Joint Committee on the National Security Strategy

UK Resilience

Monday 27 March 2023

4.30 pm

Watch the meeting

Members present: Margaret Beckett MP (The Chair); Angus Brendan MacNeil MP; Sarah Champion MP; Bob Stewart MP; Lord Reid of Cardowan; Lord Strasburger; Lord Butler of Brockwell; Viscount Stansgate; Stephen McPartland MP; Baroness Fall; Lord Robathan.

Evidence Session No. 1 Heard in Public Questions 1 - 14

Witnesses

I: Elisabeth Braw, Senior Fellow at the American Enterprise Institute (AEI), and member of the National Preparedness Commission; James Ginns, Head of Risk Management Policy at the Centre for Long-Term Resilience; Lord Harris of Haringey, Chair of the National Preparedness Commission; Rois Ni Thuama, Head of Cyber Governance for Red Sift.

Examination of witnesses

Elisabeth Braw, James Ginns, Lord Harris of Haringey and Rois Ni Thuama.

Q1 **The Chair:** I thank our witnesses for joining us today. Ms Braw is joining us virtually, as are some of the members of the committee. We are very grateful to you for coming to be with us.

We waited rather a long time for a resilience strategy, and mentioned it once or twice, and then we were presented with a Resilience Framework instead of a resilience strategy. I would be interested to know what the four of you think of that and whether you think it represents a downgrading of government ambition and interest in resilience, which this committee has long argued is of double importance.

Lord Harris of Haringey: You can get into all sorts of interesting semantics as to whether a framework is more all-embracing than a strategy or whatever. In my view, a strategy implies that there are deliverables against which you can be measured. I am not sure that you

can have deliverables against which you can be measured for a framework.

From that point of view, I see the framework as being something less than a strategy. However, I would also argue that what is critical in all these things is the extent to which there will be high-level political commitment to delivering the objectives. If you do not have that, it does not work. I think back to former Ministers from the Cabinet Office with these resilience responsibilities. Two in particular took their role extremely seriously and had the seniority and clout to make things happen. The two I am immediately thinking about are Oliver Letwin and David Lidington, in the last few years. In both instances, they were senior enough in the government structure to command the respect of other Cabinet Ministers, and they were determined to make things happen and did make things happen. That is important, whether it is a framework or a strategy.

The Chair: A very important point. Thank you.

Rois Ni Thuama: The Government mentioned two timeframes in the document, 2025 and 2030. My view is that it is too soon and not soon enough.

When I say too soon, I refer back to 2018, for example, and a report published by the National Cyber Security Centre in co-operation with the Solicitors Regulation Authority and the Law Society. In that report, they addressed the most significant cyberthreats that the legal sector was facing. Five years later, we discover that 42% of the top 100 law firms in the UK have conformed with National Cyber Security Centre best practice, eight are quite good, and 50 have no protection at all.

Also in 2018, the Government, alongside the National Cyber Security Centre, introduced a six-page document on the minimum cybersecurity standards which all government departments, as well as suppliers, were expected to conform with. If you simply take one of the elements, which is a public-facing piece of technology that can be found easily, we discover that of the 598 government departments, 371 have unique domains. Of the 371 unique domains, only 38% had conformed with national cybersecurity standards. The minimum cybersecurity standard was "shall", meaning "must", across all departments, and the Government themselves are only at 38%. So, on 2025 as a timeframe, if we look back and realise that it has taken us five years to get to 38%, that is why I think it is too soon.

I also think it is not soon enough because, as the Government so rightly point out in all the documents, we are facing a converging of threats, which I do not need to go into again. In that respect, if we are to make use of this as a document, we need to see something additional to accelerate the adoption of best practice.

The Chair: Interesting.

James Ginns: I think this represents a step in the right direction, but it is not the fundamental step change that a previous Paymaster-General, I think, was calling for. In that sense, perhaps, the ambition is not as great as it could have been. It falls down in the overall governance of risk. Take, for example, a novel pathogen, a serious risk. We want to be sure that the work of the people who own that risk is overseen by someone outside their department who is suitably empowered, and that both, in turn, are scrutinised by independent external experts accountable to Parliament, possibly to this committee. Then we will know that mitigations will be actioned, and we will be more assured that they will be funded and therefore more assured that resilience will improve. In that sense, this lacks ambition.

This committee called for the role of a chief risk officer, suitably empowered, to be established across government. That has not happened. The Lords Risk Assessment and Risk Planning Committee called for a national resilience institute to oversee, independently from outside government, resilience overall. Again, that has not happened. The sort of industry best practice that we call three lines of defence does not appear in an overarching risk management framework. In that sense, I think, ambition is lacking.

The Chair: Although we are assured that resilience is now taken very seriously. What the three of you are saying so far—I will come to Ms Braw in a moment—is that you do not think the structures match the ambition of the words.

Lord Harris of Haringey: I talked about the political structure at the top, but there is also an issue about the organisational structure in government itself. Yes, there is a new resilience director; the post-holder, Mary Jones, is extremely good and highly impressive. However, as I understand it she has a dual reporting line, which never inspires confidence; there is one line into the deputy national security adviser and one to the head of strategy in the Cabinet Office. Put yourself in the position of a resilience director trying to get directors-general in other government departments to take things seriously and you wonder whether those structures are strong enough and robust enough in the circumstances.

The Chair: Ms Braw, sorry I should have come to you before.

Elisabeth Braw: I assume you are still on the question of whether the title of this document waters down the original intent—as Lord Harris said, it does suggest that—and when it comes to the political weight behind this document. It also matters in the selling of the document to the public; since it is a whole-of-society strategy, it has to be sold as a concept to the public, including the private sector. Going from the original intention of a strategy to a framework suggests, maybe unintentionally, that the Government may not be as serious about resilience as they originally said they were. That is a great shame, since societal resilience is the area where we as the UK have the most opportunity to improve the

state of affairs and the security of the country, as threats keep changing and threats outside the military domains keep growing.

Q2 **The Chair:** Clearly, you all think there are problems with these structures. Do you think the problems are such that they could have a significant effect on our ability to respond to or recover from any major shocks?

