

Joint Committee on the National Security Strategy

Oral evidence: Ransomware

Wednesday 15 November 2023

3 pm

[Watch the meeting](#)

Members present: Margaret Beckett MP (Chair); Lord Butler of Brockwell; Baroness Crawley; Lord Dannatt; Baroness Fall; Stephen McPartland MP; Lord Reid of Cardowan; Lord Sarfraz; Lord Snape; Viscount Stansgate; Bob Stewart MP.

Evidence Session No. 5

Heard in Public

Questions 67 - 85

Witnesses

I: Rt Hon Oliver Dowden MP, Deputy Prime Minister and Chancellor of the Duchy of Lancaster, Cabinet Office; Rt Hon Tom Tugendhat MP, Minister for Security, Home Office; Lindy Cameron, Chief Executive Officer, National Cyber Security Centre.

Examination of witnesses

Oliver Dowden MP, Tom Tugendhat MP and Lindy Cameron.

Q67 The Chair: Good afternoon. Can I say, right at the outset, that we are pleased that the Government have now published the review of the Computer Misuse Act 1990 and the consultation responses, and the NCSC's annual review? It would have been helpful if we could have had some notification of them being published. It would have been even more helpful if they could have come earlier, but I understand that that might not have been wholly within your control. We are grateful to have received them now.

Lindy, you are quoted throughout the NCSC review—as you are, Mr Dowden—so, again, it would have been really helpful to have had them beforehand, and I apologise if it means we miss anything out that we should not. I am sorry that this session has been a bit difficult to arrange, but we very much appreciate seeing you now. Thank you very much for coming.

We are told that the UK is one of the most targeted countries in the world for ransomware attacks. Why do you think that is?

Tom Tugendhat: There is a very simple reason: the English language. Then there is a more prosaic reason, which is, I am afraid, our open banking systems. The combination of the two means that the UK is particularly targeted by those who are able to communicate with us and who can see that they can quickly move any ransoms taken into different banking systems and outside the jurisdiction of the United Kingdom.

Our banking system is open for a good reason: it supports a very free economy, which is extremely important for the prosperity of the United Kingdom, but this is where the co-operation between tech companies, the Government, and indeed Governments around the world, is so important in helping to support both the openness of the economy and the protection that is required to make sure that such openness does not become a vulnerability. That is why I am afraid it is true that we are particularly exposed, but it is also true that, alongside others, we are leading in ransomware defence.

Q68 Stephen McPartland: The NCSC annual review states that we are facing an enduring and significant threat for our critical sectors, and we need to accelerate work to keep pace with this changing threat. Are you able to confirm that, as a result, the ransomware threat to the UK is continuing to increase?

Lindy Cameron: It certainly continues to be one of our biggest challenges. It is the biggest threat to UK business in general, because, as the Minister has highlighted, criminals basically want to make money, so they target businesses where they think they can do so, or sectors where they think that applying pressure and hijacking data will force the payment of a ransom. So yes, we continue to think that ransomware is probably the most significant criminal cyber threat to the UK.

Stephen McPartland: We understand that a lot of the ransomware attacks have been attributed to Russian-speaking cybercriminals, and the NCSC has seen a new class of Russian cyber adversary emerge. You said that finance is one of the biggest drivers. Can you explain to the committee how these groups are ideologically driven, more than financially driven?

Lindy Cameron: That is right. Finance is one of the biggest drivers for criminals, but we are also obviously alive to a number of state actors who are interested in, frankly, espionage or pre-positioning themselves for potential disruption. In the last year we have seen, and call out in our annual report, a new class of state-aligned adversaries who are sympathetic to the ideology of states, in particular Russia, and may be acting without direct state direction but in sympathy with that ideology rather than purely for financial gain.

Q69 Baroness Fall: I want to turn to Russia in particular. The NCSC annual review also refers to Russia as one of the most prolific actors in cyberspace. On what measure of intelligence is it, and has it got worse

since the Ukraine invasion?

Tom Tugendhat: I do not want to be too categorical on changes, for very obvious reasons: because the nature of the changes demonstrates our awareness of certain threats. It is certainly true that Russian activity has been a significant driver of ransomware threats in the United Kingdom. It is also true that the Ukrainian conflict has, in different ways, occupied a lot of Russian cyber activity time. Without going into too many details, it has occupied some of their capability and capacity. That said, it is quite clear that connections between Russian activity and ransomware in the UK, or ransomware attacks in the UK, are an area of ongoing and continued concern.

Lindy Cameron: We have not seen the Russia-Ukraine conflict increase the ransomware threat from Russia to the UK, partly because the activity we have seen in the Russia-Ukraine conflict has been very focused on Ukraine, perhaps more so than we expected—and, of course, that is a state-on-state conflict. So we have not seen a specific increase.

It is probably still quite early to judge how that conflict has affected the ransomware groups, because there are two real reasons why Russia is a particular source of ransomware threat. One is that it has a large number of people who are skilled and interested in this, and the second is that people can act with impunity. Effectively, it is a jurisdiction in which they feel they can act without the state trying to prevent them doing that. It has been a comfortable operating existence, and it is hard to tell how that will change over time as the conflict continues.

Baroness Fall: Where would you say the balance was in Russia between state sponsorship and criminal gangs?

Lindy Cameron: For ransomware specifically, it is quite hard to tell, to be frank.

Q70 **Baroness Fall:** Moving on to non-Russia, where is the threat elsewhere, and is it growing in China?

Tom Tugendhat: That is not an area of massive concern at the moment, but we are aware that it is a concern for other countries. The UK is less the focus of Chinese ransomware attacks than other countries. I will not speak for them for obvious reasons, but it is a concern that some activity within jurisdictions affiliated to China or connected to Russia—countries like North Korea—have been particularly active in this space.

Lindy Cameron: To be specific, we have not seen China-linked ransomware affect the UK at this stage, but the Minister is absolutely right that other countries, particularly in Asia, see a different geographical picture. We have seen impact from Iran and North Korea-based groups, but it is much more limited than that from Russia, which is by far and away the majority of the geographical focus of ransomware actors.

