Joint Committee on the National Security Strategy

Oral evidence: Ransomware

Monday 19 June 2023

4.20 pm

Watch the meeting

Members present: Margaret Beckett (Chair); Baroness Crawley; Lord Dannatt; Baroness Fall; Richard Graham; Angus Brendan MacNeil; Lord Reid of Cardowan; Lord Sarfraz; Lord Snape; Viscount Stansgate; Bob Stewart.

Evidence Session No. 4 Heard in Public Questions 53 - 66

Witnesses

I: Graeme Biggar, Director General, National Crime Agency; Rob Jones, Director General of Operations, National Crime Agency.

Examination of witnesses

Graeme Biggar and Rob Jones.

Q53 **Chair:** Welcome and thank you very much for coming to give evidence today. As you may have noticed, this is the fourth oral evidence session of our inquiry into ransomware. We were very grateful to the National Crime Agency for hosting us for a very informative visit in February, which I think we all much enjoyed, but this is an opportunity to explore a variety of issues on the public record including, I hope, some of the operational challenges that you face when you are trying to address the threat from ransomware. I should say, for a wider audience, that this is a hybrid meeting so some Members are joining us remotely.

We have heard conflicting evidence on recent ransomware trends, and what I would like to hear first is your understanding of whether the threat from ransomware is still increasing or whether it is now beginning to wane.

Graeme Biggar: Thank you, Chair. I am happy to kick off on that, but we have Rob Jones here as well, who is our director general of operations. He has been working on cyber and ransomware himself for some years now.

It is quite difficult to tell. One of the operational challenges we face is our understanding of what is happening and the reporting from companies or individuals, but particularly companies, about whether they have been attacked. We do not get the majority of reports in, so it is quite hard to tell. We look at different sources. If we look at Action Fraud reporting, which is one place where companies or individuals are meant to report in, we see that roughly 30 ransomware attacks a month are reported. That has been relatively stable, dipping slightly but not in a statistically significant way. If we look at some of the websites that track cryptocurrency ransom payments, we see that over the course of this year they have been trending up slightly and are back to 2021 levels.

It is slightly hard to tell, which is not a very satisfactory answer, I am afraid. Broadly, it has not changed very significantly in scale over the last three years. On Russia's invasion of Ukraine, we did see a bit of a dip. We think that has returned to where it was before, but in terms of the number of attacks it has been broadly stable to the extent that we understand it. Would you like me to say a word about the nature of the attacks?

Chair: Yes, please do.

Graeme Biggar: Those have changed somewhat in the last two or three years. When you started this inquiry, ransomware was very much still someone hacking into a company's website, encrypting the data and requiring a ransom to get the key to decrypt it. We still see that, absolutely, but we have seen a move over the last year to exfiltrating the data rather than encrypting it and then threatening to publish it on the dark or open web. That is a slightly easier thing to do; you do not have to be as deep into someone's IT to be able to exfiltrate the data as you would to encrypt it. We have seen that as one part of how the threat has evolved.

Another has been the move away from very significant targeting of critical national infrastructure on the back of the attack on Colonial Pipeline in the US and the response to that from the US authorities. A number of the ransomware groups, that we assess are predominantly still Russian speaking and, largely, Russian based, have moved away from the CNI and looked to other and broader sectors including small and medium-sized enterprises on the basis that they are less likely to have the weight of law enforcement and the intelligence community descend on them. That has been a second trend.

The third trend, and Rob might want to come in as well, is the evolution of what we have termed ransomware as a service. Initially, you had these very sophisticated, as I said, largely Russian-speaking groups developing their own strains and conducting the ransomware themselves. Over the

last 18 months, we have increasingly seen them, in effect, hiring out those services and providing a series of tools to let other people use that ransomware and charging a price for that. That has been worrying in the sense that it has reduced the threshold for entry into this crime, so it is easier for a broader range of people—

Chair: You do not have to be an expert.

Graeme Biggar: Exactly; you do not have to be as much of an expert to do it. They are some of the trends, but Rob might want to pick up.

Rob Jones: Could I, perhaps, just build on a couple of those points? The affiliates operating the ransomware as a service model have, in effect, industrialised what was quite a stable high-end model that we well understood. They were people who were, perhaps, out of our reach in jurisdiction to risk, typically Russian speaking, but that business model was relatively stable. What ransomware as a service and the affiliate model have done, is allow a more chaotic approach from our adversaries and, perhaps, there is a less considered approach to those attacks.

Graeme talked about the classic ransomware attack where you may be negotiating with somebody about your encrypted data. What we see is a hybrid model where you have everything from that more classic model through to a very adversarial hack-and-leak where your data is posted almost immediately. All this is to engage a classic extortion model where there is an imbalance of power and you have to pay, and that is the monetisation of the model. That leverage is obtained either through the encryption or a very adversarial approach where you are told, "Your data has been posted. If you want it taken down and you don't want it to proliferate across the internet, you'd better pay". That more chaotic approach is, obviously, more challenging because it has lowered the barrier to entry and has pushed that model on from something that was quite niche to something more mainstream.

Chair: That is very helpful. Can I just go back for a second to where we began? I hear and, of course, take very seriously what you say, but there have been some recent reports which have suggested that, globally, ransomware attacks are decreasing, but that attacks against the UK are rising and that we are now one of the main global targets. It is hard to quite square that with what you are saying because what you seemed to be saying is it is much as it was. It may be rising, but there is no great, huge—

Rob Jones: The UK has always been one of the main global targets. We have a vibrant economy. The UK financial sector has always been a target and always will be. We have lots of SMEs that could become targets for this type of activity. The way adversaries flex how they attack is maybe skewing those figures because of the perceptions of what is playing out in the UK versus the US and elsewhere. I agree with Graeme's assessment that we have not seen a big spike. What we have seen is a change in the operating environment for the Russian-speaking groups and some disruption because of Russia/Ukraine, a change in where some of the

infrastructure is based, and a change in some tradecraft. Overall, the activity internationally feels about the same as it did in 2021 with some dips along the way, but a recovery towards those sorts of levels.

Chair: Thank you very much. Lord Dannatt.

Q54 **Lord Dannatt:** Can we move the conversation towards UK ransomware strategy? In 2019, the National Audit Office criticised the Government's implementation of their National Cyber Security Strategy and warned that they risked making the same mistakes with their subsequent cybersecurity efforts. As I think we know, since 2019 there has been a sharp increase in ransomware attacks, so the question really is: have UK authorities' resources and capacity expanded sufficiently, so far, to address this threat? Then, the corollary is whether enough long-term funding has been allocated to meet the scale of the challenge that we now face in ransomware.

Graeme Biggar: I will kick off, Lord Dannatt, and Rob will come in—he has been on this journey longer than I have. To be clear, we are not here to speak for the Government; we are here as an operationally independent law enforcement agency. We have seen a significant increase in cyber funding over the last 10 to 12 years from the national cyber programme. That did not exist before, and it does feel like one of the threats that we deal with where the Government have made an effort to fund it. There is a separate question about whether that is enough and what we have done with all that, but it certainly has not been ignored.

A new cyber strategy came out in December, as you will have read. We and our operational partners are happy with the direction of that. There have been long debates about the balance within it between, for example, resilience and disrupt. I think we are all agreed that the most important thing to do is to improve the cybersecurity of as many companies and organisations around the UK as possible. At the same time, there is an important role for identifying, deterring and disrupting ransomware groups, which is what we, with others, are focused on.

Rob Jones: What has worked well across Whitehall in relation to the response to ransomware and what we have done differently as the threat increased is the convening power to be able to pull together a coherent ransomware strategy. We have recognised that the threat is extraterritorial. It is not a classic serious organised crime threat. We cannot just go after people in the UK. We need a range of tactical options—from sanctions through to the ability to seize crypto assets—to undermine the business model.

What we have focused on with partners across Whitehall, in UKIC, and in policing is the doctrinal approach to undermine that business model, which is looking at the enablers and that low barrier to entry to prevent affiliates proliferating and codifying the response where we go after the most harmful strains. That approach has worked well.