Rois Ni Thuama: If left unaddressed, certainly, but there could be minor refinements where we could see some major outcomes. For example, in the first six pages of that document there is a source to the DIT and there is the supply chain resilience framework. If you are a business in this country and you hit on that infographic—we need information to be accessible, digestible and actionable—what is notable by its absence is a pillar on cyber, but we have all the information.

The National Cyber Security Centre is pre-eminent, and even in the private sector we look to the NCSC for guidance and help. We have thousands of CVEs and millions of unique malicious objects, and it is very untidy and difficult for businesses to deal with all this stuff because of the noise. It is a shame, then, that the DIT has omitted this significant pillar, because if any business or critical national infrastructure or the Government are to lose, it will likely be through supply chain attacks, which is something we need to address.

The Chair: From what you were saying about an excellent civil servant reporting to two places, Lord Harris, it sounds as though you think perhaps that there should have been a director-general associated with this field to give you that clear sense of authority and potential power.

Lord Harris of Haringey: That would have been important. It should not matter. You would hope that all civil servants and all Ministers would take these things seriously. The reality, as we know, is that that is not the way it happens. I am quite taken with something that Oliver Letwin wrote for the National Preparedness Commission, which I chair, where he asked, "Why we do not just enact a national resilience Act modelled on the Climate Change Act and thereby establish a national resilience committee modelled on the Climate Change Committee? Without a mechanism of this sort to focus the mind of government on national resilience, we can be sure that Britain will remain singularly ill-prepared to meet a range of crises". Of course, he held that sort of role for a number of years. He talks about the dynamics of Whitehall combining to get these things working properly.

The Chair: I see you nodding, Mr Ginns.

James Ginns: I would agree with Lord Harris. The absence of what we call the three lines of defence in the private sector means that we will not achieve clear accountabilities for exactly who owns and mitigates different risks. I do not think this structure will allow us to avoid silos in different departments, which has inhibited response in the past.

The Chair: Indeed it has.

James Ginns: I do not think we will avoid risk incubating under the surface here, or that we will effectively challenge group think, which has been another problem in the past.

Q3 **Stephen McPartland:** I will start with Ms Braw so she is not left out. The recent refresh of the integrated review has pledged to build on the resilience framework to create a new operating model for security, described as security through resilience. Is there a risk that this could prevent the Government from focusing distinctly on resilience, absorbing it more into defence or foreign policy?

Elisabeth Braw: I appreciate you bringing me in first, and I am sorry I cannot be there in person.

The challenge is: how do you bring in the rest of society? The Government are only one actor in societal resilience and the framework is ambitious in describing what it wants the Government to do at all levels of society. How do you bring in the rest of society, especially considering that so much of such a large chunk of the private sector that is crucial for the continuity of society is privately owned, for example?

What is described in the framework makes absolute sense and there is nothing objectionable about it. It is just incomplete, because it does not describe or outline how the private sector should be integrated into these plans beyond saying that the plans should exist. One area is exercises. Exercises are indispensable, which is why the Armed Forces keep exercising all the time. They exercise to find out the gaps in the theoretical plans that they have on pieces of paper—now in the cloud, I am sure.

However, you do not find out what the gaps are by studying those pieces of paper over and over. You find out what they are by exercising. That is an area where so much could be done at not very great expense, because companies will be happy to participate free of charge. It is in their interest to help to eliminate gaps in contingency planning, and, as we saw with Covid, not many companies were prepared and had to improvise on the spot. I hope that answers your question somewhat.

In other areas, of course, wider society, which I think means the rest of us ordinary citizens and the role we can play in that scenario, is unfortunately almost completely left out of the framework, because there is no clear organisation in the UK Government that could deal with the population. The framework instead talks about the local resilience forums and voluntary organisations, which is fine, but how are they supposed to bring in the wider population, and what are they supposed to do with the wider population apart from communicate to them?

I hope that answers your question. I am happy to add further details if needed.

James Ginns: My view is that the danger of this is implied in your question. Resilience could be seen increasingly through a national security lens rather than being seen across the whole broad spectrum of

risk that we face. I know this committee has warned before about the NCSC being overly focused on defence and foreign policy issues. I am concerned that with this phrase "security through resilience" we will end up with an overly skewed focus on national security, if we are not careful.

Lord Harris of Haringey: Clearly, if you are more resilient, you are more secure and better able to deal with external threats, the threats that the integrated review refresh is focused on. However, you also need to be resilient against all sorts of other threats, all sorts of other things that can happen—natural catastrophes, things that might be triggered by organised crime, all of that. There has to be a holistic approach.

There is a danger that if you silo-ise it too much—if you can use the word "silo-ise"; I hope you know what I mean—there is this, "Oh, we'll deal with this", and nobody is looking at the systemic consequences or the fact that risks will not arise that neatly fall into one category or another. The chances are that two things will happen at once. If you have a natural disaster, you may well find that nations that are hostile to you will use that opportunity to try to undermine confidence in your emergency arrangements, in what the Government are doing and so on.

These things will happen together and they will interact. The approach that is taken in the document on lead departments makes sense in so far as you must use the expertise and the knowledge of those lead departments, but there is also a danger that those lead departments just think in terms of that area of activity. They may even be too close to some of the key providers in that area and not look at the wider context.

There has to be somebody or some part of government that is in charge of the system-wide effect on all different types of activity. That is one part of the whole of society strategy, as well as what Elisabeth has been talking about: making sure that you involve every level of government, every type of business, every community and, indeed, every household in some way in building greater resilience.

Rois Ni Thuama: To build on Lord Harris's point, we may very well face risks that we cannot know about at the moment. The trouble is that we are facing known threats and we are not addressing them. The fundamental principle of criminology is that crime follows opportunity. We are a bed of opportunity for bad actors and not sophisticated nation state actors, because we are not making it difficult for anybody to get into our businesses. Ninety-seven per cent of businesses across the country are SMEs. It is not trivial to oblige them to conform with certain things from cyber.