Q71 **Lord Sarfraz:** How confident are you in the sector's ability to quickly

recover from a large co-ordinated attack on our critical national infrastructure, the health system, or the rail network?

Oliver Dowden: One of my principal roles as Deputy Prime Minister is cross-government co-ordination to make sure that, particularly in relation to cyber, we are sufficiently resilient. We operate a lead government departmental model.

On the specifics for each sector, it is very difficult to generalise. Different sectors have different levels of preparedness. The financial services sector, for example, has a very high level of preparedness, possibly because there is greater financial risk involved. In other areas, we have to work harder to make sure that they are prepared in the first place. The first thing we want to do is prevent anything happening in the first place. If those attacks were to happen, we are confident that they would be able to recover, but the speed at which they were able to do so would depend on the degree of preparedness they had in the first place.

Lindy, I do not know whether you want to talk about some of the actions that we have been working through with the NCSC to help them in that recovery process.

Lindy Cameron: We work really closely with the lead government departments and the regulators in each sector, obviously setting aspirations for how resilient they should be as part of the overall approach to national resilience. It is worth saying that cyber is often a vector to create a crisis in CNI, but it is not by any means the only one. In fact, some exercises that we do more widely on non cyber-related crises give us a really good insight into the levels of preparedness of different sectors for the kinds of consequences they might experience. Often the cyber element is about the initial attack surface; it is not necessarily about the consequences.

Using the cyber assessment framework, which is a tool that we developed as the NCSC, we have been helping to set a level of maturity that we would like leading government departments to ask their regulators to hold sectors to. That takes into account the level of resilience needed and the maturity of the sector. We set out publicly in the government cyber strategy what we expect of central government and local government. That is the aspiration we have set, and we are providing assistance to the regulators to try to help with that maturity, whether through exercising expertise, helping with skills and so on.

Lord Sarfraz: That is in relation to cyber, which is quite broad. On ransomware, are exercises or simulations done in this critical national infrastructure?

Lindy Cameron: Yes. We encourage people to think it through. Whether they should worry more about ransomware or more about the state theft of data or the potential for pre-positioning in order to disrupt depends on the sector, frankly. Different sectors will have different levels of risk. We see, particularly for private sector CNI, that thinking through the financial

consequences of ransomware is often a real incentive for boards to act quickly, because it is a risk they have to bear and, indeed, fund. Ransomware is one scenario in our Exercise in a Box toolkit, which we offer very widely and publicly through our website, to help businesses of all sizes to work through what kinds of scenarios they should respond to.

Oliver Dowden: There is a lot of commonality between a ransomware attack and a cyberattack. Often it will involve denial of access to critical data. We undertake a lot of broad exercising programmes. The most recent very large-scale exercise we did was Mighty Oak in relation to a national power outage and the lack of access to information and data. There are commonalities and things that we can learn about our ability to respond to ransomware. They are often not entirely compartmentalised.

Q72 **Lord Snape:** What contingency plans are there, if any, and what discussions take place about the ability of some of our national infrastructure organisations to recover from a ransomware attack? I am thinking particularly of the railway network. Given the concentration of signalling centres, an attack on a York signalling centre, for example, could paralyse the east coast main line from Newcastle to the south of Leeds. Are there any discussions with infrastructure providers like Network Rail, or any alternative to the existing system if such an attack takes place?

Oliver Dowden: The short answer is yes. The way we work through this in central government is that I chair two relevant committees: the National Security Council resilience committee and the ministerial cyber board. Through both of those, particularly the ministerial cyber board, the first thing I seek to do through my officials and analysis is to understand the extent to which individual departments and their arm's-length bodies are prepared, and the risks that they carry, and to challenge each of those departments to make sure that they are sufficiently resilient. In the event that an attack takes place, clearly it will be led by the individual government departments, but, particularly in major incidents, we can help them to co-ordinate the response.

For example, we have the GC3, which is a joint operational unit hosted in Government Security Group and delivered by the NCSC, the CDDO and the Government Security Group together to help co-ordinate the cross-government incident response. Again, many of the challenges one might find for a ransomware attack could also be caused by other factors—say, a power surge that put out signals and so on. So they might not have tested for a ransomware attack, but they will have tested for that kind of failure, if you see what I mean.

Q73 **Lord Dannatt:** The Government have imposed cyber resilience requirements on infrastructure operators through the NIS Regulations 2018. Your own post-implementation review of those regulations, however, found that many operators and regulators apparently do not have the skills and capabilities either to implement or to enforce them. What are you doing to address this?

Oliver Dowden: This is something I take very seriously, and indeed it is a problem across the wider digital economy. One of my previous ministerial posts was Secretary of State for Digital, Culture, Media and Sport, so it is not unique to this sector. It is about working with the Department for Education and with DSIT to make sure we have that skills pipeline for the long term.

In the short run, one of the things that we are doing to try to help include seeing whether there are external resources that they can draw in, and NCSC is validating those external providers of resources so that they can rely on that. DSIT has also organised training courses for new regulator staff. I would also say, and maybe I should have said this at the outset, that there is a very varied picture between different regulators. Some have fairly limited challenges. Others are much more extensive. I do not know whether you want to say some more about the validation point, Lindy.

Lindy Cameron: Thank you. We just had a bit of a breakthrough. We had a meeting of regulators a couple of weeks ago where they all agreed that the new Cyber Security Council will be a key part of helping them to see where people are accredited and what really good cybersecurity professionals look like. That move towards an industry body—a bit like in chartered engineering—where you understand what a chartered cybersecurity professional looks like, will really help people recruiting to understand how to find the market and, frankly, help to shape the market.

We then, as the Minister says, think about how we can help people to understand which organisations they can get good skills from. We are looking very hard at the ecosystem in the private sector to understand how we can effectively match people who need those skills in the regulators and in the sectors with cybersecurity expertise providers, whether those are organisations or individuals. We are trying to help that market to function better, which is partly why we worked with DSIT, formerly DCMS, to create the Cyber Security Council.