Could we do more with more resource? Of course we could. It is the classic challenge for serious organised crime. We have a good, well-funded response in relation to what we are now dealing with. Looking forward, we have some considerations and tough prioritisation decisions to make over the next few years as we head into another spending review.

Lord Dannatt: My takeaway from that is, yes, of course, as with anything, more resources mean you could do more but, if I understood you correctly, the ability to organise, to focus, and to make the whole approach more cohesive has, hitherto, been the more effective approach.

Rob Jones: It has. The system in place in the UK to deal with a big attack—the national security structures that that engages, the ability for COBR to be convened, the ability to work right across civil contingencies to deal with that—is envied across the world. Thankfully, we have not had the highest level of cyberattack in the UK, and I hope we never do.

The work the NCSC has done, in terms of breaking out reporting and working with victims and law enforcement, has bridged that gap. In terms of response and the maturity of what we have developed, we have come to the point of deciding where we go next. That means looking at the legislation that we work with, looking at the extraterritorial actors behind this and, ultimately, extracting a cost from the people behind this, who are typically outside the UK.

Graeme Biggar: Lord Dannatt, could I just add briefly to that? I do not want us to give the impression that this is fine, it is completely resourced and we have got it. If you take a step back from ransomware and look at crime affecting the UK, one of the major trends—as I said to the committee when they came to the National Crime Agency—is more crime going online and more of the crime that is not online being supported by technology. That is a really significant shift in the way that crime takes place that has not yet been accompanied by a similar shift from law enforcement, including the NCA, and ransomware is then one part of that.

That is, potentially, the most acute manifestation of the crime. It is the one serious organised crime that could bring the country to a standstill and has not yet. As Rob has suggested, we have not had a C1 attack, in the way we describe them, but it is part of a bigger challenge we have, which is shifting both the NCA and law enforcement and, frankly, the Government machine that sits around and beside that, into dealing with the online world in the way it currently demands.

Q55 **Lord Dannatt:** You said, quite rightly, that you are independent law enforcement agencies. Nevertheless, this committee takes a very keen interest in keeping an eye on ministerial oversight in a whole range of things, including national security strategies such as cybersecurity. Could you tell us what level of interest Ministers are taking in the implementation of the various cyber strategies, particularly, those highlighted in the integrated review and the integrated review refresh?

Indeed, when did you last meet Ministers on these subjects? We would just like to know the degree of dialogue that you have with the responsible Ministers.

Rob Jones: In relation to cybercrime and the Home Secretary's responsibilities, there is weekly engagement with the Home Secretary around our work against these threats. In relation to the implementation of the strategy and Cabinet Office responsibility, there are regular meetings where the different strands of activity are tested, which we all play into. That interest is very real, keen, and is part of the cross-Whitehall response to the implementation of the strategy. Our focus is cybercrime and, when required, there is now day-to-day dialogue in relation to progress.

Lord Dannatt: Is there anything you want to add to that?

Graeme Biggar: Yes, my team spoke to the Home Secretary on Thursday last week about a particular cybercrime capability. The Chancellor of the Duchy of Lancaster has responsibility for cyber resilience, the Home Secretary for cybercrime and, under her, the Minister for Security, a former Member of this committee, I think. It is inevitably diffuse. This is about the risk of crime against computers and that is all-pervading. It needs to be pulled together and there need to be committees and strategies around that, but it is searching for a holy grail that does not really exist to have one person who is responsible for everything.

Lord Dannatt: I think I understand that. From what you are saying, you feel that you get a decent degree or a sufficient degree of ministerial access and there is sufficient open-door policy as it were so that, if you have issues within the strategy, you can then ask for further support.

Graeme Biggar: Absolutely.

Q56 **Viscount Stansgate:** Good afternoon. By the way, it was really enjoyable to come and visit you, and it is nice of you to return the compliment and come here. I wanted to ask about a piece of legislation, the Computer Misuse Act 1990. I do not know how many people can remember what computers looked like in 1990.

Chair: That is a good thing.

Viscount Stansgate: It would be nice to know. There will be museum pieces from that date. Obviously, such an enormous amount has changed in that time. Could we have your thoughts on what changes you think should be made to the Act to bring it up to date? It probably could not be brought up to date and would just be replaced with an entirely new framework of legislation, but what would be in it in order to better support the operational response to the problems we are discussing today?

I will ask my follow-up question as well because it may trigger your response. Do you have any other legislative reforms that you would like

to bring to our attention that you would like and benefit from? Are there, for example, any Private Members' bits of legislation already in hand waiting for somebody to win the ballot and introduce them if the Government cannot find the time to do so?

Graeme Biggar: I am happy to pick that up first, and Rob will no doubt chip in. The Computer Misuse Act 1990 was, to be fair, updated in 2015 with some changes but, clearly, it is old. We fed into the Government's call for information a couple of years ago, and the consultation they did at the end of last year into this year, and are really supportive of a number of the changes they are proposing within that. There are some more that we would like to see happen as well, all of which are mentioned in that consultation response.

The ability to take down domains and IP addresses is in there as a part of what the Home Office was consulting on, and we would really welcome that and support it. We would really welcome the preservation of data before we go in to seize it with a court order. That is in there, and there are a couple of other things that are in there that Rob will pick up on that I cannot quite remember off the top of my head.

In terms of other issues where we think legislative change is necessary—these were identified in the consultation response; it is just that the Home Office did not feel they were quite ready to bring forward to Parliament—it is currently not an offence, or at least not an offence in a way that we can effectively use, to steal data, nor is it an offence to handle stolen property if it is data. Those are major impediments for us in being able to investigate and disrupt the crime, because data is the currency of the modern age and there is a massive value to that. To not criminalise the theft of it, or the handling of it, is just wrong. It is complex, which is why the Home Office is pausing on it, but it is really important.

The second thing we would like to push forward is extraterritorial jurisdiction. At the moment, and I am simplifying slightly, if it is not a UK citizen or someone based in the UK or using UK infrastructure, it is very hard for us to get a case taken to court. In the round, of course, the vast majority of online crime, let alone ransomware, takes place overseas and is committed by people who are not British citizens and who are not using British infrastructure. We would very much like the extraterritorial jurisdiction of the CMA to be expanded to allow us to do that in a way that many other countries, including the US, can.

Viscount Stansgate: Can you give us an example of exactly what you mean by wanting to have these powers relating to extraterritorial jurisdiction? If you found someone who you thought was guilty of something, what would you hope to be able to do under a new legislative framework?

Graeme Biggar: We could take a case to the CPS. We could get a threshold test for it to say that it would be willing to charge. We could then put a red notice into Interpol and try to get them extradited to the

UK to stand trial. For example, in February this year, we put information to the Foreign Office that enabled it to put sanctions on seven individuals who we assessed, together with the Foreign Office and the Foreign Secretary, were involved in quite serious ransomware attacks on the UK and globally.

What we are not in a position to do is have arrest warrants out against them, because they are based overseas, they are not UK citizens and they were not using UK infrastructure. That would be an example of the difference it could make. Clearly, they would need to be in a jurisdiction that would extradite them to us—and I am sure we can come on to the efficacy of sanctions—but it is an extra tool in our armoury. It is one that the US uses. They have managed to arrest someone and are going through the extradition process to transfer them from Switzerland to the US. It was a relatively major cybercriminal who travelled, so it can be effective.

Viscount Stansgate: Has the United States ever exercised these powers in respect of a British citizen who has been extradited to the USA?

Graeme Biggar: Could you repeat the question?

Viscount Stansgate Have the USA Government ever used the powers that they have to identify someone in the UK and used extradition treaty arrangements to take them back to the USA for prosecution?

Graeme Biggar: They have certainly tried, because there was a very famous case in relation to Lauri Love where it was not successful. There are probably a number of cases where they have been successful.

