HOUSE OF LORDS

Select Committee on Risk Assessment and Risk Planning

Corrected oral evidence: Risk Assessment and Risk Planning

Wednesday 27 January 2021

11.30 am

Watch the meeting

Members present: Lord Arbuthnot of Edrom (The Chair); Lord Browne of Ladyton; Lord Clement-Jones; Lord Mair; Baroness McGregor-Smith; Lord O'Shaughnessy; Lord Rees of Ludlow; Lord Robertson of Port Ellen; Baroness Symons of Vernham Dean; Viscount Thurso; Lord Triesman; Lord Willetts.

Evidence Session No. 8 Virtual Proceeding Questions 82 - 91

Witnesses

I: Ed Butler, Chief Resilience Officer, Pool Reinsurance; Suzanne Raine, Affiliated Lecturer, POLIS, University of Cambridge; Dr Simon Harwood, Director of Defence and Security, Cranfield University; Dr David Blagden, Senior Lecturer in International Security, University of Exeter.

Examination of witnesses

Ed Butler, Suzanne Raine, Dr Simon Harwood and Dr David Blagden.

Q82 **The Chair:** Welcome back to our evidence session on security. Our second panel consists of four witnesses. We have Ed Butler, who is the Chief Resilience Officer at Pool Reinsurance; Suzanne Raine, Affiliated Lecturer at POLIS at the University of Cambridge; Dr Simon Harwood, the Director of Defence and Security at Cranfield University; and Dr David Blagden, Senior Lecturer in International Security at the University of Exeter. Welcome to you all and thank you very much for giving evidence to us today. A transcript of the meeting will be taken and published on the committee website and you will have the opportunity to correct that transcript where necessary. We have a number of questions for you but please do not feel that it is necessary for each member of the panel to answer each question. You can pick and choose which questions you want to answer.

My first question is for all of you. What is your view on the security risks contained in the 2020 National Risk Register? Is it a comprehensive picture or are there security risks to which the UK is particularly vulnerable or for which we are particularly poorly prepared? Who would like to begin? Dr Blagden, you have unmuted.

Dr David Blagden: That was my mistake. I echo one of the things that Lord Ricketts said in the previous session, which is that the number is growing ever upwards from the 2010National Security Risk Assessment that was a very neat 15 categories and then the 2015National Security Risk Assessment that was 20 categories and it is now 38. I do not have many grievances either way with the domestic component of those risks. One thing I note is that war, to put it bluntly, or variations of international military conflict, feature relatively lowly. There are some manifestations there of CBRN attack, cyberattack, but actual conflict between states is conspicuous by a relatively limited presence.

Suzanne Raine: Thank you, and it is delightful to be here. I wrote something last week called *Half of our National Risk Register is Missing*, so that is a bigger point. On the small point of what is missing from what is on there, I could not see, for example, the food supply chain on it. I might have missed it, but I could not see that. There is something about the interconnectedness of the world and our dependencies on it that I think is not articulated.

My bigger point is that a risk register in any other form is not just bad things that might happen randomly but things that thwart what you are seeking to achieve. What is clearly not in this National Risk Register—and there may be a secret one that is more comprehensive—is that there is nothing that sets out what is going to prevent us achieving what we are seeking to achieve as a country. Until you have done that, you cannot manage your national security risks properly. So for me there is something fundamentally misconceived about what is on it at the moment, but also we have to be really clear that sticking stuff on a table

and calling it a risk register is not the same as having a risk management process. I know that we are going to talk in more depth about that, but you asked Lord Ricketts whether he thought the process was right and I think there is quite a lot of work that could be done to improve the process that ought to sit alongside having a risk register.

Ed Butler: I have nothing to add to what Suzanne and David have said. But if we are talking vulnerabilities, we must consider not just the risk itself and those 38 there in isolation but what about systemic consequences that result from such a high-impact event? We have been discussing Covid but that is a really good example of looking at things not just in the single but in the round. In my experience, one needs to be conscious of when risks start aggregating and it is not just one event that happens but when we get a domino effect: do we have the mechanisms, resources, policies and the decision-making in place to cope with the magnitude of a whole series of risks happening at once?

Dr Simon Harwood: I think it would be naive of me to start by saying, "Is the list a comprehensive one?" I am not an expert in any of the particular individual risks that are on the current National Risk Register. However, what I see is that it contains a list of things that we are comfortable with. I hypothesise that the associated risk assessment, at least the open source unclassified version, does not provide sufficient evidence as to the level of threat to act as a platform for debate, assessment and involvement for those who need to interact with it. Furthermore, the current risk is simply assessed on an XY graph—the likelihood of occurrence versus the impact—rather than a much more detailed assessment that we would need to understand the impact of that risk.

We have not taken an approach of what I call anticipatory risk assessment. You may be familiar with black and grey swans. The list that we have at the minute contains just grey swans, known threats. The big and worrying ones are the black swans that we know nothing about, but we do not have a robust process to identify the black swans. As Lord Ricketts said in his excellent evidence, what use is simply having a list of risks that we do nothing about?

