the second one, which we looked seriously at, was less successful, and that's common across the west. So, as Ms Alessandri said, we moved to a much more interventionist approach—a single approach to incident management—and much more directed advice to business, and, frankly, much more direct interventions into the way the internet works, to promote its safer use.

Q72 **Layla Moran:** But Mr Martin, isn't one of the measures of this whether or not the amount of fraud is actually going up or down? You have got the numbers from UK Finance that said that unauthorised card fraud has actually gone up in 2018 compared with 2017. So, if that's happened, how can you say that it's working? What's going on?

Ciaran Martin: There are definitional issues about whether one terms it formally as cyber-security, so there are terms about card fraud—

Q73 **Layla Moran:** But their own assessment is that the majority of that card fraud is happening because of data breaches, which speaks directly to the kind of thing you are talking about.

Ciaran Martin: Yes, and there is a serious and sustained problem with transnational organised cyber-crime. Of course, a lot of that can be done globally; a lot of the data can be held globally. Most people—well, pretty much everybody in the UK—will have their data held by organisations domiciled in another jurisdiction.

Q74 **Layla Moran:** But we also saw some of this. BA was one of the ones that had an issue, so there are British companies. Surely the consumer has a right to know whether these companies are safe to give their details to, and that doesn't seem to be happening right now. Can you guarantee to consumers that when they give their details to reputable companies such as BA, it is safe?

Ciaran Martin: I can't give a guarantee on behalf of companies. What we can do is have a set of interventions that try to tackle the ecosystem of cyber-crime. We do work very closely with those companies and we worked very specifically with BA to identify the sorts of flaws that were evident in the breach that you refer to. We have done a number of interventions. For example, our promotion of two-factor authentication—you know the secondary verification in addition to a password—

Layla Moran: Oh, we know that very well.

Ciaran Martin: Of course you know it. It was in our advice following the attack in the summer of 2017. What it is designed to do is make those thefts of credentials and basic personal information less valuable on the open market, because if an organisation, on its web-facing services, has two-factor authentication, the use of a stolen bulk data set to force its way in through brute force log-ins does not work. If an organisation doesn't have it, it does. That is why we promote that sort of improvement.

Q75 **Layla Moran:** But currently, if you are a consumer and you go to one of these websites, you do not know whether the company is following best practice. This Committee, in terms of the banks, had recommended a league table so that we, as consumers, can make choices about who we give our data to—the new money is data—but that was rejected as an idea. Do you not think that consumers should know which companies are reputable—doing the bare minimum, as you described it—and which are not?

Chair: A kitemark is what I think of.

Layla Moran: A kitemark or something similar.

Ciaran Martin: There is some information out there. For example, the Cyber Essentials scheme, which has an uptake of tens of thousands of businesses, is the bare minimum. There is a policy in train under DCMS's leadership, with our support, on internet of things devices that is designed to help consumers differentiate on security grounds. Basically, the web economy that has existed for the past 20 years, which is based on the voluntary provision of personal data as the currency for a service, is a deeply flawed model for cyber-security reasons, as indeed it is for all sorts of other reasons, as we are learning.

The difference with internet of things security is that people by and large pay for it. There is a pilot under way. It is all in a DCMS report from last autumn on an internet of things code of practice. We are seeking to introduce, in effect, the equivalent of food packaging labels, so that for a particular product you can say it is red, amber or green. The green may cost a little bit more, but the security will be guaranteed and warrantied.

I actually agree with the fundamental premise of your question. It is just that we have inherited an internet economy globally that was not designed with security in mind and where it is incredibly hard for consumers to know—frankly, institutional investors struggle, as we have said before, to know how companies are managing cyber-risk.

Chair: It is like a bike lock system, but for—

Ciaran Martin: So I do agree with the thrust of it and we are just looking at the best way of intervening in that way.

Q76 **Bridget Phillipson:** I want to go back a step. Mr Martin, the point that you made was that things hadn't really moved on so much since the last strategy and that there wasn't a great deal to take from that because things had evolved. That is my understanding of the thrust of what you were saying.

Ciaran Martin: There was a big change in policy.

Q77 **Bridget Phillipson:** And Ms Alessandri, you said that there was some form of lessons learned exercise, but the NAO Report is very clear that there wasn't an evidence base generated, there wasn't a robust lessons learned exercise and there wasn't a programme closure business case, so there was no robust baseline for the next phase. Is that correct?

Madeleine Alessandri: As Ciaran Martin has said, there was a big policy shift around this. When you look back with hindsight, there probably was more that should have been done to understand the evidence base of the first national cyber-security programme, which is why in the current programme we are rigorously trying to learn as we go along. I am sure that we will talk about the evidence base further on. This is a really challenging area to get evidence on. Most industries, companies and boards are struggling to understand how you put a value on what you put into cyber-security, because how do you know what hasn't happened through you putting something in?

It is a really challenging area, and I am very grateful to the NAO for recognising that it is a hard area, but we are making improvements. We recognise that we have more to do, but as we bring this programme to an end—we have two more years to run of it, until 2021—we are committed to ensuring that we have a stronger evidence base as we go along, and we will do a very robust accumulated lessons learned as we pass through, to help us for the future.

Q78 **Bridget Phillipson:** But if you did not fully consider what happened last time—what worked and perhaps didn't work so well—how can you be

confident that what you are doing now is the right approach?