Rob Jones: There have been successful cases with FBI and DOJ and the classic US playbook of OFAC sanctions, sealed indictment and then a viable extradition has worked well. We can now mirror that with OFSI sanctions, our own sanctions regime. The bit that Graeme has described is that extraterritorial reach around indictments, and that is a missing part of our armoury. It is challenging because extraterritorial jurisdiction and extradition will be inherently complex, but it is something that we think is worth pursuing.

Viscount Stansgate: Did you say the Home Office has currently paused its preparations for a Bill to that effect?

Graeme Biggar: I think it is taking forward a Bill to that effect—I think, in the fourth Session—but you would have to ask them; I am not entirely sure. In all the information that came into it from the call for information, it split it into two categories. One was where it thought the case was very strong and could be legislated on straightaway, and then a second category of issues that had been raised which it thought were important but needed further work and that would go into the next Bill. I have been focusing on the ones that apparently need further work.

In response to your point about the US extraditing, I would say that we would prefer it if the US did not need to extradite because, if they were

cybercriminals who were operating out of the UK or who were UK citizens, we had the powers to prosecute them ourselves. With, for example, the first point I mentioned, the theft of data not being a crime, we are not able to do that. That was one of the most significant cases. Could I mention one final thing on legislation?

Viscount Stansgate: Please do.

Graeme Biggar: It is not so much legislation but very closely related to it, which is sentencing. The sentences for a number of CMA offences are really quite low, and then, with the way judges use them, even lower still. This matters to us in two ways. First, because we think they are just not fit for the crime. The damage that you can do with ransomware or other online crimes when you hack into individuals' or companies' systems and the amounts of money that can be stolen are really significant. We see it with ransomware. For some of these offences, the sentence would be two years maximum. We do not think that is in kilter with other sentencing.

Secondly, there are limits, quite rightly, on the covert powers we can use against people we suspect of criminality that relate to the seriousness of the crime being investigated. For a lot of those crimes, the threshold that is set is a crime where the sentence for someone who is 21 years of age or over and not previously convicted is three years. The crime needs to get a sentence of over three years for us to be able to use some of our covert powers.

For example, with targeted equipment interference, as we legally call it, or hacking, we can hack into a criminal's phone or computer only if we can get a TEI warrant, which requires the crime to be sentenced for over three years. With directed surveillance authority, even to do open-source research on someone, there are strict rules around it, and quite rightly so. If I wanted to Google the Chair, I can do that once. If I want to do detailed research online into the Chair then I would need to get a directed surveillance authority, and quite right too. You want to have controls around this—you do not want phishing from law enforcement—but I cannot even do that unless the crime has a sentence of over three years. Those are essential tools for us to be able to investigate crime overseas. For both of those reasons—the sentence fitting the crime, and our ability to investigate it—we feel the sentence needs to be increased.

Viscount Stansgate: Are there any proposed legislative changes that are, in your view, ready to go that you would support and want to see introduced?

Graeme Biggar: I have a real feeling that that is a very useful question for me to know the answer to because there must be something that I should know about, but I cannot quite think what it is, so I might have to come back to you on that.

Rob Jones: If we can, we would be happy to write to you after the session.

Chair: I think Lady Fall wanted to come in.

Baroness Fall: I was just curious to know whether it was in scope in the Online Safety Bill and whether you could use that as a device. Secondly, just around the public debate, obviously, the security versus individual debate is as old as democracy, but we have seen before in my time in government new technology coming and causing a debate. Do you think the public debate is at the point where they would see the argument straightforwardly in terms of Parliament?

Graeme Biggar: Personally, I think so. To your first point on the Online Safety Bill, there is talk and some provision around there that would help criminalise some of the theft of data, but not to the extent that we would want, so there is a link into the Online Safety Bill, absolutely. On your second point, I absolutely think the public would want us to be able to investigate and arrest people for stealing data, not just their own data but data en masse from companies. There are more difficult debates around encryption and what the right balance there is between our ability to investigate and people's right to keep their information secret, but on the theft of data I think you would find widespread support.

Baroness Crawley: Just to follow up on the sentence not fitting the crime, it is quite shocking to hear that you have to get above that barrier of three years. What discussions have been had with the Ministry of Justice about this?

Graeme Biggar: I do not think it is shocking, honestly. I think it is important that, for the use of covert powers against the public, there is a threshold and three years fits for the vast majority of crimes that we would want to be investigating. It just feels that this one is a bit of an outlier. To me, it is more changing the sentence for this particular crime rather than reducing the threshold from three years, although that is a Home Office and MoJ decision. We have discussions all the time with the MoJ about sentencing. We have fed our views on this particular aspect into the consultation on the Computer Misuse Act and the Home Office is taking that forward with MoJ.

Clearly, it goes into quite a complex set of arguments with the MoJ, because, as you will know, the prisons are pretty near full, close to 80,000, and so it has to think very carefully about the opportunity, cost and the choices that come with increasing sentences for some offences. At the moment, the number of people who have been convicted of these offences is pretty small and I do not think we would make much of a dent on the prison population but, rightly, it has to factor that into its calculation.

Baroness Crawley: When you say pretty small, what are we talking about?

Rob Jones: CMA offences will be low hundreds. It goes to the heart of the challenge in that the legislation did not envisage the digital age we now live in or the exponential growth in threat as well as the success of

the internet. That was not what sat behind the CMA. It was people stealing each other's passwords and doing stupid things on computers. It was not elite Russian-speaking actors targeting the UK and extorting millions of pounds, so the two things just do not square.

Baroness Crawley: Thank you.

Chair: Mr Graham, please. We seem to have lost the line to Mr Graham. Mr Graham, are you able to ask a question?

Q57 **Richard Graham:** I am, and I do apologise, Chair. It is, as a colleague mentioned already, very gracious of the two distinguished guests to come back to us after our recent, incredibly helpful visit. The questions I would love to ask you a little more about are more on your operational achievements and challenges. There are different ways of expressing them. My first question would really be around whether you think the Government have focused too much on the UK's resilience against ransomware attacks and, perhaps, not enough on response and recovery. What level of support do you think is right for a small or medium-sized enterprise somewhere in the country if they are attacked by a ransomware group?

Graeme Biggar: I am not quite sure how to answer that question really. Not far from your constituency, of course, a local authority has, indeed, suffered. The main point would be that it is so much better if they are not attacked in the first place, which goes back to the balance between resilience and disruption. Fundamentally, we are a law enforcement agency; we investigate crime. When we step back and think about the best ways of trying to reduce the harm that comes from crime, stopping it happening in the first place has to be better, so I would expect and argue for a really strong focus on resilience.

Chair: If they were attacked, would it come to you?

Graeme Biggar: If there was an attack, yes. If it is reported and reported as a crime, it would come to us. It is a complex picture. If there was a data breach, then it should be reported to the Information Commissioner's Office. Many attacks are reported to the National Cyber Security Centre, part of GCHQ that works really closely with us, and which you visited on the same day you came to us. It can also be reported to Action Fraud, which sits under the City of London Police, that, again, works really closely with us.

There are occasions when organisations will be attacked and report it to either the National Cyber Security Centre or to the ICO and ask for law enforcement not to be told, which is kind of unhelpful. By and large, when the system works, which it does most of the time, if there is a report coming in, then it will be shared among those four organisations—if the ICO is involved—and then we will work really closely with NCSC on the response.

The National Cyber Security Centre will work on trying to stop it getting any worse and on recovery; we will work on supporting the victim, as we

would on any crime, and the investigation that goes with it. Between us, we have a really quite strong understanding of how to stop attacks getting worse and how to manage the repercussions from them, so we would provide that support to the company or organisation.

Richard Graham: Director General, can I push you a little on that? We all know the reality of the strength of attacks that are coming and that the strength of defences, certainly in the case of most small and medium-sized enterprises, is not going to be adequate for preventing a serious cyber hacking attempt. From my own experience, which you obliquely referred to, with Gloucester City Council, I do not see a way in which local government at the second tier, possibly not even at the first tier, let alone much smaller SMEs, without government assistance are really going to be able to be sure that they can prevent such an attack by having strong defences. Are you really suggesting that there is adequate expertise to ensure that basically no one in the country will be hacked by a ransomware group?