What I believe we need is a comprehensive resilience framework that looks at the risk and also our ability to mitigate. At the end of the day, if we have a risk in the top right-hand side of the graph that is a big risk but is really easy to mitigate, is it really a risk? Well, it is because it sits with impact and likelihood, but if we mitigate it, it is not a risk. We are not making an assessment of connected resilience and I think Lord Ricketts' evidence and other evidence has pointed to that.

The Chair: This is going to be extremely helpful for our eventual report. Thank you very much.

Q83 **Lord Clement-Jones:** This is very much a continuation on from the first question. Dr Blagden, I want to take you back to your paper of 2018, which I think you entitled *The Flawed Promise of National Security Risk*

Assessment.[1] You identified nine flaws in the NSRA. What do you identify as the most critical ones currently?

Dr David Blagden: One big issue is that you write lists like this for public purposes and as soon as that is going on there are all kinds of implications, one of which is decision-makers' political incentives. We do not want to be proven wrong, so we either add more things to the lists or we broaden the categories. The 2020 National Risk Register has clearly gone in the direction of adding risks. The 2015 version did not have as many, but it had some absurdly expansive categories such as "instability overseas". Instability overseas can be anything, but providing we have a category like that we cannot be proven wrong.

The other implication of it being public is that there are things we do not want to say. The 2010 National Security Risk Assessment does not name hostile countries, for example. We are very reticent to talk about threats. One consequence of that is that the likes of Russia and China, for example, are simply spoken about as diplomatic commercial partners, and then something like Ukraine happens and Whitehall is shocked by it. It [UK foreign policy] could seemingly not see that various measures such as supporting a particular movement in Ukraine might have other consequences vis-à-vis a powerful actor that we were conducting relations with, but of course we do not want to name powerful states in a public document like the risk register as anything other than productive partners because that would have political consequences of its own. Fast forward to 2015, we are now naming Russia as a threat and a concern, but China is still very much simply a commercial partner, even though there are obviously bits of the British Government that know full well that China is not simply a commercial partner.

Another major point is the qualitative variation that you get within categories. If we are going to talk about terrorism, that could mean the murder of Lee Rigby, which was tragic and awful but ultimately a statistically trivial addition to London's murder rate, right over to a 9/11 with nuclear weapons—9/11 times 100. So these categories, even in trying to capture and distil certain concerns, can be so expansive that they end up concealing other sorts of concerns you might have.

The third one I will mention, if I can treat myself to a third, comes to something that Ed mentioned in his opening remarks, which is some of the interactions you get between categories. Distilling things down into little silos makes them neat to look at but something like cyber—"cyber" is not anything by itself, it is just a technological vector for other things, whereas international military conflict is a state of political relations between countries and public disorder is really making the referent object of security, that is the thing we are supposed to be protecting, also the thing that we are saying is the source of the threat. These are not even

[1] David Blagden, 'The Flawed Promise of National Security Risk Assessment: Nine Lessons from the British Approach', *Intelligence and National Security* 33:5 (2018), pp. 716–36 [DOI: https://doi.org/10.1080/02684527.2018.1449366; Open Access Version: https://ore.exeter.ac.uk/repository/handle/10871/31835].

apples and oranges really, they are sort of apples and elephants, but they could come together in ways that interact to produce ratchet effects. If we are going to say that international military conflict is a top-tier risk but then we are going to say that CBRN attack is only a tier 2 risk, we might say, "Hang on a second, the worst-case possible outcome of international military conflict is CBRN attack so why is one of them sitting below the other in the prioritisation?" Anyway, I will stop there.

Lord Clement-Jones: Thank you. That is very helpful. We have come across the arguments about the interaction. I do not know that we have come across the arguments so much about the problem of saying too much on the one hand and too little on the other that you mentioned as your first point. How do you cure that? There is no appetite to go private again and not publish the register, is there?

Dr David Blagden: No, and I do not think there should be appetite to go private. It comes to some of the stuff that Lord Ricketts said about it being fine for there to be classified analyses underpinning these sorts of things. We do not want to have published vulnerabilities, "This is how you would hack our nuclear power stations and turn them into a bomb". This vulnerability is not something we should be publicising, but the NRR is supposed to function as the top level of strategy that the whole of government can buy into, the emergency services and the wider country can buy into and ultimately the public can buy into and recognise that is what is being done in their name and they can have a debate about. I do not think it should return to being a private undertaking. There are some little fixes in thinking about how these sorts of documents can be done that do not necessarily address exactly the point you just asked.

The bigger point is perhaps around the politics of how these things are presented. As a general rule, we should display much more humility about our forecasting capacities and preface any undertaking such as this with very clear and big bold font on the front page that this is not a crystal ball of the future. Obviously bad stuff will still happen. But this NRR is simply an effort to prioritise concerns in the world. It comes a bit to what Suzanne said about being explicit about what you want to achieve in the world. You can have that explicitness and then a top level of government with the courage to own that, rather than the incentive to broaden out the categories and add to the categories because then at least we get nothing wrong, we do not have 'egg on our face' afterwards—but the problem then is that you have not achieved any prioritisation. If your register covers the whole world, it also has not told you anything about the world.

Lord Clement-Jones: Thank you very much. The other witnesses might like to add to what they said in answer to the first question, but particularly on the question of the merging of the National Risk Assessment and the National Security Risk Assessment. How well are security risks now presented?