Madeleine Alessandri: I need to be fair to the people who were there at the time. They will have looked back, but there was not that evidence base, which is now there. As the NAO has said, there was not a robust—

Ciaran Martin: As I said earlier, although the NAO Report is absolutely right about the absence of a formal exercise, in terms of the policy consideration in 2015, there was a big push from about 2005 to 2015 across the west, including in the UK, to solve cyber-security through the promotion of voluntary information-sharing partnerships between different sectors of the economy. Looking at the evidence, as we did, in the 2015 period just after the election, we realised that more weight had been placed on that than it could bear. It was a useful contributory part. So we did look at the evidence and stop.

I am sure that, as Ms Alessandri has said, the process for doing that and its auditability and formality might have been different, but I don't think it is completely fair to say that they didn't have a hard look at the interventions they had been trying to make, at which of them had worked and which had failed, and switch accordingly. She is also right that we tried some new things for which, by definition, there were not yet metrics. There are now, and we will look to build on those.

Q79 **Bridget Phillipson:** So will that happen next time? Will there be a full exercise when this strategy runs its course, to understand?

Madeleine Alessandri: Yes, and we are already working on that. In a sense, you can't wait until it finishes at the end of the five-year period; we need to be doing it continuously now.

Q80 **Chair:** You say "continuously," but how will you then report that? Will we, as scrutineers of this, be able to see documents that come out of that continuous work? Will there be an end point? It is a simple process question.

Madeleine Alessandri: I believe that at the beginning of the strategy we committed to publishing a report on progress annually. There is an annual report that comes out of the National Cyber Security Centre, and we have been reporting about the programme in the SDSR report, which comes out on an annual basis. But we recognise that there is probably more we should do in terms of transparency here. There is a thirst for that, so we will commit to publishing an annual report on the programme, and the first one will, I hope, be out by the end of May this year.

Q81 **Chair:** So it will be annual from then on.

Madeleine Alessandri: Yes.

Q82 **Bridget Phillipson:** The total funding for the strategy is £1.9 billion, including £1.3 billion for the programme. How was that figure arrived at, Sir Mark? How do you know that that has been set at the right level?

Sir Mark Sedwill: It was an allocation done through the spending review. Essentially, you cannot be absolutely confident that it is the right level,

because we are always making a judgment, as with any spending decision, about the level of resources, the level of risk and the impact you are seeking to achieve.

It is a significant sum. It is a portfolio really; it has been allocated across a series of programmes, all of which have their own business cases. But in the end, of course, the judgment about the level of resource that Government devote to this and, as both my colleagues have been suggesting, the level of resource that the private sector independently devotes to it—essentially, our intervention is catalytic—can only come as we see what level of assurance we can provide.

Q83 **Bridget Phillipson:** So, on reflection, did you bid for the right level of funding?

Sir Mark Sedwill: It was before my time, but I think it was a reasonable bid to have made at the time, particularly given the uncertainty about this. Just to give you an example, part of the funding set up the National Cyber Security Centre. There was no model elsewhere in the world that we could just lift and shift, and say an x hundred million variant of this or an x times two hundred million variant of this looks like the right one. Because we have essentially been at the cutting edge of this, we have had to make judgments as we go.

Q84 **Bridget Phillipson:** As you have set out, it is a significant threat, and you would expect the level of funding to be commensurate with the risk we face as a country, but I am still not really clear how that figure was arrived at. Was it just that Ministers plucked it from the air?

Sir Mark Sedwill: Not quite from the air, but it was arrived at through the usual spending review process. Essentially, bids—

Q85 **Chair:** But that doesn't reassure us—

Ciaran Martin: I am the recipient of somewhere between 40% and 55% of the funding, depending on the year. At the time of the 2015 spending review, we made a bid as part of a wider confederation of public authorities that were eligible to do so. We put in evidence for that bid.

Roughly speaking, we have gone up from around £65 million in the first year of the programme to provisionally around £170 million next year. That was to sustain some of the temporary increases that we got from the last programme, to enhance the detection regime, to set up an incident management function that we didn't have, and then there was a bit—this was the bit where we had to take a lot of care—for the experimental innovation that I was talking about a little bit earlier. We did four strands of a bid in the normal way, DCMS did some on skills, and so on. That is how it was arrived at.

Sir Mark Sedwill: Of course, it is judged against all the other bids. You could ask the same question of, for example, the security service about the amount that they asked for to upgrade capabilities to deal with some of their national security threats. It is just the usual process by which the

bids come forward, and then there is a process of negotiation with the Treasury about the impact you expect to achieve.

Madeleine Alessandri: There was the SDSR and then the spending review, and then there were also internally quite a lot of scrutiny and challenge sessions, which were run by my predecessor in the role at the time. There was further scrutiny by the previous Cabinet Secretary across it as well. Because we were doing something quite new here, it was quite important that there was that challenge, and that challenge happened through those processes.

Q86 **Bridget Phillipson:** Evidently, it is a big sum of money, and we would want to make sure that it represents value for money, but value for money does not necessarily mean keeping that number at a low level. Mr Martin, the work you are doing is fantastic work, but it could be that you require additional levels of resourcing. Perhaps that number is too high, too low, or about the right level. We just don't really seem to know.

Sir Mark Sedwill: It is important, through this conversation, to keep in mind that there is the programme itself—or portfolio of programmes—where we are essentially engaged in direct delivery, and then the catalytic effect we are seeking to have on the wider economy. Most of the money spent in this country on cyber-security is going to be spent by the private sector, and it should be.