Lord Dannatt: In a sense, you have answered what I had in mind to ask next, which was whether it would be better to establish a specific cyber resilience regulator to oversee the NIS Regulations. You have partially addressed that already.

Lindy Cameron: The Cyber Security Council is not a regulator. It is effectively more like the Institute of Chartered Engineers. It is an institute that will accredit high-end cybersecurity professionals.

Q74 **Stephen McPartland:** The 2022 resilience framework is committed to reinvigorating the national exercise programme and that Government should undertake regular internal cyber exercising. What plans do you have to undertake such cross-sector exercises with key infrastructure operators?

Oliver Dowden: We have those plans, and we are currently going through the process of determining which sectors and scenarios we should conduct exercising programmes against. As you might imagine, there is quite a lot of demand from different government departments and across Whitehall and agencies to undertake exercises. I am absolutely confident that cyber disruption and access data disruption will form a significant part of a number of those exercises. We are going through the process of agreeing what they are. We should have them by the end of the year, and we will then announce them. I would be very happy to share the list of exercises with the committee once that determination has been made.

Lindy Cameron: We, as NCSC, are also doing quite a lot to support lead government departments and regulators in delivering exercises. We have done a couple recently with the downstream oil sector, for example. We also help to test the interoperability of response plans between different parts of government and the firms supporting key infrastructure with our high-end expertise, as well as exercising alongside international partners to make sure that we think about some border issues that might come into play and see the dependencies. We have launched a new assured cyber incident exercising scheme, which allows people to use the assured providers we referred to earlier to do that exercising. Plus, we have the free Exercise in a Box tool, which allows people to think that through.

Stephen McPartland: Okay, great. Oliver, I know you mentioned that there is a lot of demand across government for these exercises. Do the infrastructure operators know that they are going to be engaged in these exercises? Are they working with you, or is it just for them a whole list of, "This is one of several we're going to be doing?" If they are not really aware of it, how will we actually test the response as opposed to a tick box exercise?

Oliver Dowden: There is a whole spectrum of exercises. At the very high end, if that is the right word, we had Operation Mighty Oak, as I mentioned, which was a two-day exercise involving over 6,000 different officials and external bodies—maybe I should not go into too much detail about those—as well as other third parties, and extensive ministerial engagement over two days. We also undertake regular red team exercises and penetration testing, so the bodies involved will almost always know that they are part of this process. At the beginning of the process, they should have in their corporate collective mind what they think their preparedness is. We then test that and show them what their actual preparedness is and the lessons that those organisations learn.

Critically for me in the Cabinet Office, it is all about the interdependency between different bits of government, different departments, cascading risks and so on.

Q75 **Stephen McPartland:** Thank you. Lindy, you mentioned a number of points. In correspondence, the Government have referred to the NCSC's UK industrial control systems lab cyber project, and there seem to be layers upon layers. Can you tell the committee a little more about that

project and how it would impact on the critical national infrastructure operators, who have an actual job to do with critical national infrastructure every day, not just preparing for ransomware attacks?

Lindy Cameron: Of course, although I should probably first start by saying that people imagine that this is some big shiny building. It is effectively more of a project than a building.

That project is part of a much wider set of really important work that we do in NCSC that is designed to protect the critical national infrastructure. As the Minister said, ransomware is only one of many cyber threats that they face. In fact, for CNI in particular, in our annual report yesterday we called out the need for them to think more widely about the kind of threats they face and to be really mindful of the type of data loss they might experience or the pre-positioning for disruption that might come from greater interest by state actors as well as ransomware criminals.

However, as we have also said, preparing for ransomware is a really good benchmark for understanding whether they have the basics right. Unfortunately, far too much of my job is about telling people that they still have not done the things that we have been telling them they ought to fix for the last 30 years, which is a bit of a challenge.

We are increasingly worried about those threats, and CNI often depends on what we call operational technology, which is quite a challenging technology because it was not really designed to be internet-facing. Effectively, quite a lot of critical national infrastructure is trying to connect old technology with newer internet-facing technology. The architecture for that in tech terms can be quite challenging, and they need to make sure that they have really high levels of resilience to ensure that they have not accidentally exposed key services to the internet.

The ICS lab project was originally conceived to help us answer a five-year challenge to create world-class training, exercising and testing capability. It was originally funded for three years. We delayed the start slightly because of the Russia-Ukraine crisis, because we wanted to focus more on those immediate challenges. It has been running for the last year, and we have concluded that there is more private sector capacity out there than we had previously anticipated. All the engagement we had with those private sector initiatives caused us to pause and review whether this is really the best value for money.

We will now change tack slightly to focus more on other things, in particular the criticalities work that we do, which is about the interdependence between different sectors that the Deputy Prime Minister referred to: the key understanding that, for example, if the electricity sector was affected, that would affect a number of other key CNI sectors that might not have built that into their plans, and the CNI knowledge base is about understanding the details of those dependencies. We will shift focus on to those rather than carry on with the original project, because our experience is that the private sector is doing a better job

than we had expected, and we do not want to duplicate what the private sector can already do at really good value for money.

- Q76 **Baroness Crawley:** About this time last year, Mary Lanigan, the leader of Redcar and Cleveland Council, gave evidence. One of the things we picked up was that before the council had a very significant ransomware attack it had been given assurance that its security systems were adequate. I wonder whether your expectation of what is adequate has moved on since 2021 when it experienced its attack, and what are you doing more generally to help local authorities to recover should they be attacked, given that they have a huge constituency of very vulnerable people who depend on them? Mary told us that it was perhaps 18 months before they were up and running again, and certainly for the first few weeks and months many local authority departments were depending on pen and paper to make records. So could we start with how you are approaching the unique vulnerability of local authorities?