Suzanne Raine: I am going to controversially say that I do not think that we have a National Security Risk Assessment system. That is part of

the problem, because there is an assumption that we have one that is not working properly but I think we probably do not have one at all, by which I mean a system that allows for constant monitoring, anticipation and, most importantly, a formal warning of when a risk is changing and escalating or reducing. There are some areas where the system works well because there is an assessment and warning system in place. As Lord Ricketts was saying earlier, in terrorism we put a lot of effort into setting up a risk management system and in so far as it is possible it works precisely because you have a dedicated assessment resource that is receiving every piece of information available to the Government, thinking about it, monitoring changes and it has a formal warning function to signal an alert—and somebody has to do something because it is a formal function and a function independent of political influence.

There is no equivalent across a whole range of other national security risks. The JIC, which has been there a very long time, analyses and thinks about national security threats but does not have any formal warning function. One of the problems is that as the world has become more complex we have a British government system that has evolved gradually over the last 100 years and may not be structurally deft enough to be able to deal with the complexity or the interdependencies of some of these national security threats, which are also about trade and supply and all those things that departments that would not normally be involved in national security conversations need to be pulled into. Who is working out what we know and turning that into understanding and when are the warnings sounded and by whom? That is the bit that is just not there at the moment.

One solution would be to say that we are going to expand the remit of the JIC to cover everything that we consider to be a national security risk and we are going to give a formal warning function to the JIC or some of the other assessment bodies—cyber assessment or terrorism assessment or health assessment, whatever you call them—and when they flag a warning, that will kickstart a process in government. Until you have a formal structural function there, you will continue to be in a situation where people write papers. Across government people are writing papers and sending them to each other, but who decides when to do anything about any of it? I think that is the thing that would need to change in order for things to improve.

Dr Simon Harwood: I think we are going to find ourselves agreeing with each other today. In a simple answer to the question, "Is merging the two bits together into a bigger risk assessment a good thing?", yes, it is. Why is it a good thing? Not because you have an ever-growing list of risks, which frankly is just a piece of paper that people may look at occasionally. It is because we should be looking at the affect and effects of that risk and how to mitigate them.

The example I always like to use is that it will be an absolute catastrophe if our GPS system goes down. We will not be able to find our way anywhere, we will not be able to use the stock exchange, we will not be

able to take money out of cashpoints, we will not be able to use our credit cards. The current way we assess the risk is by saying that country X has an anti-satellite weapon, it could knock out satellites—but we also have this thing called a Carrington event or space weather that can have exactly the same effect on the satellite constellation of taking it out.

By having two lists on a risk register, the effect is that we lose the timing stamp in the UK and globally to do these things. So we really have to start moving from an ever-expanding list of risks into what we are going to do about them, this connected resilience. On that point, we have to make very strongly the point that these are not isolated risks. They are at best linked, if not actually systemic, in the way in which they connect. It is interesting that the different risk registers around the world all contain different risks. That is because different regimes have different risk appetites or views on risk aversion. That is why some countries rank things higher than others, but ultimately all of the risks are the same.

Very quickly if I may—in terms of a classified risk assessment, yes, we have to have something that sits behind to work out what the threats are, but what we really need is a framework or a mechanism in which people can interact with those risks and mitigate them. I think nobody would argue that government should not own the risks, but government is not wholly responsible for mitigating those risks. That is the public and industry.

Ed Butler: This is all about threats being a combination of intent and capability. As Suzanne said, how will the National Risk Assessment identify, track and mitigate these risks to national security? I concur that there is no standing body such as the Joint Terrorism Analysis Centre, JTAC, which Suzanne knows well. A similar structured model could be expanded, potentially building a body out of the JIC. COBRA stands up when there is a crisis and it usually deals with those crises very well, because it brings cross-government departments together, experts and specialists together. They look at the crisis, respond to it, make decisions and we get through it—but we do not have a standing COBRA, as I understand it, which could focus on national security risks on a continual process. So the committee may want to look at something along those lines.

The Chair: Thank you very much. The JTAC model is one that we may well wish to recommend once we have given that further thought. Thanks very much for the idea. Lord Robertson.

Lord Robertson of Port Ellen: James, do you want to bring Des in on the insurance thing before I move on to the other, broader issues?

The Chair: Okay, good point. Lord Browne.

Q84 **Lord Browne of Ladyton:** Thank you and apologies that the instability of my internet chased me off for a bit, so I missed some of the last evidence. My apologies to the witnesses. At this point I should draw attention to my register of interests, particularly in my capacity of the work I do at Cambridge University. I am presently actively working with

Pool Re on a conference on bioterrorism and insurance for that.

This question is directed to Mr Butler. Could you outline for the committee how Pool Re's model works and how it has proved to be flexible over the last few years under its current leadership to respond to an evolution in international risk, in particular in terrorism risks?

Ed Butler: Thank you, Lord Browne, and it is good to see you again. As some of you know, Pool Re was established because of the availability of terrorism insurance evaporating in the wake of the Provisional IRA's attacks on the financial centres and districts of London in the early 1990s, which led to a a clear case of market failure. Initially, Pool Re was set up to be a simple mechanism to transfer taxpayers' money into the market to provide solvency. Now we provide not just a mechanism but also a substantial buffer between an attack and the taxpayer; that buffer is no in the order of £10 billion. We very much have a public policy objective to improve the resilience of UK plc to terrorist attack. We are a mutualised scheme, we are owned by our members, and we write commercial property cover across Great Britain.