In a sense, that is the challenge with judging the exact value for money. You can do value for money, I think, on individual programmes against their business cases and so on, but the broader question of the impact on the economy and on the cyber-security environment is a hard one to judge. We will have to develop, essentially, assurance metrics—probably something related to the kinds of metrics that they use in insurance, or that actuaries use and so on—to make some of those judgments as we go along.

Ciaran Martin: May I add a supplementary observation? First, as I have just said, our budget from the programme goes up significantly over the years. While a lot of that, frankly, is sustaining the big data detection machine and some of the specialist skills required to keep it, on some of the newer and more innovative stuff there is, of course, the capacity to keep doing that. A further significant uplift might have been beyond our capacity to deliver, although it is inherently unknowable.

Secondly, the one thing I would say for the programme is that we got the broadly indicative set of numbers in the spending review in late 2015. The programme came out in late 2016. We are now going into the 2019-20 financial year, and in 22 years in the civil service I do not think I have had the stability of funding. It was an uplift and, as Ms Alessandri and Sir Mark have said, there are processes to make sure it has been spent and divided correctly, but in terms of the broad brush and being able to plan over a five-year period, I do not think I have had that sort of strategic funding stability before. It is very welcome indeed.

Madeleine Alessandri: I would add that because of the number of projects that we have across the programme, and because we were trying some new stuff out, we had to continually test what we were doing, learn what we were doing, and then adapt. That means there have been some projects that we started off and then stopped, because they were not hitting the indicators we expected and not having the impact we wanted. There were others—and active cyber defence is a really good example of this—where we piloted it and it was a lot more successful, so we were able to put more money into it. We are continually looking at our projects through that kind of optic: where we are having the most impact.

Q87 **Bridget Phillipson:** Sir Mark, why was the programme re-profiled in the first two years?

Sir Mark Sedwill: Sorry, which phase? Oh, the money that was moved into other areas?

Bridget Phillipson: Yes, into other activities.

Madeleine Alessandri: Shall I answer that? So £100 million was loaned to other national security priorities, counter-terrorism—this was 2016, and given what we saw in 2017 you can see how different priorities were weighing up, but it was a loan. We have already had 50% of that money back, and the remaining 50% I expect to get in the 2020-21 year. The other £69 million was money that was then put towards two projects, the Verify project and the Foxhound project, which I think we have touched on before, both of which sit within the aims of the national cyber-security programme, even though they were not initially envisaged as being part of it.

Q88 **Bridget Phillipson:** If cyber is such a big priority, how could you, in effect, afford to loan money to other areas of the Government in that time—and for some of it to not yet be returned?

Madeleine Alessandri: If we go back to the earlier part of the conversation about what we were trying to do here, this was something that had not been tried before. We were doing some innovative new work. Actually, the re-profiling to the later period gave us a chance to do some of that "test, learn, adapt" element. Now, for example, on active cyber defence, we can put more money into that, which is something that we could not do until we really knew how it was working. Re-profiling more towards the last two years has not been to the detriment of the programme, but Ciaran may have a view on that from a delivery point of view.

Q89 **Bridget Phillipson:** But if this is such a significant area—and we do not doubt that—which requires a significant increase in funding, as we have heard, how could you manage to reduce funding by a third for the first two years of the programme?

Sir Mark Sedwill: There is a question, which I think Mr Martin referred to earlier, about absorbative and institutional capacity, particularly when you are at that building stage. Do you want to add something to that?

Ciaran Martin: There is an element of, how far can you expand in a new area? I think the fact that it will be returned at the end of the programme, when we have built up the capability, is probably more useful to me personally and to my organisation.

There is another point—I am talking not about the counter-terrorism part, but about the Foxhound and Verify programmes. The Committee has done its own work on the troubles of Verify. Foxhound, at the moment, for those who do not know it, is essentially about secret desktops and mobiles for senior policy makers and Ministers. Both of those—Verify being the way that citizens authenticate themselves to Government services, and Foxhound because it is the way that senior policy makers can communicate securely—if you take a step back and look at the macro picture, I would say are cyber-security objectives, particularly Foxhound.

As the Government's chief cyber-security adviser, I was not content with the situation where members of the Cabinet, such as the Cabinet Secretary and so forth, did not have access safely to secure mobile technology that allowed them to talk in secret. Thanks to this programme, which is Cabinet Office-led and supported by our cryptographic experts, we are now getting there and rolling out the handsets. That is a very significant cyber-security delivery breakthrough for the Government.

Q90 **Chair:** Mr Martin, you are talking about the things that you are doing. I just want to ask, though, how you are sure that you are adding value to the market, because you would think that large private sector companies would have a strong interest in doing this work themselves. What are you doing that is seriously driving change in the private sector? You have described it for the public sector quite clearly, but what are you adding to the private sector?

Ciaran Martin: It is fundamental to our mission that we do only what the Government can do. Out of everything I have mentioned, the closest we have come to anything resembling a commercial function is that point I made in response to Ms Phillipson about small public-sector bodies.

When we looked at the effectiveness of cyber-security efforts in the Government to date in 2015, we found that, remarkably, despite the existence of a $100-billion-plus global cyber-security industry, there were things where there were what people would call market failure. We are targeting interventions where previously there were not any. We are trialling them in Government, but we are using proof of concept in Government, so the private sector can copy it.

The automatic blocking in Government that I mentioned can be rolled out to the private sector, and we are in discussions with the Internet Services Providers Association about whether that can be made the default for all consumers. Some major providers have already agreed to provide it for free for small businesses and charities, but can we step that up?