To Lord Harris's point about there being a business centre, for example, this cyber governance and cyber risk belongs as a conversation at board level and with business. Although the National Cyber Security Centre is doing a fantastic job, in my view, it is not its job to further drive these good business practices throughout the country.

Stephen McPartland: If you were a small business, would you feel that

you were incredibly unprotected right now when it comes to cybersecurity in the UK?

Rois Ni Thuama: I think it is unduly burdensome to expect smaller businesses to stick to the knitting and do what they do to build their business and to look at the incredibly complex area that is cybersecurity. That is why the National Cyber Security Centre should be a source for these businesses. To expect them to pivot from one department into another department to try to find the best practice is unduly burdensome for the smaller businesses.

Stephen McPartland: Would you consider that to be one of the main obstacles to achieving this new operating model: that small businesses just do not have the bandwidth, capacity or skills to do what would be required?

Rois Ni Thuama: Yes, and with the right tool it would be a trivial matter to see what small businesses look like across the country to determine to what extent they are protected. That is not difficult technically.

Stephen McPartland: Can I widen the question out to the other witnesses and ask what they feel the main obstacles are to achieving this new operation strategy?

Lord Harris of Haringey: There is a real issue here about the ability of government to engage effectively with business, communities and the voluntary sector. It is not geared up to do that. Government likes to think that there is somebody it can call and it will just happen. It is a bit like Henry Kissinger saying, "Who do I call when I want Europe?" There is no single point; at least, there was not when he was asking the question.

If you want the business community to do something, it is not just a question of getting some of the largest corporations in the country into a room and telling them what is needed. There is this enormous structure of small and medium-sized enterprises that also need to be told what is needed. Similarly, if you want to engage the community sector, it is not just about talking to the largest voluntary organisations in the country, because most of these things will have to happen at a local level.

There is a failure perhaps to understand the scale of what is needed and a failure to know how to do it. There are lots of fine words in all the documents about partnership, and I am all for partnership, but I am not sure that government quite understands that partnership means a relationship between equal parties who are listening to each other and know how to do that. There is an assumption that you can cut corners, as far as that is concerned. That leads to weakness, because you get effective resilience, effective preparedness, only if you have, if you like, a herd immunity where every organisation, community and household is taking the appropriate and proportionate steps. Whatever the threat—whether it is a threat from cyber, the threat of a water shortage or the threat of a disruption to food supplies—you want every part of society to be taking the appropriate and proportionate measures.

James Ginns: I would build on that by going back to the structural point that we made at the beginning: that we need an overarching risk management framework across government that avoids silos, so we avoid a national security silo, we avoid a civil contingency silo—that was stressed in the resilience framework—and we look at something that goes right across government. The role of a chief risk officer is crucial, somebody who has a mandate across government who is suitably empowered to look at the full spectrum of risk across the board.

Elisabeth Braw: It is important to remember that businesses are the front line in the geopolitical stand-off that is unfolding and intensifying at the moment. As a result, companies are extremely exposed to whatever the other side thinks. We have seen companies try to leave Russia only to find their assets frozen. We have seen the pipelines of certain companies which they co-own and are co-investors of being sabotaged to the tune of several billion euros lost. We have also seen companies struggling to leave China. We have seen companies being penalised by the Chinese Government when their home Governments have said something that the Chinese Government took exception to: for example, Australia's winemakers lost 97% of their exports when the Australian Government asked for an investigation into the origins of Covid and China then imposed punitive tariffs on Australian wine.

All that means that companies are extremely exposed. They are not prepared for this risk and they are not in a position to handle it on their own, because it goes beyond the operations of a single business. At the same time, insurance companies are saying that it goes beyond them, too. We have seen Lloyd's of London saying, "We no longer insure against state-backed cyber incidents". Of course, it is hard to know how exactly it defines state-backed, since it is an insurance organisation, not a Government. Nevertheless, all this is happening, which makes it even more important to have this regular consultation between government and companies.

The challenge there is how you select the companies or the executives that the Government interact with regularly. The few times this has been tried, the Government have stumbled over the issue of competition. Do you give companies that are invited to engage in dialogue with the Government an unfair commercial advantage? I do not think so, but that is where they have stumbled every time. Some Governments have managed to figure it out. Finland and the Czech Republic, for example, have just invited companies and let the chips fall where they may. Those are the challenges. I think there are ways out of it.

Q4 **Lord Butler of Brockwell:** I wanted to ask about the replacement of the Civil Contingencies Secretariat by the Resilience Directorate and the COBR unit, and what you think the impact of that was. As I interpreted it, this was about having the COBR unit to deal with the current crisis and the Resilience Directorate to have the long-term planning. That seemed to me to be really rather a sensible change. Do you agree?

Lord Harris of Haringey: I think the risk that they were trying to mitigate by creating the two separate structures was the risk that the immediate—what is done by the COBR unit—squeezes out more strategic and longer-term thinking. I understand that and I accept that.

What slightly worries me is that if you have two separate structures that are not properly integrated, you may not get enough of the learning from one feeding into the considerations of the other. That is the danger. Ultimately, if you are talking about splitting between two places the adequate level of resource that went into the old Civil Contingencies Secretariat, you will not necessarily get a better result unless you have increased the amount of resources available, the amount of people who are doing the work. Ultimately, it will come down to how much this is being resourced, how much they work together and how much clout they have within the government machine.

James Ginns: I would tend to agree with that, although I think it is a welcome step to separate the immediate crisis response from the longer-term focus on resilience. In the past, the longer term has been neglected, and it is important that consideration is given to lower-probability catastrophic risk events. The longer term needs more focus, and this structure has a chance to achieve that and tackle something that has been neglected. To that extent, I would welcome it, subject to the structural point that we made earlier.

Lord Harris of Haringey: But there is a risk from having lots of little separate units, and in various parts of the different documents you see that there is a unit that will be doing this, another unit that will be looking after democracy, and all these things are going to happen. You have separate centres of excellence being created. I am sure each of them has a value, but if, at the same time, you have a series of different interlocking strategies, there is a real risk that you are creating new vulnerabilities because you have fragmented the whole structure. The question then comes back: who has an overview of the overall position? Who is able to make those assessments and balance out all those different structures?