Since we were set up in 1993 we have responded to the changing nature of threat in a number of ways by what we refer to as closing protection gaps. In 2003 we included cover for chemical, biological, radiological and nuclear attacks; and the establishment of an in-house threat analysis capability, closing an information gap in 2016. We also included in the scheme, in 2018, protection against terrorists using a cyber trigger to cause a fire or explosion. That was in anticipation of terrorist entities moving up the cyber technological curve. Lastly, on the back of the attacks in 2017 we have included what we refer to as non-damage business interruption (NDBI) cover within the scheme. Principally we were created just for an attack that caused property damage by a fire or explosion, but obviously we have seen a change in the nature of terrorists' methodologies. They are now not causing property damage but they are causing significant business interruption cover.

Over nearly three decades we have demonstrated that with a successful public-private partnership between the Government and the insurance industry we are in a better position to manage terrorism risk. We have made it more affordable, we have established and grown a private market for terrorism insurance protection of UK assets up to £2.2 trillion of property cover. We have paid out over £1 billion in claims in today's money, without having to resort to the taxpayer or the Government's loan facility. We have developed a sophisticated £10 billion risk-financing structure, creating a buffer of multiple layers between an attack and drawing on the loan facility. We have paid, of note, over £1 billion to the Treasury for the facility of its guarantee. I think importantly—and others may want to comment—we have invested heavily in partnerships, into research, with academia and into risk mitigation initiatives with the Home Office and the counterterrorism police. Our purpose is to better understand and mitigate contemporary and future terrorism threats to the UK.

Lord Browne of Ladyton: Thank you. We will have an opportunity in a later session to go into insurance in this area in more detail, so I will hand back to Lord Robertson and he can follow on from that.

The Chair: Before you do—Ed Butler, where does your funding come from?

Ed Butler: We receive premiums from our members. There are about 150 members who pay premiums for the reinsurance cover that we provide for them and we pay some of those premiums to the Treasury for the loan facility that I talked about.

The Chair: Thank you.

Q85 **Lord Robertson of Port Ellen:** I was going to ask a little bit about terrorism, but in a way it has already been dealt with and I do not want to get into repetition on this. I will ask Ms Raine, and maybe the others as well: does the National Risk Register focus too much on the domestic risks and less on the risks to the country from foreign state and non-state actors?

Suzanne Raine: I think we are a little bit hampered by not having seen the classified version of it.

Lord Robertson of Port Ellen: So are we.

Suzanne Raine: I suspect that there is no shortage of concern in government about the threats to the UK from hostile actors, either overseas or among us. The question that I think somebody was alluding to is why terrorism comes so high in these threats. It is possibly simply because the system is set up so that there is a means by which the changes to the threat are monitored and a very clear communication for when the risk is escalating. If you had a similar system for all the other threats it would obviously get a lot more competitive at the top but it would equalise it. So it is not that terrorism is being over-prioritised but just that it is organised in an efficient way to allow that cycle of warning and preparedness and resilience to play out much more smoothly than it does on other national security risks, or indeed any other risk.

The terrorism risk is monitored continuously by looking at tiny, tiny changes and new pieces of information. The clearest analogy is with things such as the Met Office and the Environment Agency, which are constantly being asked not to say what has happened but to predict the near future and measuring water levels on a daily basis. That is the kind of thing that is probably the way we need to be looking across a much broader range of risks.

Lord Robertson of Port Ellen: That is a good point. Does anybody else want to jump in?

Dr David Blagden: It is interesting, first of all, that this National Risk Register and national security risk assessment—merged things that they are—is ultimately owned by the Civil Contingencies Secretariat. I think that would be quite odd in the context of a lot of countries—that

something that is about the assessing of high-level national security concerns belongs to a bit of one government department specifically focused on civil contingencies. That is probably right and proper to an extent, because we are talking about the consequences for society, but I wonder whether that leads you into a sort of preoccupation with domestic concerns rather than international concerns. The National Risk Register is owned by the Paymaster General. Again, it is a novel orientation for something that is supposed to sit at the top level of national security policy that that is where that process—if it is a process, as Suzanne has identified—actually sits.

The other thing, as I mentioned in some of my earlier remarks, is that talking about state threats is harder. If you start talking about what the UK thinks about the situation with Russia, a lot of people are reading—Estonians, Americans and people in Russia are reading with great concern—what you are talking about. But I think one consequence of that is that you end up shying away and leaving big tracts of stuff that you ought to think of as risks underassessed. There is quite a stark divide with the National Risk Register. It is all very well to say, "Yes, this sits in the Cabinet Office but we liaise with the other departments". Be that as it may, there is a bit of divide between what is in the National Risk Register and the sort of stuff the MoD is now talking about.