There is another intervention, which is, as I alluded to earlier, about the Government sponsoring the takedown of malicious websites. The

Government has access to datasets that the private sector does not have, and it can accumulate private sector datasets. If we give that to industry—we have done this to a small provider—they can ask hosts of those websites to take them down. It may surprise the Committee, but when you ask people, backed by authoritative Government information, to take down a website that is hosting malicious software, by and large they will. That is what has led to our share of malicious hosting to fall from—

Q91 **Chair:** So it is the power of the Government being the Government that says, "Don't do this"—

Ciaran Martin: It is more than that; it is using Government data, but it is also using Government techniques. There is no money in that commercial service. No one has an incentive to take down these websites. What we have done on the spoofing of Government brands is also replicable in the private sector.

All cyber-attacks involve the spoofing of identity of some sort. It is A communicating with B, and A is telling B to trust them, even though they shouldn't. That is why people get fake emails from HMRC and so forth. We piloted this with HMRC. At the time, in terms of brand spoofing across the world that we could see for ourselves and through our international partners and industry, HMRC was the 16th most spoofed brand in the world. We have been doing this for two and a half years. It is a very simple piece of code that tells the internet how to recognise a genuine email from HMRC. It is not fool-proof, but you have to work a lot harder to do it. As of February this year, on the same metric HMRC was the 146th most spoofed brand in the world.

We are collecting spoof emails. In the first full year, we collected half a billion spoof emails from people pretending to be HMRC that did not land in people's inboxes. That is an intervention. We have tested this with commercial providers, such as retailers. If the major supermarkets have their brand spoofed, they do not get punished by their customers, because their customers know it is not their fault. There is no market in anti-spoofing, so the Government have stepped in with a technical intervention. We have published the details of it, and that is the sort of intervention we are doing.

Q92 **Chair:** That is really interesting, because Mark Zuckerberg is talking about regulation of the internet at the moment. You have just given us an example of some of the interventions that the Government are making. What is the place of the state as a security and internet regulator? Perhaps that is more for Sir Mark. We have China and Russia playing it slightly differently from us. Is that the way we are going, Sir Mark?

Sir Mark Sedwill: No. Those are not the examples we would want to learn from.

Q93 **Chair:** I thought you might say that. From what Mr Martin has described, which sounds very sensible—

Sir Mark Sedwill: Just to draw together the point Mr Martin is making and then to answer yours, essentially you can expect the private sector to improve its own resilience. We can do things to enable them to do that, such as providing best practice, the kitemarking idea and so on, but that is only one part of it. You also have to go after the threats, and that is the point Mr Martin has just been referring to. That is something the state is best equipped to do, because there is not a market in that. The private sector cannot do that collectively, but we can. There is an opportunity in this, too, because we can make the UK a better and safer place to do business as part of the "trading safely" agenda, which is part of our economic offer.

In terms of cyber-space governance, you are absolutely right that it is a big international question. It is something that is being partly addressed through the UN, but inevitably countries such as those you have referred to have as much of a stake in that as we do. We are looking at coalitions of the willing, such as the OECD and some of the other countries that have similar systems to ours, to try to approach this. It is a very embryonic stage of internet governance more generally.

As you referred to yourself, this area has governance unlike the governance of other domains. The law of the sea 200 years ago is not a bad parallel. It is provided by some big private sector providers, so we have to work effectively with them. The really big providers are beginning to show more interest in this than they were hitherto.

Q94 **Chair:** Can I just ask a quick point on GDPR before I ask Ms Moran to come in? Obviously it is a European regulation. Is it in UK law yet? Forgive me, but in the many votes we have had, I have missed what we have actually done.

Sir Mark Sedwill: Yes, it is. Data adequacy is obviously a big question for us as we go through that.

Q95 **Chair:** Would there be an intention that UK law would change as EU law changed? Whatever happens in the next few weeks, there is an EU digital single market and, you could argue, a world digital single market in some ways.

Sir Mark Sedwill: We would obviously have to see as significant changes came through, but there is essentially a trading requirement for data adequacy for us to be able to continue to trade, as there is with any other jurisdiction. It is true for the United States dealing with the EU. There is a requirement to operate to either the same or common standards. This is bound to be an evolving picture. It makes sense for the EU, the US and other jurisdictions to be operating as far as possible to the highest standards.

Q96 **Chair:** It makes sense, but at the moment what makes sense does not always happen. I thought it was worth asking the question.

Sir Mark Sedwill: I'll leave you to make that comment.

Q97 **Layla Moran:** Sir Mark, how can we say that the current approach is

working if only one of the 12 strategic outcomes will actually be met by 2021?

Sir Mark Sedwill: That is a question about deadline and delivery. I do not think it is—

Q98 **Layla Moran:** Are you comfortable with only one in 12 being met by this point?

Madeleine Alessandri: If I can just clarify the difference between the National Cyber Security Strategy, which set out its objectives there, and the programme. The programme was never intended to deliver on its own the totality of what we are trying to achieve in the strategy, because the programme money was trying to have a catalytic, transformative impact, but there will be other money spent in Departments as part of their business-as-usual baseline, which will also contribute to the work of the strategy.

In terms of programme and programme deliverability, as the NAO reported, of the 12 strands, three have all their projects totally on track, a further eight have more than 80% of their projects within those strands on track, and there is just one area where less than 80% are on track. If you look at whether we will be delivering the programme objectives for this portfolio of projects, only one strand is below 80%. It is not significantly below it. It was 73% at the end of last quarter. I asked for the figures for this quarter, but the team said to me, quite understandably, "We are still getting in the returns, because it has only just finished," but we are seeing that trending up, closer to 80% than 70%.