Lord Butler of Brockwell: What struck me about it was that the COBR unit should not be fully employed. What will it do when there is not a current crisis? Under the old secretariat there were the dual roles. I am not quite sure what the COBR unit will be doing when there is no crisis to deal with, a fire to put out.

Lord Harris of Haringey: It could be doing exercises.

The Chair: That is exactly what I was just thinking.

Lord Butler of Brockwell: Oh yes, of course.

Lord Harris of Haringey: That would be very useful. I do not know whether that is the case. That was also why you would sometimes have spare capacity in the COBR unit, which could then be thinking about

strategy. You have lost that capacity by separating it out, but I hesitate to say, in answering questions from you, how best to manage the Civil Service.

Lord Butler of Brockwell: I did not like resources to be unemployed. Anyway, thank you. That is a very adequate answer.

The Chair: If they are not intended to do that, they should be.

Lord Butler of Brockwell: Yes, quite. Thank you.

Q5 **Baroness Fall:** Can I ask a question on the back of that? Given that we talk about systemic challenges such as China—I will not name them all, but if you think about economy, national security, sovereignty and human rights, to name a few—does this more devolved approach mean that we are not able to mount a systemic challenge back?

Lord Harris of Haringey: That is the risk: that because there is no overview looking at the whole system, we will not necessarily respond to something that may be a very hybrid attack or a combination of different threats and issues happening simultaneously. You can have the problems associated with a drought, extreme heat, bad weather and everything else, but if it is exacerbated by disruption to your supply lines because of things that are happening internationally and then you have cyber consequences, you need to have a holistic approach to this. There is a danger that you go down the road of looking at this risk by risk rather than taking a threat or risk-neutral approach, which is: what are the consequences that we now need to mitigate?

If I can give a very simple example, we all know that at the beginning of Covid there was a sudden desire to think about how we channel help to people who live on their own and are vulnerable. A lot of effort was made, volunteers were sought and everything else. Most of the volunteers, incidentally, were never called, but that is by the by. The need to be able to identify and support vulnerable people living on their own is true in a pandemic, and it would be true in a drought and in a flood. You need to address the consequence rather than worry about whether this is a Covid-related response or a flood-related response.

Elisabeth Braw: It is a very relevant question. On the one hand, we have an authoritarian country—China, or indeed other countries—and on the other hand we have the UK, where we might say that that is a devolved responsibility and nothing to do with the centre of government. That will not impress anybody. We have the opportunity, or the potential, to work with allies, maybe not within existing frameworks like NATO or, indeed, the European Union but within smaller groupings.

There is the Joint Expeditionary Force, for example, which is obviously a military force. There is that opportunity to work in an alliance that is rather more than an informal grouping involving the UK and like-minded countries in northern Europe. I wonder if the JEF could be an opportunity for the UK to share best practices and to work out the kinks in its dual system by working with closer allies that are very good at that and seeing

what they do. Not all their solutions will be applicable to the UK, because the UK is set up differently. Nevertheless, it can learn from them, particularly the ones in that group that have come quite a bit further than the UK.

Work could be done in that group essentially to put up a combined shield to say, for example, that we have multinational companies in all our countries and they are vulnerable, but we have thought about it and we have exercised it, including with the companies. Even if China, Russia or any other country were to target our civil society, including our companies, we would have a good idea of what to do, including mutual assistance in this group of nations.

Q6 **Lord Robathan:** The Government plan to expand their risk assessment model to look broadly at vulnerabilities. I detected a certain amount of scepticism in the panel about the resilience framework, scepticism that I share. We have talked a little bit about who owns different risks, a holistic approach, silos, two reporting chains, and so on. I would like to tease out a little your suggestion of an overview. How well suited is Whitehall to working in a broad manner when the vulnerabilities that we are talking about are likely to cut across so many policy areas?

Lord Harris of Haringey: My own view is that we are too departmentally focused, which makes it very difficult necessarily to have a co-ordinated approach. If it cuts across different government departments, two Secretaries of State do not agree and ultimately it can be resolved only by going to Cabinet or the Prime Minister, that is often not the best way of resolving these issues.

There is the difficulty of how you grasp it. It is too big for the Department of Health and Social Care or for the Department for Education. The Cabinet Office is actually quite a weak central department, which creates some real issues. There is a genuine problem there. The Government have made some changes to the way they carry out the national security risk assessment. Those are positive changes; I do not decry those. Some risks will now be assessed over a five-year period rather than a two-year period. Two years was much too short a timeframe. I seem to recall a time—again, there will be others who know more about this than I do—when there were full-scale assessments that looked five years ahead and 20 years ahead. The Ministry of Defence produces a process that looks 20 or 30 years ahead.

You have to look at it in those contexts and see developing trends. A distinction is drawn between chronic and acute risks. You also need to have within that developing risks: something is moving quite slowly, but you can see that over the next five or 10 years it will become significant. You ought to be taking account of that now. It is important to look at chronic risks as well as acute risks, but you must not lose track of that picture.

I have already made this point, but I will make it one more time: resilience needs to be multidimensional. You need to be able to deal with

more than one thing at a time. You will do that only if you have that overview, and I do not think that government—this is not a political point; it is any government structure in this country—has a particularly good way of dealing with that across that.

There is an emphasis in the framework on what are called civil contingencies risks. As far as I can work out, that implies that you are excluding domestic, financial, organisational or social risks. I am simply not sure that this is a helpful distinction. I can understand the point that this is a risk that is there all the time and we have a government department that deals with it, so let them get on with it rather than involving the centre in that. However, the overall resilience of the nation is affected by those problems. You may say, for example, that the NHS is a continuing issue which the Department of Health and Social Care deals with, so we are not going to look at it centrally. But if you have risks that are affecting the nation and work on the assumption that you have a functioning health economy, not looking at that in the round is a danger.

So I am not quite sure that separating out civil contingencies risks from the rest is terribly helpful, because it militates against looking at systemic and interconnected risks.