Oliver Dowden: I can tell that my colleagues are itching to come in too, but I will start. In broad terms, remember that one can never be totally cyber secure. That is impossible for even the most high-end organisation. The GCHQ might be one of the most secure organisations, but one can never say that an organisation is totally secure.

Secondly, the maturity of preparedness has improved across the public sector and across local authorities, but the threat has evolved considerably too, both in the state-based threat or state-aligned threats which the Security Minister described and in the maturity of the technology. We are just at the foothills of the impact of artificial intelligence on the ability both to conduct attacks and to be resilient to them, so there is inevitably a cat-and-mouse game going on.

In terms of our assessment, again, we work on the lead government departmental model. DLUHC is the lead department in this case, and its cyber support programme has provided grant funding and access to technical support for over 190 local authorities. We have also put additional funding through. In this current spending review period, there has been funding of almost £90 million for local government cybersecurity. The threat increases all the time, and our response increases all the time.

Lindy Cameron: That is absolutely right. Specifically, the government cyber security strategy that was published in January 2022 set an ambitious target, asking for the most critical functions to be significantly hardened to cyberattack by 2025, with all government organisations being resilient to known vulnerabilities and common attack methods by 2030. That is a really stretching target. We deliberately agreed pretty challenging aspirations, so it is certainly true that we have been pretty tough about what we expect, partly because the understanding of the threat, as the Minister says, has changed and evolved.

Local governments hold quite a lot of population-scale data, for example, which, as they now understand, is of real interest to people in training

artificial intelligence models, as I am sure Mary explained, as well as a lot of particularly sensitive data. It is really important that they and other parts of government understand that it is not just criminals or scammers they need to be resilient to; they also need to think about how to harden themselves as much as possible against a wider range of actors. As the Deputy Prime Minister says, that is extremely difficult to do, and it is a constant challenge to try to keep up to speed, because every time you upgrade your system, for example, particularly if you have a range of complex systems or older technology, that creates the possibility of allowing an attacker in. So it is a big challenge, and we recognise how tough that is for local government in particular.

Q77 **Baroness Crawley:** Thank you. There has been historical underinvestment not only in IT but in OT systems. It that one of the key issues as far as local authority vulnerability is concerned—the fact that operational technology and information technology are often just patched on top of each other?

Lindy Cameron: OT is not a particular challenge for local governments. It is a particular issue for CNI sectors, water, electricity, and nuclear. For local governments, the challenge is the same as for businesses. Businesses often accumulate a range of complex IT systems over the years. In the private sector, mergers are a particular challenge in that you are trying to bring together a number of IT systems.

In recent years, the understanding of the importance of constantly updating technology to make sure that you are not running old systems that are no longer supported has increased. You may have a bespoke system that you need, but it is very expensive to replace. Therefore, the challenge is for boards and councils to understand that, as much as it may be a challenge, it is sometimes important to prioritise that investment. That is not just a local authority challenge; it is an issue for the entire private sector in the UK as well as for the public sector.

Oliver Dowden: There are always challenges in relation to the hardware and the need to upgrade it. However, I would not underestimate the most basic things, and this is what I spend a lot of my time doing as a Minister. For example, as soon as an upgrade to existing software becomes available, you need to do the upgrade immediately, because that is almost certainly designed to patch a vulnerability. Often, as we know in our own private lives, and it is the same for businesses, we delay doing those things, which increases cyber vulnerability.

So it is not just the spending requirements that are significant; it is getting the basics right. If I had one silver bullet, it would not be to spend vast amounts more money. The single best silver bullet would be that everyone upgraded their software the moment they got an upgrade notification. That would be the single, most transformative thing that we could do for cybersecurity across government, private sector and business.

Lindy Cameron: That is absolutely right. In cybersecurity, human behaviour is as important as the technology.

Baroness Crawley: Where do local resilience forums come into this? I do not think they have particular responsibility for cyber issues, do they? Yet they are quite an important cog in the local authority wheel.

Oliver Dowden: The principal role of local resilience fora in this context would be in a recovery phase in the event of a major incident. Post Covid, we have been doing a lot of work to improve the capability of local resilience fora, but they are more at the consequence end rather than the preparedness end. The preparedness end is principally done through the NCSC cyber assessment framework and related initiatives.

Q78 **Baroness Fall:** I want to turn to smaller businesses and charities. The tier 2 businesses are off your radar in terms of big infrastructure, which, quite rightly, will be a national security issue. There is a sense that they cannot pay the money for the insurance and do not have access or the money to pay for consultants to help them out. Are you sure you are helping them as much as you can, and what more could we do?

On the national security side, do we feel that tier 2 is a vulnerability, because it is not as wrapped around in your radar when it comes to concern about a cyberattack in a made infrastructure.

Oliver Dowden: A lot of the time, we focus on what we have done wrong, or what we could improve as a Government. I genuinely think that we have been world-leading in creating the National Cyber Security Centre out of GCHQ and taking a whole-of-government and whole-of-society approach. I go around the world and have lots of visitors into the UK, and they tend to come to us to learn those lessons, so the creation of the National Cyber Security Centre has enabled us to get visibility of that problem in the first place, and to provide a range of tools to help them. Since taking up this brief, it has struck me quite how respected the NCSC is. I thought that was worth saying before Lindy came in.

Lindy Cameron: Thank you. We do lots of work with small businesses. You are absolutely right. I do not think we see them as second tier. In fact, often we see that small businesses are the gateway to a major incident for a bigger organisation or part of the public sector. We have seen that in the last year with a couple of supply chain attacks that have affected a large number of other players, as well as service providers of different kinds that provide services often not seen.

We encourage big businesses to think through what their supply chain looks like and what support they are giving smaller businesses in their supply chain—everything from setting standards and asking them to meet the basic cyber essentials criteria, as government does, to supporting them to ensure that their cyber resilience is good enough and that they are not in effect imposing risk on other people in the supply chain. For security, defence, and critical national infrastructure, it is particularly important that they take that whole-of-supply-chain approach. We have tried to drive home to boards that often the weakness

will not necessarily be in their primary systems; it will be somewhere further down.