Q99 **Layla Moran:** I hear what you are saying about programme versus strategy, but how much of the strategy is the programme meant to be effecting? If you set yourself a deadline of 2021 and then you are quite blasé about the deadline, what is the point in setting the deadline at all?

Madeleine Alessandri: If I may, I do not think that we are being blasé at all. Cyber-security is a tier 1 priority for Government.

Layla Moran: I am just asking what is going on.

Madeleine Alessandri: There is a difference between the programme and the deliverability of the programme projects, and the achievement of the overarching National Cyber Security Strategy aims.

Layla Moran: Yes, but you have the date on that document.

Madeleine Alessandri: Yes, but it also says in there—on page 69, I think—that the strategy never anticipated that it would be able to meet all of those very ambitious and broad outcomes by 2021. That is stated in the strategy itself. Of course we are seeking to do that and achieve that.

Q100 **Layla Moran:** I am just trying to understand your mind-set here. When it was written, how many of the 12 did you hope that you might be able to achieve by 2021?

Madeleine Alessandri: I was not in my role at that time, but I imagine that my predecessors hoped to achieve all of them by 2021.

Q101 **Layla Moran:** What is your assessment, now that you are in the job, on the ground and in the driving seat? Why has only one been achieved?

Madeleine Alessandri: The difficulty is that the measures, as they are reported by the NAO, are measures of our confidence in the evidence that we have. They are not a recording of the actual deliverability of the different strands; they are the confidence that we have in the evidence.

That takes us back to the earlier part of our conversation. It is really challenging, in some of this space, particularly when we are doing some new, innovative work, to get the evidence base that we would like. We are working hard to try to improve that. We are bringing in academia and industry to see how we might improve that. The red is around the confidence that we have in our evidence base, as opposed to the confidence in delivery.

Q102 **Chair:** Can we ask the National Audit Office, just to clarify for their report?

Tom McDonald: Just to clarify what the National Cyber Security Strategy document says about 2021, two of the strategic outcomes—secure by design, and science and technology—have specific objectives that should be met by 2021. The rest are open ended.

Q103 **Layla Moran:** Okay. Thank you. On the evidence base, what is your assessment of why it is so low in so many cases?

Madeleine Alessandri: Some things are easier to measure than others. Incident response, which is showing very green, is much easier to put a number to. We have a whole range of different metrics, some of which are qualitative and some of which are quantitative. Because this is quite innovative in many areas, it is quite hard to measure. If you take, for example, a lot of the work that we have been doing on training and interventions in schools, we are seeking to improve the skills pipeline that we have in cyber-security, but it is going to take a number of years for us to really understand whether the investment we are making in those educational establishments and those young people actually converts into people who take careers in cyber-security. That is why some of this is quite hard and quite long-term.

Q104 **Layla Moran:** Understood, but in the end, Sir Mark, you are the account-holder, so how do you decide where the priority of the funding goes?

Sir Mark Sedwill: Again, we just have to make a judgment in this area. It is a portfolio approach; it is designed to catalyse wider action.

Q105 **Layla Moran:** How confident are you that you are making the right calls, though, if you have not got the right evidence in front of you? If it is so innovative, it is good, but how do you know you are making the right calls?

Sir Mark Sedwill: Part of that is being able to make the kind of adjustments that we have made already, as we identify what appears to be working. We will obviously look internationally to see if there are different techniques being tried elsewhere that we can adopt. But in general—again, just to take a step back and draw an analogy—we have got to be careful not just to aim at the things that we can measure, because you can measure response. It is always harder, particularly in the short term, to measure the effect of preventive action, whether in this area or elsewhere.

However, I think we are all confident in the judgment—I think the NAO Report bears this out—that increasing resilience is the right direction to go, but a lot of that, of course, is increasing resilience by getting the private sector and citizens to increase their own resilience.

Chair: Mr McDonald?

Tom McDonald: There is just one observation that I think we would make from the series of Reports that we have done and that the Committee has taken. Some of the things that are being funded now under the second cyber-security programme are genuinely new and innovative, and are very difficult to measure. Some are not, and they are continuations of things that the previous cyber-security programme was funding.

If you look down the list, you see there is "Understanding the threat", "Cyber-Crime", "Keeping Government Resilience", "Protecting Critical National Infrastructure"—lots of these things did not start in 2016. I think it speaks also to how the allocations were made, and knowing what your evidence base is. What I am trying to say, I suppose, is that the world did not start in 2016 and why we made the criticism of the lack of an evidence base is that, yes, some of this was new but some of it was not. There should have been more evidence available at that point.

Q106 **Layla Moran:** Which brings me to my point. Ms Alessandri, why did it take until nearly halfway through the current programme to put in place a programme-level performance framework to measure the progress?

Madeleine Alessandri: The decision was taken at the beginning of the programme to have it on a devolved basis, so the money was moved out to Departments and they were responsible for the evaluation.

It was realised in 2017, through the national security capability review, that actually we needed to have a much better handle and grip of this in the centre, so that is why we brought it in. We have set up a performance framework and we are working to plug the gaps that we have got in the evidence base, and I fully accept what our NAO colleague says around that evidence base.