Elisabeth Braw: I want to add to Lord Harris's point and to the original question about how we discern emerging threats, where they are located and their nature. It is useful to think about the Roman Catholic Church, which has a formidable global organisation of people who are on the ground in every corner of the world where they are permitted to be. They see what is around them on the ground and feed that information into the system. It is completely open information, a secret to nobody. As a result, the Roman Catholic Church has an incredible overview of what is going on in the world, including in the remotest corners.

Western Governments have access to the same information through companies of theirs that operate all over the world, including in remote areas far away from capitals. We must remember that diplomats usually stay in the capital, and if it is a dangerous country they very much stay in the capital, whereas companies are out and about in the country, including with managers on the ground. If the Government were to have regular dialogue with companies, with executives, they would get a much better understanding of emerging risks in a number of very risky countries and, indeed, in less risky countries—information that may have eluded the intelligence professionals and diplomats the UK has all over the world—simply because business people operate in different areas and regions of countries and look at different aspects of those countries.

Rois Ni Thuama: I am not entirely pessimistic. We cannot let the best be the enemy of the good, and there are some minor changes. The risk that we face, certainly in cyber, is that there is this expectation that there will be some emergent new sophisticated technology, like Stuxnet, that will be unforeseeable and will do an awful lot of harm. Because we are looking to the horizon for that black swan event, we are not doing the things that we need to be doing that we know now will make a difference.

I mentioned the minimum cybersecurity standard. It is six pages. It is National Cyber Security Centre guidance. If every government department, every critical national infrastructure and every supplier to the CNI was to configure its digital assets to conform with that best practice, we would see immeasurable difference quickly. It could be done in weeks, if not months.

James Ginns: Lord Harris made the point about the overarching risk management framework and its role in co-ordinating assessment across government. That would be very helpful, co-ordinated by a chief risk officer, as I have said.

I welcome the focus and the framing around vulnerability. That is a good development. We do not learn much from these documents about how that is to be done. It needs to be impact driven, so driven from the risk. There needs to be a good look at the strength of existing mitigations and crisis response capability, the source of the risk and how much control we have over that. All those feed into vulnerability assessment.

I agree entirely with Lord Harris on the time horizons. I think 15 years at least is necessary for the NSRA to get a grip of some of the slightly longer-term risks that lie ahead. I would also support an emerging risk log to keep track of risks that are developing and emerging, possibly even beyond that timeframe.

Mitigation of the vulnerabilities is crucial—and, again, not much in the documents speaks to that—but assigning mitigations to accountable owners in government with accountable timeframes for putting those mitigations into place is key. We come back again to accountabilities.

Q7 **Angus Brendan MacNeil:** There is some interesting stuff there on black swans, the known knowns and what have you. The Government have been informing the way they assess risk, including separating acute and chronic risks into separate processes, looking at longer timescales and inviting more external challenge, including through an annual report to Parliament. Does this go far enough, and what would you like to do to reform the national security risk assessment and make it more transparent? I am also drawn to just doing some of the easy stuff, the known knowns, that Rois Ni Thuama mentioned.

Lord Harris of Haringey: I think I have already made the point that some of the improvements that have been made to the national risk assessment process are extremely valuable. Moving the framework for at least some of the risk from two years to five years is valuable. I do think there is a need to look at both chronic and acute risk. I would also include developing risks, as we have mentioned.

The point that James Ginns has just made about being clear what mitigations you put in place is essential, but first you need to have a baseline assessment of where our vulnerabilities are. There is a reference in the document to producing something of that nature, and that should be what informs the extent to which you put various mitigations in place.

There needs to be transparency about all this. I accept that there will be some areas where, for national security reasons, it may be difficult to be entirely transparent, but in the annual report that is to be produced as a result of the resilience framework, and which I assume will come to Parliament, there should be an opportunity to go through all that and an opportunity for a parliamentary committee such as this or other committees to look at this in some detail and to see how significant or how effective the mitigations are that have been put in place and what the justifications are.

In the last iteration of the national risk register, there are mitigations listed against each of the risks. I appreciate that it is now out of date and there will be a new one in perhaps a few weeks' time. I have no sense as to how that has been weighted. I think it says that £5 billion will be spent on flood defences over the next six years—or £6 billion over the next five years, I cannot remember. How has that figure been arrived at, and how does that relate to the mitigations put in place for some of the other 37-odd risks that are listed in the risk register? Has that assessment been done? Where does that happen? I assume that the new process of risk assessment will make that clearer, more transparent and more rational. I assume that there will be a mechanism through the annual report to Parliament that will enable there to be some scrutiny of that and to understand the nature of the decisions and the choices that have had to be made by government.

Angus Brendan MacNeil: While I have you there, you mentioned earlier supply line risks and associated things, and it made me think of risk aggregates. Of course, there is a great political elephant in the room in the UK in much of the dialogue, and that is Brexit. What does that do to the risk and aggregated risks? Does that make things less or more risky? I have asked that question as openly as I could. It is the elephant in the room. That is the problem. It is one of the biggest risks.

Rois Ni Thuama: I will not address exactly Brexit, but I will say that while we are sitting still and not legislating for this stuff the EU is taking a charge. For example, the Digital Operational Resilience Act will come into play across Europe, and any financial entity that has an interest in Europe will need to comply. It has taken a whole of society approach in a way for the financial entities and ICT third party suppliers—to your point about the supply chain. Its risk management is that the board bears final responsibility.

As we look at businesses and talk about risk, as I said earlier, my concern is that we are looking for this black swan event when really we need to deal with the belts and braces. Ultimately, the pain will be in whether it was foreseeable, whether it was reasonably avoidable and whether it witness proportionate to avoid it. All those things will make up an inquiry later on if we do not address them. The EU is stealing the march on us there with the Digital Operational Resilience Act and it is conforming with best practice. To be honest, if you read it, you would think it was written by the National Cyber Security Centre. It is a sensible document that will make its financial entities more resilient.