Graeme Biggar: No, I was not, and I would not. I am sure Rob will give a better answer.

Rob Jones: Thank you. I completely understand the question. What we all need to reflect on is that some of these attacks—even though they may be linked to sophisticated state actors—exploit very basic vulnerabilities. It is not so much what an SME can expect post-attack as what they should expect to prevent attacks. Basic cybersecurity and basic tradecraft will prevent many of these attacks.

What we typically see when CIR companies are engaged and NCSC works with victims is that there is a very basic vulnerability—an unpatched vulnerability that has been exploited, a phishing email that has been clicked on. That is not to blame anybody who is a victim of cybercrime. It is not; it is just the situation that we find ourselves in. People need to engage in good cyber hygiene, cyber essentials, basic standards. If you are engaging cyber insurance, then you should be expected to have a minimum standard of cybersecurity.

Unfortunately, many of the companies that fall victim do not have that and there is quite a sorry tale of basic vulnerability being exploited time and time again with these attacks. You are always going to have very sophisticated CNE where state-level actors are sitting on networks. You would not expect an SME to defend themselves against that, but some of the affiliates we are talking about are using pretty straightforward tactics around social engineering, email compromise and compromised credentials to attack some of these victims. We need to engineer as much of that out as we can pre attack.

If you are attacked and you are in the middle of an incident and you engage the NCSC, you will get access to a good CIR company and the ability to mitigate that attack. However, once you are in an incident, you have lost your own destiny and that is why the emphasis on resilience is so important. No resilience strategy is 100% effective. Some attacks are

going to get through and, obviously, that is where we and the NCSC become involved, but there is still too much that is not done to understand the vulnerability. This is mainstream business as usual. It is not something left at a desk where you do a bit of cybersecurity when you think you might be vulnerable. It is just part of e-commerce, part of business, part of running an email account.

Graeme Biggar: Also, once you are attacked, it is tough. Could we get better in helping local authorities or SMEs when they are attacked? Absolutely, but, as we know from the Gloucester experience and lots of others, once you have been attacked it is a long, hard road to recovery and it is expensive.

Richard Graham: Yes, and, of course, both of those things lead to something which this committee has discussed before with different representatives of the Government, which is whether, at least for local government entities, we should consider doing what we did for flooding, which was to create a Flood Re. Therefore, in this case, it would be a cyber re where, in effect, the insurance sector provides the funding to enable people to be insured so that we do not see local government entities or any other branches of government in effect going bankrupt when dealing with the costs of rebuilding all their servers and so on. What are your thoughts on that?

Graeme Biggar: I have not seen that proposal; that is quite interesting. Certainly, I think the insurance sector could play a bigger and more useful role in trying to prevent cyberattacks happening in the first place. Lots of companies now have cyber insurance. It is a developing market; it is not yet as effective as we would like it to be. One advantage from that, I hope—and Rob can add to this—would be increased reporting.

I mentioned in my very first comment that it is quite hard to answer various questions around ransomware because of the patchiness of reporting. If you report your bike stolen or your house burgled, your insurance company will ask for a crime reference number. If we could get into that position with cybercrime and ransomware where people are insured, be that normal insurance or a cyber re like flood as you were talking about, and we could make part of that typical reporting into law enforcement, that would enable us to have a much better picture of the overall threat and, therefore, a better response to it.

Richard Graham: We have raised the issue with the Minister for the Cabinet Office and we need to follow up on that. That is an issue for us and the Government, but it is encouraging that you recognise that a cyber re could have a role to play. Director General, earlier I think you said that a case would be referred to local police or regional units. Are you comfortable that constabularies across the country have the expertise to be able to deal with all the different aspects of this? At what stage are they likely to bring you in, realistically?

Graeme Biggar: Rob has been all over this, so I will let him answer.

Rob Jones: There is a national system which, obviously, the NCA sits at the top of with the City of London Police. There is then a regional network and growing capability in forces. If a victim reaches out to a force or to Action Fraud, they are going to get a basic level of service around what they see in front of them. If that incident escalates and it is a significant data breach, or there is a ransom demand because of encrypted data, that will pretty quickly be escalated to regional organised crime units. If it is one of the prioritised ransomware strains that we are concerned about, because we prioritise them in terms of threat, harm and risk, we will either be dealing with that, calling it in to the NCA to deal with the level of capability that we have, or working with the ROCUs for the safest and lowest-harm resolution to that incident.

What does that mean? We will treat it as a crime in action. It is a live extortion, trying to get money out of an innocent member of the public. All the tools that we would use in covert law enforcement will then be brought to bear, because those offences, absolutely, would engage legislation which gets you a minimum of three years. Every tool in the toolbox would be used to try to resolve those incidents, including technical surveillance and a range of other tactics that are available to us.

It would escalate from the report of that incident, depending on what it looked like. Over the years, the response locally has not been as good as it should have been, and I think national policing would be the first to accept that. That is linked to the online fraud response, because some of this is cyber-enabled fraud. But the system has matured and what we now get is—to reassure the committee—cases being escalated through the ROCU network to the NCA, and we get work coming down from the NCA into the regional organised crime units.

Richard Graham: That sounds like an implicit if not an explicit agreement that all of us could probably do more to try to upskill both the constabularies' response as well as the likely victims' defence mechanisms. What about the handling of a hack or a ransomware hack? Certainly, in the case of my city council when it was hacked, one of the difficult issues has been that the agencies, quite rightly, for reasons of wanting to focus on disrupting the hacker, were reluctant to allow the local council to say a great deal. In fact, it was only very recently that they announced publicly that private data had been accessed and stolen, although not—as we all still continue to hope—released into the public domain.

Do you see that as a likely continuing trend on the basis that the agencies will want to explore in as much detail what has happened, perhaps in order to help disrupt the attacker, at the potential cost for some people of being unsure as to whether their data is being held by people it should not be?

Rob Jones: Each case is assessed on its merits. The reality is that, with some of these incidents, we know we are not going to be able to identify the actor behind it in a jurisdiction where we can go and arrest them or take disruptive action. My language around the safest and earliest

resolution to the incident is exactly what we are trying to do. We are trying to protect people's data, allow recovery, allow a CIR company to work with the victim, and get people back on their feet very quickly because, ultimately, if we do that, then the extortion model fails. The extortion model works only if you have leverage over the victim.

Quick recovery and being able to talk about it publicly is a great way of disempowering the attacker. Where we can, we will talk about it, but there are some cases where we will counsel victims against public communications, because you cannot get involved in resolving a crime in action and using covert tactics if you are also speaking publicly to the adversaries about that.

Hacker leak is different. The way the business model has changed from a classic ransomware attack is if data is being published and it is out there, and members of the public can see it out there. You have seen some of this play out in the media recently. Then, where we can, we will help victims to talk about that, as will NCSC, and engage their statutory responsibilities in terms of reporting to ICO and elsewhere. It is not a blanket "You can't talk about it", absolutely not.

Richard Graham: I get that. Director General, do you want to come in on that?

Graeme Biggar: You said I gave an implicit answer to a question earlier on and I can give an explicit one if it is helpful, which is about whether we have the right skills in the right places, and whether we need more. Just to be really clear, government has funded the establishment of regional cyber teams alongside the regional organised crime units as well as a capability in the NCA, and that is really important. This is still relatively small; we are talking 250 people in the National Crime Agency and 300 spread around the regions. We would not expect each of the 43 territorial forces, with the exception of the Met, to build up their own really significant capability to deal with major ransom attacks. Do they need to develop their digital skills and their cyber skills, with a small C, to deal with the massive push into online crime? Yes, they need to do that, but I would not expect Gloucestershire Constabulary to have a big capability, or any capability really, to respond to major ransomware attacks. That is for the regional tier that we work really closely with, and then for us.

Richard Graham: That is very helpful. The replacement for Action Fraud is being provided, in part, by Capita. It, of course, recently suffered a pretty substantial attack itself. Does that rather affect the credibility of the reporting mechanism?