That is why it is so important now that we look ahead and we collect evidence as we go along, and we learn the lessons as we go along, so that as we go into the next spending review and we look at which of the projects and the work that we have done should now be sustainable in

Departments as part of a bottom line going forward, and what do we need to continue and to continue to have a transformative—

Q107 **Layla Moran:** Are we going to get updates, Sir Mark?

Sir Mark Sedwill: Certainly we will give you updates. I suppose that the only point of caution that I just want to add is that because this is evolving so fast, we have got to be forward looking and not backward looking. We obviously need to do whatever we can to build the evidence, including the evidence from comparators and benchmarks overseas.

However, if we had relied on the evidence, we would not have invented the National Cyber Security Centre. That was essentially a judgment call, that it was the right approach to take. There was not really a parallel elsewhere whereby we could say, "The creation of a body of this kind, bridging the secret world of GCHQ and the open world", which had not been done before, was necessarily going to achieve the effect that we wanted.

So a judgment was made and we will have to continue to do that as we move ahead, given the pace at which the threat is evolving. We will collect all the evidence we possibly can, but we will still just have to make policy judgments about where the priorities should lie, and some of that will have a lot of evidence and some of it will not.

Q108 **Layla Moran:** We will move on to the NCSC. Mr Martin, why were the running costs so much higher than were made in the business case?

Ciaran Martin: Partly it was the significant uplift that we had. Because of the hybrid nature of the organisation that Sir Mark has just referred to, building a capability that can operate out of a commercial centre within the Government security zone that is both an outward-facing capacity that allowed us to do 1,500 engagements with critical companies in the open within the last six months while at the same time having 77 highly classified desks in a secure facility, was quite a challenge. That is why we went back to the programme once we had worked out the full costs of that and we set it up accordingly.

Q109 **Layla Moran:** On 2021, let us draw a line moving forward. Sir Mark, how do you intend to make sure that the next phase is more evidence-based and more prioritised than the last phase?

Sir Mark Sedwill: Unlike at the beginning of this programme, we will have, for the reasons we have set out, a better understanding of the picture. I would expect that we will put together essentially a portfolio business case rather than just business cases for the individual programmes and projects within it in the way that, as the NAO points out, was not done at the beginning of this programme. It was essentially an allocative programme, or an allocative portfolio, as opposed to a single delivery programme. I think we will be in better shape to do that, and we would expect to draw on the evidence and look at examples from elsewhere as other countries start to move into the same territory, and put together a portfolio business case on that basis.

Q110 **Layla Moran:** How much of that forward thinking is already playing into what you are going to do next time? We know that the Army, for example, has in-house think-tanks that think 50 years ahead. Do you use them? Do you use others? How do you do that?

Madeleine Alessandri: We are using industry and academia. We have already started a series of workshops. There is a lot of work and thinking going on to try and bring the whole community together to make sure that what we put together for post-2021 is as robust and fit for purpose as we can make it and can enable us to continue to evolve. Success in a way is that we are agile as a country. Technology is going to take further leaps forward. The threat will continue to evolve, potentially in ways that we cannot foresee sitting here today in 2019.

Q111 **Layla Moran:** So what are the key elements to making sure we are agile?

Madeleine Alessandri: We have got to have the right structures in place, the right mechanisms—

Q112 **Layla Moran:** What specifically will be different in 2021 onwards that you have learnt about keeping agile?

Sir Mark Sedwill: We have been pretty agile so far in creating a whole new institution that has had the impact of the NCSC and some of the other changes that we have made to the programme as we have gone along. The big challenge for the Government—it partly goes back to some of the earlier conversation—is being able to do that on a faster cycle. We are still maintaining the disciplines of programmes, business cases, gateways and so on. We are doing that on a faster cycle as the opportunities and the nature of the internet change, but also as some of the threats evolve, and it is traditionally something the Government is capable of doing. There are some big shifts here in governance more generally. This is probably not for this hearing, but you mentioned some other areas such as disclosure and liability law, which will have to change as well over the next few years, so this will cut across the whole of Government and beyond.

Ciaran Martin: So, all that, but if I can offer one point where I think it will be really important: the ability to identify as far as possible technological trends and bake in security accordingly. The big strategic mistake that the whole west made in the last 20 years was not really understanding the security requirements of evolving technology. I have already given you the example of the internet of things and how we are trying to pre-empt that. We are trying to do the same on quantum computing and artificial intelligence and all the buzzwords that you hear. We now know that we need to have capability within Government, partly in my organisation and partly elsewhere, that properly understands technology and the emerging security requirements thereof, because we all across the west missed a trick in that 20 years ago, and we are paying for it.

Layla Moran: Sir Mark, you have the spending review coming up at some point. How are you approaching it?

Q113 **Chair:** When will we have the spending review, Sir Mark?

Sir Mark Sedwill: I think you will have to ask the Chancellor.

Q114 **Chair:** Everyone says to ask someone else, but you are quite important in the firmament. When would you like it to be?

Sir Mark Sedwill: The plan is for it to be this year.

Q115 **Chair:** In the next eight months, then. Realistically, you head up the Government. Lots of Departments are hitting deadlines for organisations that they subsequently have to fund. There are very clear deadlines for schools. We had Jonathan Slater in the other day from Education. Is there a challenging cut-off point that you are putting to the Chancellor? It is not sacred advice. It is probably pretty blindingly obvious, but what is the key cut-off?

Sir Mark Sedwill: We will need in any event, no matter what happens, to have a spending settlement for the next financial year, because the current one expires this year. The aim would be to have all those things decided and announced by the autumn Budget, so we will need to work back from that.