There is another interesting thing coming out of Europe: the collective redress directive. That will come into play in June, but of course it would affect any British businesses that suffer from a data breach. Traditionally in the United States we have seen an appetite for class actions, and it has looked as if Europeans perhaps do not have the same stomach for it, but actually it was the absence of a mechanism. That is changing in June, and the risk is that businesses that have not implemented sensible procedures in Britain and then suffer a data breach and lose European customers' data are not only subject to the GDPR and the right to private enforcement, but now across every member state will have a qualifying entity that can bring a class action on behalf of those data subjects. There is a lot of movement in Europe. It is making significant strides to protect its financial entities and consumers.

Elisabeth Braw: I want to come back to Angus MacNeil's original question, which is how we catalogue threats. That is how I understood the question, and I hope I am correct. The crucial difference is between manmade risks and nature-made risks, and this is where we are entering new territory. Until recently, we mostly had to worry about mother nature and what she can do to our societies. Now we are seeing an enormous increase in manmade threats, and the defining nature of those threats is that they are unpredictable. That is what makes them so powerful.

Whatever the Governments of Russia, China or any other state and state-backed actors that may wish us ill or to do us harm think up we have to be prepared for. We have no way of knowing what they are thinking up, because once they have tried something they are unlikely to try that again. That is a massive challenge. The result of such threats increasing is that we cannot even hope to blunt every threat or harm that comes our way, but we can be generally prepared. That is what we have to hope for, and we can try to accumulate indications of what Governments may be up to and what their thinking is. AI will be a useful tool to help, constantly sucking up indication signals from all over the world.

The manmade threats are also so risky because insurance cannot keep up. Insurance can only insure what it can quantify and model, and as a result price, but if it cannot model it it cannot price it, so it cannot cover it. That puts additional pressure on Governments to try at least to thwart or blunt some of the impact when those things happen.

James Ginns: On the cataloguing point, the acute chronic differentiation is quite interesting. We need to make sure that we do not end up with a secondary or subordinate register for the chronic. We just need to make sure that we keep both in view and that we look at vulnerabilities across both types of risk—the acute and the chronic—in this terminology. Vulnerability assessment is being applied mainly to the chronic, if I read the latest refresh of the integrated review rightly. That is where the vulnerability assessment is being focused. It needs to be applied to both.

As I have said, it is terribly important not to lose sight of risk that is of low probability but high impact, and some of the more catastrophic risk,

and that we keep that in view. It is stressed in the original integrated review 2021, but is not referred to in the latest version.

Lord Harris of Haringey: There are a whole series of global ambitions set out in the integrated review refresh, which are all fine and wonderful, but of course they rely on other international partners assisting that, whether it is the EU or other allies or colleagues. The implication is that we cannot always rely on those international friends, whether they are in Europe or elsewhere, to assist us. In practice, we have to build a capacity for flexibility, adaptability and resourcefulness in a fragmented and turbulent environment. What we should be building is a general capacity to deal with whatever may be coming towards us.

Q8 **Viscount Stansgate:** Good afternoon. It has been a tremendously interesting session so far. I had a couple of questions, but I ought to tell you that I wish they were asked earlier, and I think they have been answered earlier, in particular by Lord Harris, so I will tell you what one of them was in case anyone wants to add anything.

The resilience framework seems to reaffirm the lead government department model, with each government department managing its own risks. Is that the right approach, or should central government do more to ensure that all departments are held accountable for their actions? In other words, should there be more activity at the centre. I think from Lord Harris's comments so far that the answer would be very much yes, but does anyone else want to add anything before we move on?

The Chair: First, is he correct, Lord Harris? I think he is.

Lord Harris of Haringey: Yes, I think that Lord Stansgate is highlighting the issue. My concern about just leaving it to the lead government departments is that nobody else takes any notice of what is happening there. They may be quite close: if they are responsible for energy, for example, they will be very close to the energy supply sector or whatever else it might be, and not necessarily look at the other factors. Yes, there should be a mechanism in central government for marking the homework, seeing how far they have got, whether they are building the resilience that matters. Again, the emphasis on lead government departments is likely to lead to a fragmentation, which would be inadequate to deal with the systemic risks, cross-cutting risks, interconnected risks.

James Ginns: I completely agree. The oversight needs to be strong, and needs to come from the centre and from outside the departments that own the risk. That is a basic principle of risk management that applies to government just as it applies to the private sector.

Q9 **Viscount Stansgate:** Moving on to a second question, it is quite clear—and reference has already been made by the witnesses to the fact—that it helps to have senior ministerial attention, and Ministers who have been particularly prominent in allocating their time and attention to these issues have been fairly good at it. What more could the Government do to incentivise departments to invest in resilience measures?

Elisabeth Braw: I do not want to criticise the UK Government, but I will give an example. The new Swedish Government have a Minister whose portfolio is civil defence. He has an all-encompassing responsibility; he is the No. 2 Minister in the defence department. I wonder if such a model would be suitable for the UK. Far be it for me to opine on ministerial appointments, but it seems to make sense that he has this whole portfolio, including the different agencies, whereas in the UK it seems to have landed mostly on the Civil Service, with a passing string of Ministers having various responsibilities in their portfolios.

Lord Harris of Haringey: I mentioned earlier the argument that there could be a national resilience Act modelled on the Climate Change Act. The point about the Climate Change Act was that it placed a duty on government departments and on agencies to work towards net zero. A national resilience Act places an obligation on government departments to make sure that they are resilient and robust to various external threats. That would create a continued ratchet and pressure to try to improve the resilience of the nation, with every government department and every government agency having to take it seriously. I mentioned Oliver Letwin earlier. He had some trenchant remarks about the way the Treasury reacts to those things. If there is a legislative framework that requires it, that could be helpful.

Viscount Stansgate: Lord Harris, would it be fair to say that, in the absence of a national resilience Act of the kind you mentioned, it will be rather difficult to get departments to be incentivised in resilience management and preparation?

Lord Harris of Haringey: The very nature of resilience is that you need to invest resources into something that you might not need. You are investing resources into something that is looking beyond the immediate. That is very difficult for any government department, for any government Minister. It is what I call the NIMTO syndrome, the not in my term of office syndrome. You do not feel the obligation to do it, because you will not be there when it happens. This framework of having a national resilience Act would require that you did have to look at it.