In terms of what we have done, the Deputy Prime Minister is absolutely right. We take an unusually whole-of-society approach, and the national cyber strategy called that out. That means that as NCSC, which is part of GCHQ, we do not just focus on the parts of the UK that are of greatest national security interest but think about the whole of society, including individuals and small businesses. There are so many small businesses that we have tried to think about what we can do at scale.

We do a range of things. We provide incident management support if an incident hits a particular threshold and, in particular, we provide a lot of advice, and try to do that in a really bespoke way through sectors. A good example is the farming sector, where we try to provide advice at a time when farmers are most interesting to criminals and have the most money. We also provide it through the industry bodies which they recognise as providers of advice on other issues, whether that is finance or risk in general.

We also provide a number of automated services. A number of our active cyber defence services are available to small businesses, such as early warning advice that people can sign up for. However, recognising that some small businesses will not necessarily have the maturity or, indeed, the IT support to be able to do that, we are also working with the tech companies to try to make sure that the technology provided and the services people buy are secure by default and design. At the recent AI summit, we pushed really hard for the next generation of AI-enabled services to be absolutely secure by design, because small businesses in particular cannot be expected to do that kind of assurance for themselves. They need to be confident that the technology they buy is secure enough and turned on by default, rather than asked to make sophisticated decisions.

So we provide the tools and advice, bespoke if we can, and we try to encourage the provision of security. We are also working on the ability to buy internet-of-things devices that have a default secure password to make sure that the basic threshold for what businesses buy is improved. There is a whole range of measures, but we try to do things that affect a wide range of businesses in a general way, rather than give individual advice company by company.

Q79 **Baroness Crawley:** Deputy Prime Minister, as a committee, we asked whether you would consider introducing a reinsurance scheme for cyber, but you told us that it would not be considered an appropriate use of public funds. Flood Re is fully funded by premiums and a levy on household insurers. Would the Government not consider establishing a self-funding model in the same manner as Flood Re?

Oliver Dowden: We do not want to encourage a situation whereby organisations feel that they do not have to take the necessary steps in

the first place because there will be some kind of government fallback or bailout, so it is not just the cost implications.

Tom Tugendhat: This is an area where we have had serious debate. As you will know, in 1993 the then Government established Pool Re to help absorb some risks of terror insurance, because it was an uninsurable risk. The Government have introduced Flood Re for a very similar reason in the flooding context, and this is an area we are keeping under review.

The reality is that the market is addressing quite a lot of these questions pretty effectively at the moment. Cyber products are available on the market, and so long as the market is answering the need and appropriately pricing the risk they face it is encouraging the behaviour which the Deputy Prime Minister and the director of the NCSC are quite rightly championing, while at the same time providing the protection that small businesses may need should they unfortunately be targeted by a more effective attack.

Baroness Crawley: In answer to an earlier question, you said that these instances are probably on the rise. We are second only to the US in being highly targeted, so it will presumably get worse before it gets better. When you say that it is under review, is that a serious monitoring? Are you coming back to it in a few months?

Tom Tugendhat: It is more of a market question. We had to establish Flood Re and Pool Re because the market could not provide insurance based on an unknown risk, so the Government stepped in to cap that risk and allow the market to grow underneath. In a firm like Pool Re, I cannot remember how many billions they have on the management now, but it is certainly over £10 billion, which means that they have now removed the Government from being the insurer of last resort.

Flood Re is pricing appropriately. It has not quite got to that stage yet in its assets under management, but given that the market is providing cyber insurance, it is not immediately obvious that a government reinsurance scheme needs to be put in place, given that the market is providing not only insurance but reinsurance through other businesses that I could name although it is probably wise not to.

Lindy Cameron: I am on the public record already speaking about the fact that I think there is still a lot more that the insurance industry could do, and we can work with it on how to make sure that it matures in a way that means that it is better able to provide well-priced insurance, and indeed that the take-up is higher from particularly small businesses. We have worked with the Information Commissioner's Office and the Association of British Insurers, for example, to think about the anonymised data that could be provided to ensure that it is easier to price the risk effectively, because this is still a maturing market; it is much better than it was, but it still has some way to go.

On the other side of that, businesses often do not understand the benefits of insurance where it effectively incentivises the preparation.

Fundamentally, when you buy your home insurance, you check to make sure that the door and window locks are indeed compliant and that you are not away from home more than the days it says in your policy. We want businesses to do the same in cyber insurance terms, so that insurance incentivises people to be really well prepared.

We have seen that with cyber essentials, which is the basic minimum standard that we suggest companies should meet in order to contract with government and which provides a level of cyber insurance once you have become accredited. We have seen quite low levels of need to call on that insurance, because doing cyber essentials means that businesses are better prepared and are a less interesting target for cyber criminals.

We still think that there is more that we can do, and we are in a very live conversation in my team about how we can help the insurance industry as a whole to get the data it needs without interfering in competition, while making sure that the industry is providing what it is able to and that the take-up is there from the businesses that need to do that.

It gets more complex as you get more sophisticated, so pricing the risk for a very large corporate with many different IT systems is quite challenging, but, for the small and medium-sized business end of the market, it ought to be a really obvious answer.

Tom Tugendhat: As long as the market is providing the risk mitigation service, it is not obvious to me why the Government would feel the need to impose that on every taxpayer in the United Kingdom in a situation where individuals who choose to take on that risk can volunteer to do so through ownership or provision of market services.

Q80 **Viscount Stansgate:** When we first started this inquiry, one of the things we discussed in the committee was what data there is about this issue. The Government's own written evidence acknowledges the lack of data on ransomware, which creates challenges for the policy response.

Would you consider introducing a statutory reporting requirement if the expectations on victims were realistic, such as a requirement that they report a ransomware attack to a central body or regulator within a few months of the attack, and with assurances that this will not be made public, because we all understand the danger of reputational risk. Would the Government consider such a statutory requirement?