Graeme Biggar: I do not think so. We all need to be worried about cyberattacks. I am not sure Capita is any more vulnerable than the rest of us. The City of London Police is running the programme to bring in the replacement to Action Fraud. We are all really looking forward to it. It is really important because there is a system there that people have worked really hard to sustain, but it has not provided the level of capability that

we needed to understand and then help respond to the massive increase in online fraud that we have seen. From our point of view, it is really important that we get behind it and help make it a success.

Richard Graham: Lastly, just on the Conti group—because that, of course, has hacked into so many people, including Gloucester City Council—what level of confidence do you have that data will not be released by elements of that group now that you seem to have successfully dismantled it?

Rob Jones: We are not complacent about that at all. It is an ongoing effort against affiliates of and the core of that group. We continue to monitor what they do and work against them. The reality is they have compromised so many systems and taken so much data that that risk still remains.

Graeme Biggar: Rob will correct me, but we have disrupted that group rather than utterly dismantled it. That was the example I mentioned earlier, with seven members of that group being subject to the very first cyber sanctions from the UK—in fact, from any country other than the US. Elements of the strains of Conti have appeared in other ransomwares and members of what was the Conti group have appeared in other ransomware groups, so we have disrupted rather than dismantled it.

Richard Graham: Thank you very much and, Chair, with apologies, I may have to leave this meeting quite soon. Thank you.

The Chair: Thank you for telling us.

Q58 **Baroness Fall:** Thank you for your time. We understand that there are strong links between the Russian state and ransomware, and we have spent a bit of time already talking about prevention, resilience and even insurance in the face of a state-enabled adversary. Do you think it is credible to prioritise prevention, especially as they are often private sector victims, as it were? Are we getting the balance between the micro criminality against normal citizens or businesses being attacked versus a more systemic approach and reaction to that? I include in that the capacity to disrupt ransomware operators.

Graeme Biggar: It is quite hard to distinguish state-backed attacks from criminal ones. There is a spectrum of state complicity from Russia in the various different ransomware groups. There are a few that seem to be quite closely linked with the Russian intelligence services, and all the rest are at least tolerated there. We were concerned, in advance of and immediately after Russia's invasion of Ukraine, that there would be a spike in state-directed ransomware attacks against critical national infrastructure here. We saw that in Ukraine, obviously, but we did not see it here. What was quite striking, as the director of GCHQ has said, was the lack of success the Russians had in attacking Ukraine from a cyber dimension. That was due partly to fantastic work by the Ukrainians themselves in improving their defences but also to the support of a

number of countries, including the UK. So the first point is that there is a spectrum there.

Your second point was whether we get the balance right between defending against those big state-sponsored cyberattacks and lower-level criminality. I hope so. Certainly, very significant and senior government attention was clearly focused on the risk of acute attacks on critical national infrastructure. That is what got people's attention. That is the thing that could have made a real difference to the country in a macro setting. Of course, we are seeing cyberattacks of many lower kinds, including online fraud, as Rob alluded to earlier, that are hitting people all the time in many ways. They are very damaging to them individually but also to people's confidence in the digital economy, so it has a macro impact too.

As I said, that is the shift that we in the NCA and the system as a whole need to make in a bigger way than we have so far to deal with that online criminality. It is an absolutely fundamental part of our strategy. We have looked at the way crime has changed and at our place in dealing with it and decided that we need to be moving upstream overseas and online, as I mentioned when you came to the NCA. By "upstream" I mean the controlling minds, the enablers and the infrastructure overseas, self-evidently, and online is very pertinent to this committee. We need to get better at doing that.

We have already been quite successful. If it would be helpful or if you have questions on it, we can talk through our ecosystem approach to tackling both cybercrime and online fraud. In brief, we absolutely still go after the main individuals and adversaries when we can identify and de-anonymise them, because obviously they try to remain anonymous. We are also looking to try to tackle the ecosystem that they depend on—the goods, services and infrastructure that enables them to undertake their crime. We have broad agreement across the Five Eyes that that is the right approach, and we have had some pretty strong successes in taking elements of that infrastructure out.

Baroness Fall: Do you think the FBI has been more successful than the UK at disrupting ransomware and, if you think that is a fair assessment, why?

Graeme Biggar: I will let Rob come in because he will be champing at the bit. Yes, it has been much more successful than us for two reasons. It has invested in it more than we have as a country and we have as the NCA—mea culpa. Also, its legal framework makes it easier for it to do that. There are other players in the US system too, not just the FBI. We have been involved with the FBI on some major investigations and take-downs, and on too many of them it has been the FBI in the lead and us supporting. We would like to be in a position where the FBI comes in to support us.

Baroness Fall: The legal framework being?

Rob Jones: We touched on it earlier. It is that range of tactical indictments.

Baroness Fall: That is really good to know. I want to come back to what you said about Ukraine. We were advised that the NCA accompanied Ukrainian police on raids in mid-2021 and January 2022. Could you tell us a bit more about what you learned from that experience?

Graeme Biggar: I am trying to remember what raids those would be.

Rob Jones: In terms of working with international colleagues and the Ukrainians, there has been a lot of investment in underpinning and developing their capability. The point about Russia-Ukraine is that Russia unashamedly emptied the tank against Ukraine in the run-up to the invasion. Ukraine has shown that resilience can work if you do it right. Of course the Ukrainians have suffered, and they have suffered terribly from the conventional kinetic effect of the Russian war machine, but they have done very well on cyber recovery and resilience because of the international help they had. Nobody should be complacent about that, but it means that the balance of investing in resilience alongside the capability to hold people to account is not wasted.

Ultimately, you still need to be able to extend your reach and go after the people causing this. That is why the range of options around sealed indictments, sanctions, criminal infrastructure and the ecosystem that we can take down with state-level capability and law enforcement capability is really important, because it is an international threat. Investing in resilience so that you can look at your adversary and say, "Do your worst", is a really important part of the story.

Graeme Biggar: I still cannot quite place what that raid would have been, but I would add that we have also investigated people in Ukraine. Before the war, Ukraine was absolutely one of the countries, alongside Russia, where cybercriminals were based. We worked with the Ukrainian authorities in trying to investigate and arrest those individuals. That does not seem to be happening now: some of those people who were based in Ukraine have gone to Russia and some of them have turned to attacking Russia. At the time of the invasion, we had some 13 investigations or warrants out on individuals in Ukraine. We work very closely with the authorities and the population has, largely, been onside, but it has harboured some criminals too.

Baroness Fall: You talk mostly about Russia as the state adversary, but are there any other states? I think specifically of China, but are there others where you are beginning to see a bit of cyber ransomware?

Graeme Beggar: There are three in particular, and Rob will pick that up in more detail. China is absolutely the most significant cyber actor, spending more on cyber capability than every other country combined. So far, it has tended to use its capabilities for state espionage and theft of intellectual property rights rather than ransomware attacks. We in the NCA have had less to do with that threat because it has not manifested in

a purely criminal sense, but the capability is absolutely there and it is massive.

North Korea has used cybercrime, largely just for straight thefts. The Lazarus Group, based out of North Korea, has been quite successful in doing that, increasingly in stealing cryptocurrency. The third country that we have had dealings with is Iran, which also has an impressive cyber capability and has used that for actions that are on the bridge between crime and state espionage.

Rob Jones: Graeme has covered most of it, but the most interesting comparison in terms of cybercrime is North Korea. If you are a pariah state looking to bring currency in then crypto assets are perfect. One of the things about international sanctions biting is that what North Korea did was very clever in bringing in revenue from crypto assets. That was a well-trodden path. Of course, the unintended consequence of some of that activity was very significant internationally. That crossover remains and will continue. It is sometimes very hard, on any given day, to define what is state sponsored, what is state affiliated, and what is state activity.

The Chair: Just a slight sidestep, if you do not mind: you mentioned Ukraine. Is there any evidence that British support for the war in Ukraine has caused an increase in attacks against us?