Q116 **Chair:** If work is not already happening now, we—

Sir Mark Sedwill: There is a great deal of preparatory work being done.

Q117 **Chair:** What if for any reason the spending review could not happen? Obviously we are in uncertain times now. We are not suggesting that you will be able to tell us that; you do not know any more than we do what is going to happen this week or the next. However, if there were a problem, would there be a roll-over of the existing settlement for another year? That is something that we have heard a bit.

Sir Mark Sedwill: That is yet to be decided, but obviously that would be one of the options were that the case.

Q118 **Chair:** When would the cut-off point for a decision be?

Sir Mark Sedwill: Again, I think the autumn Budget would be the natural moment at which that would be announced.

Chair: Announced—so there might have to be a decision a bit before that. Okay—we can work out the winding back. We will go and do our maths.

Q119 **Layla Moran:** To the vision that you would like to push forward for this in the 2021-onwards settlement, what would you like to see emerge from it?

Sir Mark Sedwill: Essentially, if we look at all national security threats, from those that face individuals and businesses right up to those that face the nation as a whole, it really boils down to three things.

First, we want to continue to improve resilience. That means the resilience of individuals, businesses and the country as a whole. There needs to be that component to it, and a lot of that lies elsewhere, with the private sector and so on. We need to keep that process driven and catalysed by NCSC and the Government.

Secondly, we need to keep building our capability to go after the threats. The threats will evolve. Something that we have not talked about very much today is that some of those threats essentially cross the boundary between the state and the non-state. You have criminal networks that are essentially being used by state entities, and you have criminal networks that are also able to deploy state resources on their behalf. That line is much more blurred now than it was in the past. We really have to keep building our capabilities to go after those threats. It is not just cyber-capabilities but other capabilities as well to deter those states from carrying out that kind of activity.

Third—this is really important, particularly as we go through Brexit and we have to think about our overall economic model—is making sure that part of the UK offer to investors and business is that this is the best place in the world to do business in a way that is cyber-safe. If we can get all those things right and build the programmes—again, it is about catalysing; it has to be a much broader effort—I think we would be in pretty good shape.

Q120 **Layla Moran:** Would regulation in your view play a part in that?

Sir Mark Sedwill: All the policy tools, including regulation and international agreements on standards, etc., need to be brought to bear.

Layla Moran: Mr Martin is nodding avidly.

Ciaran Martin: I agree on regulation as part of the toolkit. In terms of the one thing that I would like—to get a little bit insular about cyber-security—I mentioned the two big types of threat: the everyday, ubiquitous, low-sophistication attack and the big, nation state strategic threat. I think the end state that we would like to be in at the end of the next five-year period is that the country is equipped to combat the criminal threat—the low-level but high-volume threat—much better.

Then the experts can get on with the really serious threats from other states, because there are some very bad actors out there that are highly capable, and you need to contest them one on one. We need to take away much of the, frankly, rubbish attacks that should not get through in a well-defended economy.

Q121 **Layla Moran:** Should we not be certifying organisations so that we can just cut through that?

Ciaran Martin: We are.

Q122 **Layla Moran:** But mandatorily—because at the moment it is not everyone.

Ciaran Martin: There is a role for regulation. It depends on whether you are talking about a critical sector in terms of the potential for disruption. One model that I like, as we have said before, is—in contrast to the model in some other countries where they just specify a long list of organisations and say, "You're significant and you must do this, this and this," which tends not to work because it is very hard to draw up the right list and it

dates rather quickly—the model that the Bank of England has adopted in respect of its statutory mandate to promote financial stability.

It has interpreted cyber-security as an essential part of financial stability. That seems to me correct. It asked us for expert advice as to what technical standards should be built into cyber-security regulation by the Bank in its wider framework. Then it can assess—because I do not understand how the financial system works; that is what it does—what is workable within the business model of global financial institutions. I would like to see something like that more widespread in other sectors, so that we can promote cyber-security and cyber-stability in a way that works for the businesses that—

Q123 **Layla Moran:** Is there work being done for SMEs?

Ciaran Martin: There is. We published a guide last year—one of the first in the world specifically for SMEs—in the Budget. There is something here about the sort of risk. We are not asking SMEs to be able to take on the Russians on a good day. In fact, there are cases in which SMEs have been hit by the most malevolent state actors; for obvious reasons, I will not go into any of the details. That is not the expectation of the Government. If we track that one of the most sophisticated state actors is targeting an SME, for whatever political reason, the Government will go in directly to help. That is the proper balance of risks. We are not there to protect them on a case-by-case basis from routine cyber-crime.

Sir Mark Sedwill: One additional point I would make is that a lot of SMEs are in the supply chains of much bigger businesses. Through our interaction with big businesses, we encourage them to ensure that cyber-security is cascaded throughout their own supply chains. One vulnerability is that someone could go after one SME and, if they get it right, work their way into generally strategic players, given how connected supply chains tend to be now, in terms of their IT systems. They need to take responsibility for encouraging their supply chains to get their basic cyber-security right. That does not mean that SMEs need the same kind of elaborate defences that a big company in the defence sector would require, but it means that they need to get some of that basic hygiene right.

Q124 **Layla Moran:** Is there a country that does this better than us? Who are we learning from?

Sir Mark Sedwill: We do not think so.

Ciaran Martin: The international metrics are hard—

Chair: Everyone can have a go.