The MoD is talking openly about the return of great power competition, persistent, state-based grey-zone threats—all the current jargon—and some of that comes with big risk implications. For example, we are likely to be sending an aircraft carrier group on its maiden deployment to a part of the world that the world's rising superpower regards as its territorial waters, and this is a big risk. It might be the right choice, it might be that you have made a considered assessment that trying to balance China in that way is the thing to be doing, but it is not devoid of risk implications.

So this is sitting with the Civil Contingencies Secretariat and we do not really want to talk about relations with powerful states because that brings us other consequences. We end up talking a lot about flooding and terrorism and not a lot about some of the other things that ought to be sitting on the ledger.

Q86 **Lord Robertson of Port Ellen:** Making an assumption that the security classified part of it does deal with all these things—and that may be a heroic assumption—should the risk register include things such as Brexit or Scottish independence or migration, for example, things that are actually there, or do we assume that they are being dealt with by the classified bit of it as well? Ed Butler, do you want to comment?

Ed Butler: Yes, thank you, Lord Robertson. In my experience, if you hear leaves rustling overseas, there is generally going to be a blowback into the UK of some form or other. We are well aware of the interconnected world, the internet of things, and Dr Harwood talked about satellites being taken down. But I think what you touched on—I am not referring to hostile state actors and they are clearly a growing threat—is more about

the physical drivers and the political ones such as Brexit or the break-up of the union impacting on our security and economic well-being.

Then there is the matter of transnational threats becoming national threats. (I must say sorry to Dr Blagden for sticking to terrorism, my subject matter of expertise.) Factors such as migration, immigration, climate change, population growth and urbanisation are all drivers of terrorism as well as social division, extremism and political violence. My question is, and it may be in the classified version: do we have the capabilities and sensors out there, the human, the technical, the scientific and the diplomatic, all joined up and in one place to measure and assess these and to be able to respond to them? These are all big issues coming over the horizon, which will influence all 38 of the risks on the National Risk Register—which probably in five years' time will be 58 (which I suggest would be too many).

Dr Simon Harwood: I think there is danger in splitting things up into: is it domestic, is it foreign, is it man-made, is it natural? We have to be looking at these threats and risks as a holistic fit. I hope I do not sound like a broken record but it is the changing nature of the threat. These threats are interconnected, as Ed Butler has just said. There is a connection between terrorism and the natural world; if a terrorist were to blow up a dam, it would cause a flood. Are we managing the risk of a terrorist blowing up a dam or are we managing the output of the flood? You see in that sense that they are interconnected. While I think it is quite right to keep our natural secrets secret, and we have a classified version of the document judging where those biggest state-acting threats come from, again we have to look at the output and the effect.

On a point that Lord Ricketts made—and I think Lord Robertson made it—I am chairman of Academic RiSC, which is 66 UK universities involved in national security research and development. This interaction between government and academia—being allowed inside the inner circle so that we can comment before publication of Green and White Papers, where we can understand and help make some informed decisions on risk assessments and risk mitigation—is something that needs to happen more closely. At the moment it certainly feels like debate happens within government and then we are told after decisions have been made. I do not think that is a very sensible approach. Looking at the witnesses on the call here today, I think most of us worked in government until we left and joined academia, so we do know both sides of the fence.

The Chair: Yes, I think that was the point that Lord O'Shaughnessy was asking of Lord Ricketts.

Q87 **Lord Mair:** My first question is for Ms Raine. You have spoken already about your views on how there should be more of a warning function. In something you wrote you said that a better word for "forecasting" would be "anticipation" and you described how the Environment Agency and Met Office work in that respect. You said that you believe that the government intelligence analysis profession is understaffed and struggling with workloads—presumably linked to the point you are

making about the need to anticipate. This has an impact on risk management. How do you think this should be addressed? What is your remedy?

Suzanne Raine: Thank you for asking that. It is striking that when people talk about government, they talk about departments or they talk about policy or intelligence collection perhaps, but they seldom talk about assessment and analysis as being a function within government that is esteemed in the same way that policy-making is esteemed, for example. One of the problems—I am not saying this is a solution—is that there is no government department that is solely responsible for assessment and analysis. Every department will have a section within it that does assessment and analysis in some form. For example, in the MoD you have defence intelligence, but you also have all sorts of other bits of the MoD such as DCDC that do the thinking, and in the Foreign Office you have the research analysts, but they are all subsets and they are not funded. They are funded essentially from within the department's budget.

The problem is that the thing that we esteem in government is either the collecting of information or doing something with the information. The thinking bit often is simply not in the conversation. We are collecting an infinite amount of information, which is growing daily, and somehow we have to work out what that means to us and what we are going to do about it. If we do not properly resource the bit that works out what the information says, the chances are that the decision about what you are going to do about it will not be as good as it could be. Structurally, I am very much not arguing that you should take all these different assessment and analysis centres or bodies and put them into one big melange, because I think you will then undermine their effectiveness. They need to sit within their departments as centres of expertise, but they need to be funded properly.

Cabinet Office assessment staff—and it is quite opaque—are funded from the Ministry of Defence budget. Although the MoD has just had a significant settlement, that is for capital and not resource, so the MoD is probably going to end up with a smaller amount of money to spend on resource. That impacts immediately on the amount available for Cabinet Office Assessment Staff, who under all these models in theory need to be the centre of some kind of national security risk management process. The answer is essentially that they are constantly scraping together to continue to exist.