Tom Tugendhat: This is something we have looked at. Action Fraud, the UK's national reporting centre for fraud and cybercrime, collects the data that you speak of. You are right: it is not complete, and some companies are not reporting. We are looking at ways of encouraging that. The question is whether the reporting requirement achieves the aim we imagined. There are jurisdictions that have included reporting requirements, and it would not always be sensible to include reporting requirements down to the lowest level. Unfortunately, sometimes that has meant that people have not reported when they should until they have reached the threshold.

We are looking to incentivise best practice in sharing knowledge and understanding so that a low-threshold attack can sometimes provide the information that will lead to preventing either a multiplicity of low-threshold attacks or a single large-threshold attack. The threshold requirement, or the compulsory reporting requirement, may not achieve the aim that is sought.

We are looking at countries and jurisdictions where those requirements have been put in place, and at other ways of incentivising positive community action of reporting. We are seeking to address the balance between public and private reporting and between open and closed publication of data in order to keep the maximum number of people safe and to be able to address the threat faced by the United Kingdom.

Lindy Cameron: We are very supportive of that, because we want people to tell us as soon as they can. As the Minister says, often it is not about the challenge and the impact for them as an individual business; it is about helping us to spot early what the wider impact might be, so we do not want people to delay until they absolutely have to.

We already have a mandatory data breach-reporting regime, and we have been working closely with the Information Commissioner's Office to make it clear that reporting early to the NCSC is something that the Information Commissioner will respect and reward, and certainly wants to incentivise, because that means that we can limit the impact of some of these potentially wider and challenging attacks.

We think there are a number of ways in which we can use the data that we get and to incentivise the provision of more data within those systems before it is necessary to move to a wider system where it might provide better data, but I am also concerned that it might disincentivise some behaviours that we are looking for.

Viscount Stansgate: Minister, do you have an idea in your mind of where the threshold exists beyond which you would take one view of what to do rather than another?

Tom Tugendhat: I am not keen to put a number on it, because different jurisdictions have done it differently, and none of the thresholds has answered the question in the way we should be answering it.

The scale of some incidents is incredibly low, and they would never be included in any system that had a threshold limit because they are simply not of that scale, but they demonstrate a pattern from which the experts in the NCSC and GCHQ, or indeed in some antivirus software companies, could learn lessons that would prevent a multiplication of the attack or a greater attack.

That is why I am really uncomfortable with thresholds. They suggest that the Government are interested only in this scale, this amount of data loss, or this level of penetration, when actually the Government are interested in protecting every business and every piece of data loss. That

is why the director of the NCSC was absolutely right to mention that the work we do with the Information Commissioner is really important, because we ask for data breach reporting even if the data breach is extremely minor.

On cyber, are we really going to ask everybody to report a phishing email? I do not think we are, but where are we going to set that limit? That is where we will ask for judgment calls by an alert public and particularly by companies and charities that have an idea of what to do. This is where I come back to the point that insurance is incredibly important, not just in pricing risk but in incentivising best practice. We can get to where we want to go through a risk matrix or a risk model that is better informed by the insurance sector, but also by individual action.

Q81 Stephen McPartland: The national cyber strategy sits under the National Security Council. With everything going on in the world and all the threats to the UK at the moment, how often do we realistically get to discuss cyber issues on the NSC?

Oliver Dowden: There is a long-standing convention that we do not reveal the details or topics of specific meetings when they are held, but I want to be as open with the committee as I can in an open forum. The national risk register identifies cyber as a key risk. Within the National Security Council structure, the Prime Minister, when he took office, created the National Security Council resilience committee, which I chair. I have looked back through all the topics and agendas that we have covered, and I can assure you that cyber has featured one way or another in pretty much every meeting. Cyber is one of those cross-cutting risks; if you look at almost all the risks that we have to be resilient against, it is a factor. So it is either specifically an item or it has featured significantly in the discussions we have undertaken.

There are further fora. There is the ministerial cyber board, which I also chair, which looks specifically at our preparedness in government and in government agencies and is a method by which the Government and I hold individual departments and their agencies to account. In addition, we work between government and business with the National Cyber Advisory Board, and, in respect of all those, cyber has been a significant agenda item. The final area is the UK Resilience Forum, where we also engage with the devolved Administrations; again, cyber has featured there.

Stephen McPartland: So you would not really want to set up another ministerial committee on cyber.

Oliver Dowden: One of my challenges as the lead Minister in Cabinet Office is seeing off further committees unless there is a very strong case for them. It is very easy to set up a committee, but I do not want committees that are established and then do not meet very frequently or do not provide a genuine forum by which we can collectively make decisions as a Government or hold departments to account. I am confident that the existing structure is sufficient.

Q82 Stephen McPartland: The Conflict, Stability and Security Fund will be merged with the national cyber programme into a new integrated security fund. The committee's concern is that it has a very wide domestic and international scope. How are you going to ensure that it delivers on strategic objectives, rather than just day-to-day political problems or the latest attack?

Oliver Dowden: The whole purpose is to take that strategic approach, and it flows out of the integrated review refresh that we announced a few weeks ago. My colleague in the department, Baroness Neville-Rolfe, is currently going through the process of considering the allocations under that. Those will then come to me and will then go to the National Security Council for sign-off.

I am confident that this will be a significant priority, given the scale of challenges we have in relation to cyber, which you have heard about in the remarks of all three of us. Those allocations will be made by the end of the year, so I am happy to provide an update once those decisions have been taken.

Stephen McPartland: Will specific cyber objectives be set out as if there is a national cyber programme element? If so, we know how friendly the Treasury can be when you ask for more funds. Will an element of that fund be ring-fenced for cyber?

Oliver Dowden: The clue is in the title, as it were. It is supposed to be an integrated fund. Creating ring-fences within an integrated fund would cut across the purpose of it. I do not want to pre-empt decisions that have to go through the proper process, but I am confident that cyber will feature significantly within that. As my colleagues have discussed, given that cyber is a significant factor for hostile states and aligned criminal activity, I would be very surprised if it did not feature quite significantly.