It is very difficult for elected politicians—I have been one and there are plenty of people in this room who have been in the past—and all those running it to have that longer-term agenda. It is the same in business, where the focus is increasingly on annual returns or quarterly figures and so on, rather than looking at the long-term future of the business. You need to get around that NIMTO effect, and find a way of doing that. Some sort of legislative framework, some sort of system of regulation, is the way forward to it.

I am always reminded of the Mayor of Fudai. He a remarkable man in some ways because he was re-elected as mayor about 10 times, or something like that, but he courted complete ridicule for his insistence on building a huge flood wall and floodgates to protect the town of Fudai in Japan. It was only when the tsunami happened 10 years or so ago and his town was the one that survived without serious devastation that

people realised his foresight. Of course, by then he was long dead and the only response of the citizens was to lay flowers on his grave. That was an example of foresight, which is very difficult for politicians to have looking at that distance with that sort of requirement.

Viscount Stansgate: Thank you very much for that. Let us hope we do not have to buy flowers in our case, but in the meantime thank you all very much for your answers.

Q10 **Baroness Fall:** Thank you for your time today. I want to turn to the role of society and the local tier in building up resistance. The Government now seem to recognise that local resilience forums need more resource, along with clarity on their roles and responsibilities. There is no very clear idea of their duty, their purpose, how often they meet, who they report to centrally and, of course, the funding model, given the fiscal outlook that remains challenging. What do you think about the Government's actions so far? Have they gone far enough to address the concerns set out by many stakeholders, including our own committee?

Lord Harris of Haringey: First, there is at last a recognition of the importance of local resilience forums. They have a 20-year history and in many instances have been quite variable. It was noticeable how, initially at least, they seemed to be ignored during the Covid emergency and then gradually got more and more prominence as it was recognised that they were significant. At the moment, the level of resources they have in different parts of the country remain variable. There is no regime for properly monitoring their effectiveness, and the extent to which they are politically engaged and politically led in different places differs. The London Resilience Forum is chaired by one of the deputy mayors of London. It is clearly linked into political structures, and there are parallel structures with the local authorities. That is not the case around the rest of the country, and in some instances it would be quite difficult to manage because of the way in which local government is structured.

The Government say they are putting extra resource into local resilience forums. I think you are right in saying that the expectations of local resilience forums and what they will do should be clear and they should be resourced accordingly. I am not clear whether this chunk of extra money that is being given will be continued in the future. It certainly cannot be based on just one-year grants that are then renewed. You must be able to build a long-term set of relationships and a long-term set of structures. That funding is not available.

We mentioned exercising earlier. I would like to see every local resilience forum having a major multiagency exercise each year as part of testing the structures and the nature of the partnerships between local government, emergency services, and the other key partners and areas. I do not think there is enough formal engagement with the local business community, and the relationships with the local voluntary and community sector are often fairly fragmented.

The probable reason for that in both instances, but certainly in the case of the voluntary and community sector, is that there is no local co-ordinating infrastructure. There will be separate individual voluntary organisations. In a local authority area, there might be a council for voluntary service that might co-ordinate the activities of local community organisations, but that will be very patchy. There is no single mechanism to do that. If you want to co-ordinate the activities of the voluntary and community sector, you probably need to put some resources into that infrastructure to make it happen. There is probably also a need to have some regional local resilience structures, so that you have national, regional, local and possibly very local structures in place. I think there is a lot more investment that could be done in those areas.

It is also an anomaly, if I am right, that the duties that are placed on the category 1 responders in local resilience forums are not placed in the same way on government departments or the devolved Administrations. You would like to see everybody swimming in the same direction with a clear understanding of their responsibilities.

The other thing that is missing is a proper assurance regime so that you can see which local resilience forums are able to carry their responsibilities forward effectively. That needs to be developed.

Q11 **Baroness Fall:** I have one further question, on comms. We saw the strength and the power of comms during the Covid crisis, which was pretty centralised with the daily press meeting at No. 10, and very strong messaging. Of course, social media means that that can infiltrate very strongly. Is there a problem with the juxtaposition of a local decentralised form of community resilience planning against this very strong centralised comms model? Could you see that evolving over time?

Lord Harris of Haringey: What is important in an emergency is first that there is clarity of message, that people understand what is being said and what is expected of them. That requires trust from the public in who is delivering that message. It also requires the same message to be given at different levels. It is quite possible to co-ordinate that. By and large during the pandemic there was that consistency of message at various levels. When there was not, that may simply have been the fatigue of going through a pandemic of that length; I will not get into citing things about parties in Downing Street or any of that, but the point was that it went on a long time.

However, certainly initially some very clear messages were given centrally and were being repeated by local authorities. We have done some work at the National Preparedness Commission looking at some of the local initiatives and messaging, and a lot of effort was made to make that consistent and to ensure that those clear points were put across.

You also need to communicate the resilience message in peacetime, in normal times, which is not something that we do in this country. In Sweden—Elisabeth Braw will be able to say far more about this than I can—there is a booklet that goes to every household that tells you what

to do in the event of an emergency. It gives you practical advice on what things you should keep in the store cupboard, what to do if the toilets stop flushing, your emergency supplies of various sorts. We do not do that in this country, yet I am sure that building up household and community resilience in that way would be of enormous value.

Elisabeth Braw: The UK has a fantastic basis of community engagement outside the resilience forums, to go back to the previous question. The people who made a huge difference during the pandemic—the participants in a DofE scheme who came through in so many ways, teenagers who know what to do in a crisis and have a range of skills, for example—had not been prepared for a pandemic, but they existed in this organisation and the DofE was able to ask them to help elderly neighbours, isolated neighbours and so forth. There is a huge community of people who are already involved in their local communities and in preparedness in a wider sense, but they are not linked to the local resilience forums.

If I may make a wider philosophical point, there is a desire in our society in the UK to make a difference that comes through when there is a crisis, but if we can tap into it before there is a crisis, we will be much better set up when the crisis occurs. On top of that, our society is fragmenting, it is atomising, and this engagement could be a counterforce to that. There is clearly a need for people to be engaged in their communities should there be a natural disaster or something imposed on us by a hostile state. Being engaged with fellow human beings, fellow citizens, would be a very good thing in itself even if there were to be no flooding, no hostile state's act or anything of the kind.