Graeme Biggar: No, not that we have seen. We really worried, as a security community, that it might. We have not seen that happen yet.

Q59 **Lord Sarfraz:** Gentlemen, your agency does such incredibly important work, for which we are very grateful, but are you able to pay your personnel competitively, particularly in cyber, compared to, say, policing? If not, how do you go about recruiting and retaining the very best talent that you are after?

Graeme Biggar: That is a challenge for us. If you ask the police, they would also say it is a challenge. It is a challenge across the public sector to be able to recruit and retain skills in relation to cyber or digital work in the round. We are at a bit more of a disadvantage in one sense in that our pay is typically lower than policing, so that makes it a bit harder to recruit. However, we provide the most amazing opportunities to do exciting work that makes a difference. The mission, and the passion people have for it, sustains them through slightly lower pay.

Some people leave to policing and more people will leave to go to the private sector where, instead of it being a five or a 10 grand difference, they will double or triple their salaries on leaving. That is a continual challenge for us and, frankly, we are never going to be able to match the gap to the private sector. We would like to be able to match what is paid across the rest of the public sector; we really should get to that point. We have to depend on the training we provide and the passion that people can have from working on the mission.

Lord Sarfraz: The agency is still able to retain exceptional talent, given

that both of you are still here. Could you just clarify how many people work in the National Cyber Crime Unit, and how much time are they spending on ransomware? How does that compare to operational partners such as the FBI?

Rob Jones: There are in the region of 250 people working in the National Cyber Crime Unit. The priority, in terms of what they are doing day-to-day, is ransomware. On any given day, they will be working on data exploitation and a range of different activities to support those investigations. Other issues come up in terms of hack-and-leak, or incidents where you need cyber skills to resolve them. From time to time, we will get involved in other attempts to extort people that are not classic cybercrime.

On that, one of the things we have tried to do with policing is preserve cyber specialists to do the higher end of that, and increase the overall digital literacy of investigators. That is also what we are trying to do in the NCA, because we need to maintain those specialists—you have seen some of them in action—who are very talented and who have these skills. We cannot afford for them to be called on for every challenging digital investigation. We need an overall upskilling of all investigators in digital investigations because they are so mainstream. The majority of their time is spent against the ransomware threat and their data activity. That is complemented by activity that the FBI and others do, and partners in the UK—GCHQ and elsewhere.

Lord Sarfraz: Do you feel you are effectively able to recruit individuals who are out of the box who would not usually be law enforcement candidates?

Rob Jones: That is one of the strengths of the NCA: we have coercive law enforcement powers but we are civil servants. We are a very broad church in terms of background. That is good; that is a real pull factor. You do not have to be a police officer to join the NCA. You do not have to have coercive powers but you can have them, depending on what team you are in. That is good, and everybody gets behind the work and the mission. Graeme covered the points in terms of where we need to get to.

Ultimately, we need more permeability with the private sector, because everybody needs cyber specialists and digital skills. The days of people coming in and doing a 30-year career in one Government agency are probably quite rare for a lot of young people now; they have different aspirations. We probably need to get to having the ability to recruit at scale, allow people to go out, get different experience, come back in and recontribute. A fair bit of work is needed to achieve that objective.

Graeme Biggar: One example of our ability to recruit is that the new DG Threat—one of the team that sits just beneath Rob—is James Babbage, who is coming in next week from being commander of the National Cyber Force, the joint MoD/GCHQ offensive cyber team. There is no heavier hitter in the world of cyber. He was very keen to come and work at the

NCA because of the work we are doing and the opportunities we have. That is a great sign of the attractions there can be in the NCA.

Rob is, of course, right that an awful lot of the National Cyber Crime Unit's business is on ransomware. Part of that is on the ecosystem approach that I mentioned, which is very relevant to ransomware but as relevant to online fraud and various other crimes. It is not all on ransomware but it will all be related to ransomware. It is not just the NCCU. There will be other capabilities across the NCA that contribute to this, such as our international network of 150 people around the world who work with all the other countries, including with the FBI.

Rob mentioned that we are building up a new team on cryptocurrency. Ransomware does not work unless you can pay the ransom; you do not pay it in cash, so it has to be cryptocurrency, so building up our expertise around that is really important. We are doing some of that within the NCCU and some of it outside. All the 250 are not purely doing ransomware, but it is not just the 250.

Q60 **Lord Dannatt:** The Russian Conti group has been mentioned a couple of times this afternoon already. If I am right, your agency announced in February the sanctioning of seven ransomware criminals linked to the Russian Conti group in a joint operation with the US. We are told there are those—such as RUSI, which is represented here—who are sceptical about the effectiveness of sanctions because ransomware groups are able to rebrand and develop new strains to evade sanctions. What do you expect to be the impact of sanctions? Are sanctions a useful weapon?

Graeme Biggar: We prefer to arrest them and put them in prison. I am not saying it is the—

Lord Dannatt: For more than three years?

Graeme Biggar: Absolutely. Given what is possible, we think it is a useful tool. Rob might say something—not just on what we did with Conti—about the very significant investigation he led which concluded about two years ago into the ridiculously titled Evil Corp. That resulted in sanctions, not from the UK but from the US. We can talk about the impact of that.

Rob Jones: Any sanctions effort is a slow strangle, not a killer blow. It needs to be a complementary measure for other things. People are rightly very cynical about whether sanctions will have an impact, but we have seen real world consequences when they have been used. We were very keen on the UK sanctions regime and getting that off the ground because of our experience with American colleagues and OFAC, and the work we did against Maksim Yakubets and other elements of the wonderfully titled Evil Corp.

Publicising them, calling them out, restricting their travel, and preventing their being able to spend their money and travel round the world starts to bear down on the incentives for criminality. This was a guy driving around in a Lamborghini who had a tiger as a pet—as you do. For that

type of gangster lifestyle, it matters to those individuals whether they can travel, spend their money and access a western lifestyle. It is not trivial; it does have an effect. Unfortunately, most of that measurement of effect is classified because we collect it through classified sources, but we are content that that effort made a difference. We also believe that the effort against these other groups will make a difference. It is just one element of a toolbox that we need to use.

Lord Dannatt: That is very helpful, and your earlier points are very relevant too—that you wish the legislation to be tightened up to more than three years. I have got that point entirely. Thank you.

Q61 **Baroness Fall:** We talked a bit about international operations, so I want to come back to that on the US and others. Are there any other things you could do to make those international joint operations more successful? Leading from that to a point I raised earlier about when it crosses from being criminality to national security, to what extent are we preparing, or do we need to prepare, for this sort of attack as a national security issue, with possibly even a G7 response? The G7 is working quite hard on economic security at the moment. Your list of Russia, China, North Korea and Iran do not turn up to the G7, so I am keen to know more about that.

Rob Jones: The UK has invested in the capability to prepare for that type of issue and attacks on critical national infrastructure. The real vulnerability is where there are companies or services in the supply chain supporting very important services that equate to critical national infrastructure but do not receive that same level of protection. This gets into that conversation we had earlier around good resilience. Companies that are growing and becoming more ambitious, and are in the mergers and acquisition stage of their growth, become vulnerable because they take on legacy infrastructure and technical debt that creates vulnerability. We need to hold on to that resilience point with those companies, as well as worrying about the obvious critical national infrastructure and national security issues that we talked about.

As to when you cross over from crime into state-level activity, the escalation there, together with the support and the leadership from UKIC in relation to it, is a well-trodden path and well laid out. Where we operate in the overlapping Venn diagram with people who are doing both, again, we exchange information and tradecraft in relation to that. If we are tackling one of those groups that is a real priority we can engage all of the national security infrastructure that you would expect in the UK. That system comes together to prepare for the worst and to try to confront the individuals involved in it on a day-to-day basis.

Baroness Fall: Can I just come back on the very interesting point you made about this not so much grey area but group of targets that are not quite national security but just below and maybe even transitioning from one to the other? Are you confident that you have your eye on that and that there is a resilience package around it?