Q83 Lord Sarfraz: The Home Office claims the lead on ransomware but has not made any significant policy interventions in the last year on this specific topic. There have been no speeches or statements by the Home Secretary on cyber or ransomware. Deputy Prime Minister, would it not be better for you to have the prime responsibility for ransomware, given your wider cybersecurity responsibilities, your convening power and your proximity to the intelligence community?

Oliver Dowden: I will ask my colleague, the Security Minister, to say in more detail about what the Home Office has been doing. Again, one of my challenges in running the Cabinet Office is that almost every problem has some element of other government departments in it. We have to delineate between what is appropriate for a government department and what genuinely does not really fit neatly within any government department and really requires that cross-cutting effort, particularly given the different scale of the resources that we have between the Cabinet Office, which is a form of co-ordinating department and an HQ, versus the depth of resources we would have in a very mature department such as the Home Office. Also, given that criminality remains the principal

driver of ransomware, I always keep an open mind, but I am fairly sceptical about it.

Lord Sarfraz: It has still been one year without any statements or speeches.

Tom Tugendhat: You say that, but we have made public pronouncements about joint ransomware initiatives that we have achieved with the United States, including jointly sanctioning some Russian actors about a year ago. We have published various policy papers on the work we have done. We have brought together various different partners in various different ways across the ransomware area, in fact, boosting on the work we have done through the counter ransomware initiative, which we chair alongside our US partners and others.

There are many areas in which we have been leading this work across government, and we can point to certain successes. Those successes are mostly down to the fact that we have begun what is very important, which is the identification and the sanctioning of individuals to dissuade and deter those who would otherwise seek to profit from ransomware not just here in the United Kingdom but around the world. That co-ordination action internationally is incredibly important, because a lot of these ransomware groups seek to start off in one country and then expand into others.

You are right that this is an area on which we have not made a statement, but we have certainly championed the work that the Government are doing. I have given two or three interviews about this at various points, including on MSNBC at about 6 am, so it would have been at 1 am UK time; I am surprised the noble Lord did not see it.

Lord Sarfraz: I will look that up, thank you. Minister, has the Home Office done enough?

Tom Tugendhat: There is always more to do. I am content that the Home Office is leading appropriately across government, and that the UK is very much ahead of the pack or is certainly equal to the front of the pack. I am not content with where the pack is, and this is where there is much more to do. This is where it is down to how we work with partners and with the private sector, and how we pull this effort together.

That is one area where the Deputy Prime Minister, through his leadership as Cyber Minister, has been incredibly important in pulling together the UK governmental effort, but it is down to me as well, and I am here to take the criticism for it. We are bringing in various areas that are connected but not always seen as part of the same thing.

In spring next year, we will do a fraud summit. Fraud is fundamentally connected to ransomware. It is intimately part of the same danger, and, again, that is where we are doing more. This will be the first international fraud summit. Nobody else has done it, and I am very proud that we are

leading on it, but it again points to the need to do much more internationally with friends and partners. Ransomware is one of those crime groups that is very difficult for the UK to solve alone. The vast majority of initiatives start abroad, and most times in jurisdictions over which the local police have absolutely no interest in supporting us.

Oliver Dowden: It is important to distinguish between the policy and the criminal response that sits with the Home Office—so that the committee does not feel that I was too flippant in my initial comments. As the Security Minister said, we are pulling together this multi-stranded response through the National Security Council resilience committee, through the ministerial National Cyber Advisory Board and others, and through the Cabinet Office, which goes across law enforcement, national cyber force, international partnerships, building capability and skills. We are not saying, “There we are. It’s over to the Home Office, and we wash our hands of it”. We are bringing together all those strands. It is more a question of the specific issue of ransomware and where that sits.

Q84 Lord Butler of Brockwell: My question is also about the activities of the Home Office. It is now two and a half years since the Home Office started consultation on the Computer Misuse Act. A review of the Act published yesterday said that there would be further legislative solutions in the near future, and I really want to know where those will be. Is this a reference to the Criminal Justice Bill or the Investigatory Powers (Amendment) Bill in the King’s Speech?

Tom Tugendhat: Naturally, I blame my predecessor, who sits around the table just over there, but the reality is that this is in the Criminal Justice Bill. The Investigatory Powers (Amendment) Bill is just an update.

We are also planning to look at the recently strengthened Network and Information Systems Regulations 2018 and the Telecommunications (Security) Act 2021, because those all tie together in some areas we are looking at. You are absolutely right: the Computer Misuse Act was introduced before the internet, so it is not exactly up to date, and it would seem wise to introduce amendments and updates to it.

As you will know only too well, the challenge is that parliamentary time is tight, and drafting regulations like this must be done extremely carefully, because the question is fundamentally about how security can be provided if antivirus software and defensive programs require certain levels of permission in order to act within computers.

This is one of those areas where the world has changed fundamentally from where we drafted it in the 1980s. When it was drafted in the 1980s, a computer was a standalone item, entrance to which had to be given by whoever held it. Now, most people’s data is held on the cloud, and the computer is frankly just the operating environment to access the information. The question of misuse and data protection, and therefore intervention, in somebody’s computer is meaningless if your data is held in the cloud and your computer is just the screen.

This is where it is quite clear that we need to update this. It is an area of quite careful consideration because of the way the programming operates on platforms, the way data is held, and the way defensive mechanisms now need to understand the environment of the data systems they are operating in.

Lord Butler of Brockwell: I mentioned two of the Bills in the King's speech. Which one is most likely to bear on this?

Tom Tugendhat: It would be the Criminal Justice Bill.

Q85 **Lord Butler of Brockwell:** I now want to ask you about the National Cyber Crime Unit, which employs only 5% of the staff of the National Crime Agency. In view of the huge surge in serious crime, are you confident that it has the resources it needs?