I speak from my experience in JTAC, but the JTAC model works essentially like a charity to which government departments donate people and resource. That is dependent on good will and a willingness to shoulder a collective responsibility. I do not think that that resourcing model is scalable or tenable for the long term. I think there should be much greater esteem put on the bit of government that does the thinking and it should be funded on the basis that if you get the thinking right, you probably have to spend less on the policy because arguably you could take better decisions sometimes.

Q88 **Lord Mair:** Thank you. My question for Dr Harwood is on resilience, which has been referred to quite a lot. You have written about it and you have spoken about it. You have highlighted that the current process assesses risk but not resilience—in other words, the preparedness, the recovery time, the crisis management aspects. To what extent do you think this lack of resilience is a threat in itself?

Dr Simon Harwood: Very simply, enormously. As I have said a number of times, we are simply listing the risk but then not what we are going to do about that risk. I promised myself I was not going to use any Covid examples, but we are living through that proof at the minute. We have built organisations that are razor sharp in terms of resources mapped tightly against a clear business case, but that also means the operations are razor thin. For example, Covid-19 has exposed everything that is brittle about making efficiency the priority for both the public and private sectors. As we have said previously, threats from virus-related pandemics have always been prominent on the National Risk Register. We previously mentioned Operation Cygnus back in 2016. That report has not been made widely available, but things have come out, as you said: lessons have been recognised or rather lessons have been identified, not necessarily learned in that sense.

To be fair, in a business case, in efficiency terms, why would you invest to mitigate a low-probability event when there are lots of things to spend the money on? But I think, as now has been proven, we have to start making that business case, we have to start making that assessment about where we should be mitigating some of these risks—in other words, the connected resilience aspects of it—rather than simply alone looking at the risk.

I will finish by saying that when I look at the current National Risk Register, I am stunned by where cyber, as a domain, is listed on the current register because—I think as Dr Blagden said—cyber has an effect on something else. If you look at the rest of the register, the loss of the power grid is a higher risk than the cyber threat, but it is more than likely that the loss of the power grid would come from a cyberattack: it is the interconnected nature of the threat and the risk and the resilience that we have. So I cannot recommend highly enough that we have to have a focus on resilience, not on risk alone.

Q89 **Lord Mair:** Thank you. One last question and perhaps Dr Blagden and Mr Butler could address this. On this question of resilience, what are the challenges in developing resilience capability? What are the barriers to doing that? Dr Blagden, would you like to start?

Dr David Blagden: I am not a resilience scholar per se. My one observation on this is that as we in the West—not just the UK—have moved ever more in the direction of forecasting and horizon scanning over the last 10 or 20 years. It has definitely been risk identification, risk mitigation that have been part of the vogue of security policy. One perilous consequence of that is that we become more confident about our assessments, so we end up in this paradoxical situation that my colleague

Patrick Porter has written about[2], where we profess great uncertainty—no security document can begin without some profession about how the world is ever more uncertain or ever more complex or whatever—and then proceed to display great certainty in our assessment of what the risks are in the world and what should be done about them. We like this because it gives us grounds for being very lean in everything we do.

There is almost a direct trade-off between resilience and efficiency, so we are very, very confident in our prescriptions about what the threat looks like and very, very confident about what should be done about it, and this justifies just-in-time resupply of whatever it is. It justifies very small holdings of oil and gas. When we look at the MoD, which is the case I know best, it justifies very low stockpiles of munitions or fuels or spares of anything, because we are always confident that we have just the right amount for whatever it is that is that is expected to be done. You get into these arguments and the MoD says, "We have the correct number of warships for current taskings" and you say, "Hang on a second, what if international politics were to thrust some other taskings on to you?"

You end up in this situation of great confidence and prescription in what it is that you think the world is going to throw at you, and that justifies being very lean and efficient in the amount of state capacity you have most basically, whether that is military force, healthcare or intelligence assessment capacity—whatever it is. So my main headline would be to be less confident in our forecasting efforts and, therefore, less willing to use them as justification for trimming everything as lean as it can be.

Lord Mair: Thank you. Mr Butler, what do you think? How should resilience capability be developed?

Ed Butler: This clearly comes down to resources, which are fairly scarce at the moment. I think there is a positive example in the significant investment we saw two or three years ago into the National Cyber Security Centre, which really has improved our resilience in thinking about and understanding of our vulnerabilities to cyberattack.

There is another way of looking not just at the challenges but at the opportunities to improve resilience. It is not for me to go into detail, because I know you have a session later with the insurance industry, but the greater involvement of the insurance industry and the disaster risk financing model, which I talked about on Pool Re, and the pooling of risks is a way to improve our resilience: greater leverage of the insurance industry, where and how we model risk, how we look at it and how we understand what the future frequency of events might be, whether these are earthquakes or fire or vehicle accidents, as well as what these impacts are going to be.

---

[2] Patrick Porter, 'Taking Uncertainty Seriously: Classical Realism and National Security', *European Journal of International Security* 1:2 (2016), pp. 239–60 [DOI: https://doi.org/10.1017/eis.2016.4; Open Access Version: https://ore.exeter.ac.uk/repository/handle/10871/19228].