Rob Jones: Those are the people who are the highest priority for us because they are the individuals—the elite—who created the business model which has now got out there and been industrialised with the affiliates model. They are the people who accelerate the threat and have access to coders and infrastructure. They are top of the list.

Graeme Biggar: Just on your point about international co-operation generally, this is never going to work in the way that Interpol can for some crimes, where you can work with most countries. Some of the countries are adversaries. We have a pretty tight relationship with the Five Eyes. Our head of the National Cyber Crime Unit was in Canada the week before last with them, and I discussed it in Australia last month. It is a big focus for all of us. Within the Five Eyes, we are all focused on the ecosystem approach to try to reduce ransomware and cybercrimes.

However, it is not just the Five Eyes. There is some really good co-operation through Europol and with European nations. The Germans, the Dutch and the French have all invested in this and they are good at it. Europol has too: the EC3 grouping and capability can be really effective. When we take down some of that ecosystem and the infrastructure and put splash pages up to say, "You've been hacked by", you will see that it then says the FBI, the NCA, all the different European partners and Europol.

Can we do more international co-operation? Yes: we need to build more capability and get those relationships tighter, but it is a pretty joined-up response now across like-minded nations.

Rob Jones: Crucially, if we find infrastructure in any of those countries which are friendly then there are obvious opportunities with the agencies that we work with.

Q62 **Baroness Crawley:** It is very good to see you both being so candid and helpful with your answers this afternoon. Mr Biggar, you said at the beginning of the afternoon, "We don't get the majority of attacks reported in". Indeed, witnesses to our inquiry have suggested that the UK response to ransomware is hampered by this lack of data and of intelligence. The Government have acknowledged that too. Should UK victims be required to report an attack, potentially to some central body? Would that be a good idea?

Graeme Biggar: You are absolutely right that we are hampered by the low level of reporting. We would love to see it increase and we really want it to. I will directly answer: I am struggling to think of a crime where you are required, by law, to report that you have been a victim. That would feel quite a strange thing to do. I would link it to my earlier answer to the point about insurance; that is a better mechanism: encouraging people to have insurance.

The Chair: The insurance companies require it.

Graeme Biggar: Yes, the insurance companies could then say, "You need to get a police report". That would be more in line with British

society and the way we normally work, rather than legally requiring people to report the fact they were attacked. They are, of course, legally required to report to the Information Commissioner's Office if they have had data stolen. Rob will correct me if I get this wrong, but I do not think the ICO is required to report to us if there has been an attack.

An element of it is that there is already mandatory reporting, but we would not sit here and say, "We would like legislation to mandate people to report if they've been a victim of this particular crime". It would also beg all series of questions about how you define this crime. This is a point I just want to make to the committee: your report started off on ransomware being defined as the encryption of data. As I said, that is one manifestation of a crime that is evolving. We need to keep an open mind on it and not restrict ourselves too much, as it will change. If we put mandatory reporting in place, it would be, "Well, on what exactly?" It would depend how we defined it, and then the problem would move on. Was that a sufficiently direct answer?

Baroness Crawley: So there has not been a great deal of enthusiasm for that approach in your conversations with Government on this.

Graeme Biggar: There is enthusiasm for encouraging there to be more insurance and getting reporting to increase significantly as a result; we just need to make it happen. There has not been much enthusiasm within Government, and we would not share it, for mandating and legally requiring people to report that they had been the victim of a crime.

Baroness Crawley: Thank you. Do you recognise the Government's estimates that only 2% to 10% of cybercrimes come to the attention of law enforcement? Would that be a proper reflection of the situation?

Rob Jones: It would be at the high end of that, but there is a definitional problem that everybody grapples with when you talk about cybercrime. Some of that is almost certainly going to be fraud and cyber-enabled fraud, and the crossover between fraud and classic cybercrime is such that you cannot really draw that distinction anymore. Increasingly, we are talking about a digital environment where people are being exploited via a range of different tactics. Those figures would not surprise me, but I would expect it to be at the higher end.

Graeme Biggar: I would strongly suspect, but I do not know—I should know—that that figure is calculated by looking at the figures in the Crime Survey for England and Wales on Computer Misuse Act offences. That is the survey that the ONS does when it goes around and asks, "Have you been the victim of any crime at all?" In the last quarter, 3.7 million people said they were the victim of a fraud and 1.6 million said they were a victim of hacking of one sort or another. For the vast majority of those there would have been no loss; they just think something happened, so there will not have been a problem.

I do not know the figures for the CMA well enough, but for fraud at least, for 1 million of that 3.7 million, no fraud took place; someone just sent

them a text saying, "Your parcel's been delayed", and they did not act on it. For another 1 million of that, there was a fraud but then the company repaid them, so the individual did not report the crime. We need to be quite careful in looking at the figures: 2% might sound shocking, but the vast majority of that—98%—will have been no crime or nothing material. What we need to be worried about is serious ransomware attacks that happen and are not reported to the authorities. We know some of those happen, so we are really worried about this, but it is not going to be 98% of them.

Q63 **Lord Sarfraz:** Should we just go ahead and ban ransom payments and say, "You're not allowed to make ransom payments"? What are the pros and cons of that approach? Would it make us any safer? We have heard from victims who felt they had no option but to pay the ransom; what other options might they have?

Graeme Biggar: Before Rob starts, I just need to warn you he could write a PhD thesis on this subject.

Rob Jones: It is, of course, a very good question that is being debated a lot as the ransomware threat has increased. We will no doubt keep returning to it. There are several things about it in terms of pros and cons.

First, the extortion model that we are tackling with ransomware manifests itself in lots of different crime types. Once you start creating legislation where you are effectively criminalising the victim of a criminal attack, be it for kidnap and extortion or ransomware, that is not a path that any of us in law enforcement really want to tread for lots of very good reasons: you are criminalising the wrong part of the equation and doubling down on the impact on victims of crime. You start there and then try to work through how you would actually make that legislation work.

When we get involved in these incidents with policing, partners and victims, we seek the lowest-harm resolution to the incident. We do not want to be constrained or painted into a corner by something that could do more harm than good. It could be that, under some circumstances, a ransom payment is the only way out for a company—an SME—and it could be that is the only way to potentially flush out a suspect. A range of things play out in these investigations, and each one is different. Blanket criminalisation of payment does not appeal to me for those reasons, but we do need to bear down on payments.

We have talked a little about the insurance industry already and about resilience. It is about basic levels of resilience and making sure that, if you engage an incident management company or an insurance company, people do not just sweep up the glass and move on. If you get hit by one of these attacks and you pay a ransom, you should act responsibly, report it and engage with law enforcement on that payment. We will never be involved in the payment of a ransom, but if an individual company decides to pay to resolve the incident they are not criminalised

by doing it. If it leads to the resolution of the incident and a reduction in the harm, and you can then move on to pursue the criminals behind it, that is a way out of that incident.

As we are all trying to get better at this and look for ways that bear down on the problem, we need to be careful that we do not paint ourselves into a corner with a policy or legislative solution that reduces the tactical options that we have when we deal with one of these. To be clear, we do not want people to pay ransoms and we will never advise people to do so, but you can never say never.

Lord Sarfraz: Do you have any other examples of what a victim could do other than contact the insurance company or pay the ransom?

Rob Jones: Back up your data and engage in all the things we have talked about during this hearing. Ultimately, extortion works only if somebody has leverage and there is a power imbalance. If it is encrypted data and you have your back-up and you can get back up, the opposition is very likely to resort to hack-and-leak as the next stage of that extortion. If you report and act responsibly, you will be supported in the mitigation of that hack-and-leak. If you have a back-up, good cybersecurity and good basic cyber hygiene, you have a way out.

Too many people are forced straight to considering paying a ransom because they see their company effectively bleeding out because their data is locked, they cannot decrypt it and there is an economic consequence. They look at the trade-off and say, "Well, we are losing £1 million a day, £10 million a day; why not pay?" The basics can help get you out of that.