Ciaran Martin: Is there a reliable international index that I trust? I would say no. I say that with some amusement, because the International Telecommunication Union does an annual survey, and we were No. 10 last year. If you had asked me a month ago, I would have said that we do not think that that is particularly definitive. I will say the same again, even

though we were ranked No. 1 in its 2019 survey, published last week. There are all sorts of issues. It is a worthy effort, but the metrics are hard, so it is hard to do it.

Q125 **Chair:** No one is going to tell everyone what they are doing, are they?

Ciaran Martin: No. Western Governments including Canada and Australia have followed our model, and some of the Nordic countries are looking at doing the same. We get a lot international interest, both in visiting and finding out how the model works but also in engaging. That is from across the continent, north America and beyond. There are certainly very good examples.

Q126 **Chair:** So you are sharing best practice with safe and trusted allies?

Ciaran Martin: Absolutely. Let us take a country that we have a very good relationship with: the Canadians. I would say that there is nobody better in the world at protecting Government networks than the Canadians, but my Canadian opposite number would say that they have some way to go, in terms of engaging with critical infrastructure. We have a very productive dialogue as the closest of allies.

Q127 **Chair:** That's heartening to hear. We talked a bit about the security side and the regulation side. For the Government to have a role in both is sort of okay within the UK, but of course it is a global network. How would it work globally? Will there not be weak spots at every point when we interact, or when anybody interacts with another country?

Ciaran Martin: Yes. There are three ways of looking at that. There is the part of it that you can do something about. We encourage, and mandate where possible, major transnational companies to adopt what we call segmented networks, rather than flat networks. Sorry for the technicality, but if you look at one of the most significant global compromises of recent times, we have been able to trace initial attacks in Japan all the way through to the UK and other countries because there was no segmentation; once you were in in Japan, you were in wherever you wanted to be. UK entities can do something about that, in terms of the way that they segment, so we promote that sort of best practice.

The second thing we can do is make UK infrastructure less attractive, as I was talking about, in terms of reducing the malicious hosting in the UK, which makes us a less attractive target. The third thing we can do is to publish evidence of the interventions that work in the hope that other countries will do them. If the up-front research and development costs fall to the UK but we end up with a global improvement among likeminded countries, that is great.

However, there is an element in which you are right, Chair. We are defending in an international environment. We cannot cauterise ourselves from the possibility of damage from other countries, but it can be mitigated by using those three strands that I just mentioned.

Q128 **Chair:** Sir Mark, a bit closer to home than the whole world—Europe. There are obviously cyber-criminals outside the EU, but there has been a big

increase of cyber-attacks from Romania. Where are we at, and where will we be, on our relationships with Europol, the European arrest warrant and all those mechanisms we have relied on over all these years to help to protect us, and on working with our European colleagues and allies as of now and after Brexit, if it happens?

Sir Mark Sedwill: On the presumption that we leave, it of course depends on whether we leave with an agreement. If we do not, those measures will be severed, as I set out recently in another Committee, with a significant impact, which we would then seek to mitigate. There are some mitigations, but they would not be fully effective, because those measures, as you know, are now very efficient and effective. For example, based on the European arrest warrant and the volume of extraditions—essentially, in old money—that we are able to do quickly, compared with the previous arrangements, it is certainly an order of magnitude greater, and probably two.

Q129 **Chair:** So it would really open up a big weakness in the UK.

Sir Mark Sedwill: We would have to find ways of mitigating it. Obviously, if we leave with an agreement, then this is all part of the agreement that we have reached. Some areas are yet to be locked down, partly because those are areas in which the EU does not yet have the legal instruments to extend the capabilities that we currently enjoy to third countries.

Q130 **Chair:** How long will that take, and can you give us an example?

Sir Mark Sedwill: We would expect to be able to agree that during the implementation period. Obviously, it is a negotiation, but there is a strong intent on both sides to maintain that.

Q131 **Chair:** Can you give us an idea of which areas those are?

Sir Mark Sedwill: If you look at domestic security, there are some areas where the arrangements already exist—Europol would be an example—to give third countries access to that capability. We would want to work with them to ensure that the operational effectiveness of that access is as good as the current arrangements, or is as close as we can get to it. The legal framework to permit that already exists. There are other areas, including some of the data areas, where there is no current EU legal framework.

Q132 **Chair:** Can you give us an example?

Sir Mark Sedwill: I think SIS II would be the example for which there is no current legal framework to allow a non-Schengen, non-EU country the kind of access we have now. We have said that we would like to ensure that that is available to us. We will have it for the implementation period, but we want it available to us at the end of that period. Trying to secure that will be part of the next phase of the negotiation.

Q133 **Chair:** If we do not have a deal, it will be a very big challenge.

Sir Mark Sedwill: This will be one of the areas that, however hard we seek to mitigate it, there will be a no-deal impact.

Q134 **Chair:** You are not supposed to tell us about advice you have given to Ministers, but I imagine you have advised all members of the Cabinet of this challenge.

Sir Mark Sedwill: I always ensure that the Cabinet has the information that it needs to make the decisions that it makes.

Chair: Which I take as a yes.

Thank you very much indeed for your time. The uncorrected transcript of the session will be on the website in the next couple of days. We will produce a report on the cyber-security elements of this at some point after Easter, but that seems like a long time, particularly in your shoes, Sir Mark. Thank you very much indeed. We will work with our sister Committees, the Intelligence and Security Committee and the Home Affairs Committee, and keep a close eye on how you help to keep our country safe. Thank you for your work.

Sir Mark Sedwill: Thank you.