I have a further point on this public-private partnership. Simon Harwood talked about the relationship between academia and government, but if you get the power of the three, of academia, government and business working together, whether it is for risk financing or engaging the capital markets to come and invest in risk mitigation and resilience measures, it is all in everyone's interest. We need to think more broadly than just having a government response to this. Yes, it can be supported by academia, but we should reinforce the role that industry can play, especially those who have their own investments in particular areas.

The Chair: Thank you. I was next going to call Lord Triesman, who may be having a bit of trouble with his internet. If he is not available at the moment, Lady McGregor-Smith.

Q90 **Baroness McGregor-Smith:** There has been a huge amount of debate on a whole number of issues. I was hoping that each of you individually could give the committee one policy recommendation that you would give to the Government. Perhaps we could kick off with Ms Raine.

Suzanne Raine: I have probably said most of it already, but I would improve the risk register. It is a simple thing to say, but I would produce a document at a higher classification that really did list the things that most concerned the country in what it needs to achieve and what it needs to stop happening. I would allocate the tracking of those risks to assessment bodies that were resourced and capable of doing it. I would have in the Cabinet Office a central risk assessment function that was responsible for co-ordinating with those assessment bodies, which would flag up when a risk was changing. That would work in conjunction with a set of things that could be set in motion to enable preparedness. I would increase the investment in and esteem of the assessment bodies corresponding to the risks and give them a warning function that triggers preparedness.

Baroness McGregor-Smith: In your experience, out of interest, clearly all of this is more investment, which I think is completely right. What do we spend money on that we should not? We need to find a way to pay for all this when this is all over. We can imagine our committee sitting here making lots of recommendations on how the Government should spend more money and they say they have no money. What could we cut that we think is a complete waste of time?

Suzanne Raine: It is possible that on the national security side of it—the bit essentially that is less visible in the currently existing National Risk Register—we spend a lot of time admiring the problems and going round and round in circles. The question is the balance between policy professionals, people doing things and people monitoring. I would shift the balance towards assessment and away from some of those.

I am thinking about this very carefully, because you are entirely right: you do not want to reduce your collection, because you need the information coming in. You do not want to reduce the capability to do something about it. It is about adjusting the bit in the middle, some of

which is probably about plumbing as much as actual staffing, but there is also something about repurposing some of the people who consider their job to be policy towards the understanding and thinking.

Baroness McGregor-Smith: Thank you, that is very helpful. Dr Harwood next, please.

Dr Simon Harwood: Yes, thank you. Quite simply, as I have said throughout this call, it is the establishment of a new national resilience framework, a connected resilience framework, to replace the simplistic risk assessment that we undertake. Having such a new framework will better allow people who respond to prepare, policy and regulators to make informed decisions and industry to undertake robust resilience planning, and it will act as a source for public information. Most importantly, it will highlight areas for new and emergent research and development to look at some of those risks and that resilience. In summary, out with the old, in with a new national connected resilience framework assessment.

Baroness McGregor-Smith: Thank you. I am interested in your point about how you involve industry. One of my observations has been that as industry has tried in many cases to be involved in the current pandemic, it keeps getting shut down anyway. We need a better way of working out, for example, what Covid-secure to everything else means. There needs to be better interaction with industry on how it can help on some of these very big challenges.

Dr Simon Harwood: Yes. I have to put out thanks. In literally the last two to three years, the triumvirate that Ed talks about—of government, industry and academia—coming together has got a lot better. Certainly that interaction has become much closer through the Office for Security and Counter-Terrorism. We are now starting to have those conversations, but as some of you may have seen in articles that I have written I still think that the biggest barrier certainly to government, industry and academia is the commercial one. We have something like the 2016 public procurement regulations that allow for innovation partnerships. They have not been used in the defence and security realm.

Baroness McGregor-Smith: That is very interesting.

Dr Simon Harwood: There are frameworks out there, but the commercial bit prevents us working together as one. There are many examples out there. We looked at Israel. Israel has an excellent way of government, industry and academia working together, and many other countries have this. We are just a little preoccupied with, "We can't tell you that, because it might be a conflict of interest", or something like that. There has to be a better way of working together in the interests and protection of this country.

Ed Butler: I will stick to the terrorism angle here, but what I am going to say is probably applicable to other risks. At Pool Re, the company I work for, we could present a formal annual review of the terrorism threat to

the UK, highlighting what new threats and risks may be emerging; what the protection gaps are—in other words, what is still exposed from what we were able to do before or maybe not; and then looking at what those appropriate risk mitigation measures are, and finally costing them.

This is all part, I suppose, of the risk management process, with respect: you have to understand the threats, you have to understand your vulnerabilities, you then have to know what mitigation measures will reduce those vulnerabilities; you then have what the associated cost will be, and you are left with the residual risk. Then the Government have to decide whether to accept that risk or not, or, as happens in the insurance industry whether to transfer that risk on to someone else.

We need to provide an annual review and then to go through that whole process, so that at least the Government would know exactly where they stand from a business perspective on the specific threat vector of terrorism.