Graeme Biggar: To bring it to life with an example, that is what Royal Mail did really well in January when it was attacked. That was big news. From our point of view, Royal Mail was an excellent victim. It would prefer not to have been a victim but, once it was, it did everything right. It reported to us and to the NCSC. It decided pretty early that it was not going to pay a ransom. It threw a lot of resources at trying to reinstitute its systems and set up back-up systems, but it engaged with the ransomware actor and effectively strung them along to the point where it had a back-up system in place. Royal Mail played it really well. Was that disruptive? Absolutely. Was it expensive? Did Royal Mail lose customers in the long run as people moved elsewhere? Yes, but, given the situation they were in, they played it very well.

Lord Sarfraz: For an SME, which might not have those resources to pay into bitcoin, a ransom payment is done and over with, so in some cases it might make sense.

Graeme Biggar: Or is it over with? That is part of the advice we give: you can pay a ransom and that does not mean that your data is safe or you get the encryption key. Sometimes you do, sometimes you do not, but you are always going to hold that risk. We have been over this debate many times internally and with Government about whether we

should criminalise ransoms. At the moment, we sit on the side that says you should not.

The one exception to that that we should mention is on sanctions. We sanctioned Conti, or at least individuals within Conti, so it would be unlawful to pay a ransom or transfer money to Conti now, which is a reason why we need to be quite cautious about the number of ransomware groups that we put sanctions onto.

Viscount Stansgate: I will come to the question I want to ask about resilience, but I remember raising this when we came to see you: there is no guarantee that you pay up and either get your data back or get it encrypted, or that they do not put it out there for everyone to see. Do you try to keep some sort of track of how many times that type of thing occurs?

Rob Jones: Yes, we do. We learn from those incidents and we play them back into our engagement with victims during live incidents, as does the NCSC. You are absolutely right to call that out. You are dealing with criminals, not honest people. The idea that you will solve your problem by paying a ransom and that that will be absolute is just dumb; that is not the case. However, we recognise that some of these incidents are really complex and sometimes people have paid because it has been their only option.

Graeme Biggar: Just to be clear, the data shows that, most of the time, if people have paid the ransom, then they get the key back or the data is not exposed on the open web. If the criminals always took the money and then did exactly what they said they were not going to do, no one would pay the money anyway.

Rob Jones: It is a balance.

Graeme Biggar: They have to play ball enough to make their ransom credible, but there is absolutely no guarantee.

Q64 **Viscount Stansgate:** Moving on to the question I want to ask about resilience: despite the focus of UK agencies on securing critical national infrastructure against major cyberattacks, we have been told that many infrastructure operators remain vulnerable to ransomware. The Government have resisted imposing stronger regulatory standards on those operators. Would you like to see stricter cyber resilience requirements imposed?

Rob Jones: There is quite a lot of complexity in the picture that you describe in terms of the definition of CNI and the level of investment in the protection of those systems. The NCSC and the Cabinet Office have worked very hard to protect the systems that matter, and they are well-protected. I would be more concerned about the companies that get involved in the supply chain and the long tail behind that, so understanding the small company that, because of mergers and acquisitions, has become much more significant in supporting something

that is important to UK plc. That area is probably worth a second look, but I am sure the NCSC would have something to say about that as well.

Viscount Stansgate: Tell me if I am wrong, and I apologise if I am, but take the MOVEit software, which was involved in the recent exposure of data, ranging from Boots to British Airways and so on: is it that type of vulnerability that you have just been referring to?

Rob Jones: Yes, and vulnerabilities like that. We talked about unpatched vulnerabilities and doing the simple things very well. The learning from attacks like that is played in quite quickly, but people need to pounce on that to absolutely make sure that they will not fall victim to a similar sort of attack. That is the type of thing that can creep up on organisations.

Viscount Stansgate: Can you help them pounce?

Rob Jones: Yes.

Q65 **Baroness Crawley:** Following on from learning from attacks, we have been told that technology and telecommunications providers could be doing more to secure their platforms against ransomware. Do you think they are doing enough at the moment?

Rob Jones: Could you perhaps assist by describing the type of platforms you mean?

Baroness Crawley: If we are talking about any telecommunications companies in the UK, for instance, could they be putting more resources into this area of vulnerability as far as they are concerned?

Rob Jones: It is a priority for big communications companies in particular, and they recognise that priority, because it would be an existential threat if they went down because of a cyberattack. We saw this with Carphone Warehouse many years ago, if you remember. Big attacks like that on companies involved in mobile telephony and communications are an existential threat to their business model. They absolutely see it as a priority.

Baroness Crawley: So you think they are on it.

Rob Jones: They are absolutely on it. We cannot be complacent about that: the level of challenge from the national technical authority and people like the NCSC must remain, but yes, they see it as a threat.

Graeme Biggar: The issue that comes up more often with telcos and tech companies is the extent to which they are taking the actions necessary to prevent some of their customers being the victim of online fraud, or their products being used as a vector for online fraud. We have lots of debates with them, and the Government's new fraud strategy puts front and centre that more needs to be done by those companies to protect against online fraud. By and large, they have improved their cyber defences to being attacked themselves quite successfully, but the NCSC will be the best people to give you the definitive view on that.

Q66 **The Chair:** Can I ask you one final question? I recognise you may not want to do this, but could I invite you to say what would worry you most in relation to ransomware? For example, if there were a high-damaging attack mounted against us, are we adequately prepared?

Graeme Biggar: We have not had a C1 attack, as we would couch it. We have C1 to C6, from the least significant to the most significant. A few looked like they might be a C2, but we have not yet had a C1. The cybersecurity of the organisations that would be C1 has definitely improved but, as MOVEit—the Zellis hack that was just referred to—has shown and as Rob was talking about, there is an underbelly to every company and organisation that uses software from a third-party provider. While the outside periphery of much of the CNI is now really quite well protected, there is an underbelly. That that could be hacked is what worries us most. That could be quite significant ransomware, and that is what we are very keen to see not happen.

Rob Jones: I absolutely agree with that. The unsurfaced risk in an element of the supply chain that could undermine the great defence and resilience that has been invested in is the thing that we all need to be alive to. Lots of work is put in to highlighting that, but that is an area that you need to keep constantly looking at in terms of what is getting into your supply chain as a company and what is getting into HMG.

Graeme Biggar: The one thing I would add to that is that our understanding of what is critical national infrastructure has changed. We have spent an hour now speaking about the national security community in the round, including your committee. A few years ago, we worried about a fairly narrow set of sectors. Going through the Covid experience has shown us how just-in-time society is, and how many different, really quite small companies in different places can be fundamental to the continuing normal function of this country.

We had a cyberattack against a relatively small company that provided the ability to move frozen foods around the country. It was relatively quickly resolved but could have suddenly stopped quite a lot of food being in quite a lot of supermarkets. The Government recognised that and published a new resilience framework in December that takes a wider look at resilience. As you will all recognise, Governments and, indeed, organisations like ours find it quite hard to focus on the chronic threats rather than the acute risks that are in your face, but the areas in which things can go wrong and can really matter are just so much broader than probably was the case before, and certainly more than we had realised. Cyber presents one risk to them; there are others too, but cyber is one.

Viscount Stansgate: Forgive me for saying this but if, heaven forbid, there was a C1, is it your policy to announce that there is a C1-level attack, or is that just language we are using here in the committee that you would not use publicly?

Graeme Biggar: It would probably be a government decision. I am not sure it would have much salience; it is our internal way to categorise incidents with government.

Viscount Stansgate: So it is your way of saying it is the absolute most serious.

Graeme Biggar: If that happened it would be pretty obvious to people. There is a lot of interest in whether something is categorised as a terrorist attack, for example, and there is a process with MI5 and CT police to try to think that through. People get quite interested in the counterterrorism threat level. I do not know how interested people would be in whether we consider it to be a C1 attack or not—actually, I am not sure what our policy is on announcing it, but it might be for government rather than us. Shall I check on that point and let you know, rather than just leave that one hanging?

Viscount Stansgate: Yes, please do.

The Chair: Thank you very much indeed. That has been very interesting. Thank you for coming and thank you for your evidence.