Tom Tugendhat: I am not going to have this debate in public, but a debate I have very regularly with the Treasury is how we resource different areas appropriately. This is where we are looking very carefully at how the Government operate in various different areas, because this is not just a National Cyber Crime Unit challenge; this is a whole-of-government challenge.

As the Deputy Prime Minister correctly put it, the basics for cybersecurity are the sort of systems operator tasks that well-functioning Administrations do rapidly. That is the best form of security. The National Cyber Crime Unit is the firefighter, and we all have a responsibility to make sure we are keeping our fires under control.

Lindy Cameron: I completely agree with you. Particularly in the context of ransomware, we are certainly not going to arrest our way out of this problem. As much as we really value our partnership with the NCCU, and with the NCA in general, the real focus for us is driving up resilience. We need to make sure that businesses and government are better prepared, understand what the threat looks like, and are able to minimise the recovery time and the damage done by what is, as you have described, a really serious threat to them. I would prefer to see more effort on the resilience end to make sure that we can help people to prepare, rather than simply focusing on what to do once we have seen this.

We have a fantastic partnership with the NCA. In particular, we did some really innovative work on trying to understand the ransomware threat. We built a threat model that helps to categorise the ransomware groups that are a direct threat to the UK. In fact, in the context of the counter ransomware initiative, as the Minister has described, we have now been sharing that model with a number of other countries that have basically adopted our approach to help them to understand what the threat to their countries looks like, and, indeed, to help us to understand what the global ransomware threat looks like with much more fidelity. We have done some really innovative work, but more in the understanding and threat space than in the execution space.

Lord Butler of Brockwell: The director-general of the National Crime

Agency told us that the FBI has been more successful than the UK at disrupting ransomware operations because it has more resources. The Treasury ought to be rather keen on stopping ransomware, so it ought to get a sympathetic hearing. It also has stronger legislation, so it seems as though the NCA has insufficient resources in this area.

Tom Tugendhat: I would be astonished if the director-general of the NCA were to argue for fewer resources, given the requirements on his time. The work the NCA does is remarkable and impressive, not just in this area but across a range of crime areas, including people trafficking and child abuse. The FBI is a comparator in some ways, and in some areas the NCA is a more effective outfit and in others slightly less. That is the nature: when you are competing at the very highest level, sometimes one of your competitors will be slightly ahead.

The reality is that this is not just down to the NCA. Differently from the FBI, we operate a much more integrated system of intelligence support to businesses. The NCSC is a classic example of this. The NCSC is a branch of GCHQ, the world's premier cyber intelligence service, which means that we have an extra to the NCA. It is not just the NCA; the NCA is the law enforcement arm, but we also have a disruption element, which is the GCHQ, and a public-facing element, which is the NCSC.

We also have the area that really puts us ahead, which is the whole-of-government approach to counter ransomware initiative. To the point Lord Sarfraz raised, we are the ones who led the joint statement on ransomware payments, which 47 countries signed at the CRI summit in Washington earlier this month. We have seen significant changes in very different areas.

Quite rightly, Graeme Biggar is asking for more resources, and I completely appreciate where he is coming from; I am constantly having this challenge. But it would not be right simply to compare the NCA to the FBI. The NCA does a range of things that the FBI does not, and we have a range of other services that add to the NCA's capability that would not be included in the FBI comparison.

Lord Butler of Brockwell: I understand that NCA salaries are at a lower level than in policing generally, and people in this area must be very expert. Are you happy with that situation?

Tom Tugendhat: The NCA salary comparators are very difficult to make, because the NCA employs on different bases depending on whether people are employed through UKIC as warranted officers or are part of the Civil Service. It is not a flat comparison, and it would be wrong to try to draw it across. However, it is very difficult to compete with the private sector for the kind of skills and salary levels that we are able to command in government.

The level of dedication of heroic individuals who are not just willing but enthusiastic in serving our nation and defending us from cyberattacks, and are really doing good for their country, is remarkable. It would be

appropriate to put on record our enormous thanks to many people who work in the cyber defence of the United Kingdom, not just in the NCA, but in GCHQ, the NCSC, and indeed other agencies and branches of government.

The Government will never be able to compete with the salary scales that some private companies are able to offer. I believe that Facebook's starting salary is now north of \$250,000, which is a little more than even the Cabinet Secretary. It puts us in a place where we are not competing on money; we are competing on the ability to operate at the highest level with the finest minds in the most contentious and challenging environments the world knows in cyberspace. That level of challenge, interest and competition—and the sense of duty and purpose, knowing that they are defending their fellow citizens, our freedoms, our rights and our prosperity—is what keeps people motivated and committed. We are blessed and lucky, and I am very proud to work with such extraordinary people.

Lord Butler of Brockwell: Thank you for saying that. It is true of the Civil Service generally.

Tom Tugendhat: I would agree.

The Chair: The committee shares the admiration you expressed, but, when we discussed these issues at the NCA, the comparison with the recruitment possibilities for the police service more widely was one of the things that particularly struck the committee. Although we must all be extraordinarily grateful for what people are prepared to do, another matter is whether we should be asking them to.

Tom Tugendhat: Perhaps, Dame Margaret, you would excuse me for introducing one codicil, which is that none of this should be taken by the Chief Secretary to the Treasury as my reticence in asking for the appropriate funding for the services we require. I am sure she will be expecting me to be as robust as I will always be in making sure that we get the correct support for our fantastic experts.

The Chair: We are coming to the end of the questions that we had to ask and thank you all very much. Given the publication—and I am afraid the late publication for us—of this week's reviews, I hope you will not mind if we write to you with a few more follow-up questions.

Oliver Dowden: Of course.

The Chair: Could I ask for as quick a reply as you can, within a couple of weeks if possible, so that we can, hopefully, take advantage of it in preparing our report?

Oliver Dowden: Our excellent civil servants will expedite that process.

The Chair: Thank you very much. Members of the committee, although we are coming to the end of the questions, I hope you will stay for a moment or two, because there are some discussions about future

meetings that I would like to settle. Thank you all very much for coming, and for the evidence you have given.