Dr David Blagden: One obvious thing—it has already been said in some ways, and it feels like we have been saying it for years and years, although it is probably getting a bit better—is having more capacity to bring thinkers in from outside government. A lot of what you end up talking about with these kinds of risk assessments is almost cognitively biased group think: "What are we going to consider?"

The 2015 national security risk assessment, which is the one I looked at more closely for the article I wrote, starts out saying, "We looked at all risks that were deemed worthy of consideration", and then—surprise, surprise— it came out with a list of 20. You were left thinking, "How did these 20 get chosen? There are much bigger ones I would put in there". We are talking about pressure on allies. But what if an ally was to turn against us, like Donald Trump? Also, hang on a second, we are not even talking about the break-up of the UK itself, which is clearly a non-trivial risk at the moment.

Whatever vehicle it is, it is about having some capacity for bringing more outside expertise in, such as a net assessment unit, which I know the Modernising Defence Programme in 2018 said it was going to create but I'm not aware that it has quite got off the ground yet. All the departments consult and bring in outside expertise, but then one official changes office and suddenly the fact that they consulted with outsiders is forgotten, the list of emails is deleted, or whatever it is, and we are back to square one.

I have had those kinds of experiences with the Cabinet Office and the MoD; there is some productive consultation, a person changes job and suddenly it is gone again. You say, "How about we get some people with security clearance so they can talk about this stuff in more specific terms?". Then it becomes all about little things like cost, or, "We can't bring them up to Whitehall, because there is no budget for the day, so could you send us an email of your thoughts?" You forego insights over trivial little pots of money.

In sum, I think that some sort of institutionalised mechanism for bringing in non-Whitehall challenge would be productive.

Baroness McGregor-Smith: Thank you very much. When you talk about budgets, I reflect on what the Treasury's role is in all this when we have these issues. How we manage emergency funding differently is one of the things I have been thinking through, because ultimately so much of this comes down to funding. The point about the interaction between business, academia and the Government and how they all work together and think differently together, particularly in areas where there are high security issues, is something that we really have to think about, because it is clearly not always working practically today. Thank you very much for your comments.

Q91 **The Chair:** The final question goes to Lord Triesman. He is still muted. If I may, then, I will ask his question, which was to Dr Harwood.

You have written about how a specialisation of knowledge has led to a narrowing of thinking, and you have proposed the establishment of a new emergency agency dedicated to risk management. Is this the sort of thing you have been talking about this morning?

Dr Simon Harwood: Yes, in a way. I have written about how you can deliver on the promises of a connected resilience framework. I am not talking about breaking up the existing departments of state, but if we look at national security there are departments that are cylinders of excellence: Defra, which is responsible for the environment; the MoD, which is responsible for defence; and DfT, which is responsible for transport. National security problems, as you are all as aware as I am, do not follow the lines of departments. National security challenges roll across different departments.

The classic example I like to use is unmanned aerial systems and the threat to countering unmanned aerial systems. Who is responsible for that? Is it the police in the Home Office, is it Border Force in another part of the Home Office, is it the Ministry of Defence, is it the Department for Transport, is it Defra if they are poisoning our food supplies? Who is responsible for mitigating this threat?

What I am talking about is how we undertake the operationalisation or the management of mitigating those threats and moving from individual expertise on a particular threat to looking at the system-of-systems nature of the threat. We need leadership and decision-making from a dedicated national level operation capable of working, as has been mentioned—nationally, internationally and globally.

We cannot continue to rely on the outstanding work that the Armed Forces are doing to step in for any and every extraordinary event, as has so often happened: flooding, foot and mouth, disruption of the petrol supply chain, Covid and Ebola. This time with Covid we were lucky; the UK was fortunate that our Armed Forces were not being deployed extensively overseas on a mission. They need to be focused on their core role.

Perhaps again slightly controversially, I would argue that the Home Office's remit is too broad to take on a role in its current form. The department arguably needs to be broken up and put back together again around a focus on emergency management. In the US, for example, FEMA—the Federal Emergency Management Agency—is part of the Department of Homeland Security. It has been shown to have its own flaws, let us be very clear about that, but it is at least an example to learn from. Arguably, the new emergency management agency would need a budget, as Baroness McGregor-Smith hinted at, that reflected the fundamental value of security, the underpinning of the lifeblood of the nation.

Interestingly, it would need back-up from the UK population in the form of a body of volunteer reserves. Do you remember very early on in the pandemic that we called for the public to come and support the NHS? What did we ever do with that force? The Armed Forces have a reserve force, or a territorial army as it used to be called. Why can we not get the public trained in management, logistics, supply and support? I jokingly call it the fourth emergency service, a group able to work across our communities, come together, give training in medical skills, do crowd control, logistics and communication—essentially, a group drilled to take its place alongside local councils and the emergency services.

Again, there is no business case for any of this. It is low probability, high cost, but can the nation afford to keep making decisions about risk and resilience based on these types of crude equations? Thank you, Chair.

The Chair: It has been an absolutely fascinating morning and an incredibly rich discussion, from which I should think we will probably be able to create a report all on its own. I think this morning's evidence session should be compulsory listening for any Cabinet Minister. I am extremely grateful to all our witnesses, but also to all the committee, who brought out some very interesting points, and to our staff. Now is the moment for me to bring this quite long session to an end.