It is so important to have a local, regional, societal, countrywide register of people with particular skills. I vividly remember the Westminster Bridge attack a bit more than six years ago. Tobias Ellwood, who I do not think is here today, just happened to come by and just happened to have first aid skills. What would have happened if Westminster City Council, the Greater London Authority, the Mayor of London or the Government had a database of first aiders in the SW1 area? If Tobias had not happened to come by, there would have been a database of people to call on in that moment. That is just one of many events where it would be useful to have that database of people with critical skills for an emergency.

Q12 **The Chair:** We have been talking more about local resilience forums. How would any of you characterise co-ordination between the devolved Administrations and the Westminster Government on resilience?

Lord Harris of Haringey: Clearly, the devolved Administrations have their own responsibilities. I have limited experience of how the relationship works between the UK Government and the devolved Administrations. You would assume that that could be made to work, although it will often depend on what is happening in the political relationship between the Administrations concerned.

What I am clear about is that in Scotland, Wales and Northern Ireland there are some well-developed structures for managing resilience and civil contingencies. That may be a reflection of the size of the countries—4.5 million or so in Scotland, 2 million in Wales—being a size that enables you to bring together all the relevant players and to do that reasonably effectively.

Elisabeth Braw: I should have added—to Lord Harris's point earlier—that the leaflet in Sweden is called *If Crisis or War Comes.* During the Cold War it was called *If War Comes*, and it returned in 2018 in a new edition called *If Crisis or War Comes*. It is a paper leaflet that is sent out to every household in the country, and it is available on the internet in many languages. It has been copied by other countries since 2018. In 2018, sending this leaflet out to every household in the country seemed like a slightly paranoid thing to do. When 2020 and Covid arrived, it seemed like a very wise thing to do.

Yes, it may seem a bit paranoid and may cause a bit of panic among people when they receive it, but people in earthquake zones for example in Tokyo, San Francisco, New Zealand—I used to live in one—receive such information all the time and do not panic. It is just part of life. If you receive the information and go through it before there is a crisis, you can face the crisis with confidence. That is the point. In the UK we say, "Oh, we wouldn't want to frighten people". They will be even more frightened when the crisis occurs, which is exactly what happened when Covid struck.

Q13 **The Chair:** Yes, good point. I want to ask something about the critical national infrastructure now. There has been discussion about what regulations are imposed on the operators of the critical national infrastructure. The Government seem reluctant to impose more resilience regulations on such operators and, indeed, the National Infrastructure Commission has recommended resilience standards, stress testing and so on. They also seem to be reluctant to follow up on that advice, which does give the impression that they are being advised to adopt a more forceful regulatory stance with regard to the critical national infrastructure. Do any of you have any observations on that? Do you share that view?

Lord Harris of Haringey: I think there is a problem at the moment in that most of the CNI has its own separate, regulatory bodies. The regulatory bodies were created at the time of the privatisation of the industry concerned, and they happened at different dates. They all have a slightly different legislative framework. For most of the regulators their prime focus is economic regulation, it is about price, and they do not necessarily have the powers to engage in looking at the requirements of continuity and resilience. You could use those mechanisms to do so. Certainly, the National Preparedness Commission is looking at getting some work done for us looking at the different regulatory frameworks and how those might be taken forward.

I think it is in the resilience framework rather than the refresh, but there is a statement about government intending to review the existing regulatory regimes, although it does not quite say what it will do about that. The infrastructure sectors operate in a rather different environment and clearly you would expect there to be consistency in the expectations that would be placed on them. There is also an issue, in my view, in that we have a list of what we regard as critical national infrastructure which we discovered during Covid did not cover all the things that really mattered. Perhaps that also needs to be looked at. Some of those are entirely private sector or market driven or are subject to different legislative controls. All that needs to be looked at.

Elisabeth Braw: I have one additional point to what Lord Harris just said, and that is that CNI operators are the perfect companies to involve in exercises. They have a special obligation, and it would be easy to invite them to exercises; indeed, it would be easy to make it mandatory to participate in society-wide themed exercises involving national security contingencies, both manmade ones and ones caused by mother nature.

In addition to the sectors that Lord Harris just mentioned, another sector that should be included is social media, which can be a force for good and a force for a lot of ill in a crisis. At the moment, we clearly do not have a way of telling social media companies to do very much at all along the lines of societal responsibility.

Rois Ni Thuama: So it is on the record, when I said minor refinements and major outcomes, I meant that mandating basics and standards for the CNI so that they would then be compelled to manage their supply chain would have a significant outcome.

I would also like to add this, and maybe I should have mentioned it at the start. The minimum cybersecurity standards contain a number of things that government departments and suppliers to the Government need to do. The United States introduced a similar document in 2018, Binding Operational Directive 18-01, and it has well over 90% compliance, if you compare it with our own 38% for a single signal.

Lord Harris of Haringey: The committee might want to look at the approach in Finland. I think its 2017 Security Strategy for Society sets a whole series of expectations on business operators—particularly the CNI but all businesses, because it extends to other organisations, communities and households—about what is expected as part of the general defence of the nation. It supplements it with regular, high-level defence courses that are for four weeks, so you are asking senior people from industry to meet with senior people in government for four weeks at a time to acquire a whole series of skills and knowledge about what is needed for resilience and the defence of Finnish society.

Elisabeth Braw: If the engagement with industry is just asking industry to do more, possibly without compensation, companies will do the minimum to comply with those requirements. If there is regular engagement, including the kind that Lord Harris just mentioned—the

Finnish national defence course—top executives and their companies are minded to do their part to keep society safe, simply because they know more about it.

The Finnish course, as Lord Harris mentioned, is three and a half weeks residential and does not have to be imposed on executives. It is highly selective. Participants from across society, ranging from academia to the police, are nominated. Almost all MPs have done the course or are doing it, and it is an honour to be selected. You do three and a half weeks of intense training about national security, and you emerge as part of a network of rising leaders, middle managers and higher, who are well informed about national security and know one another. As a result, they know more about what to do in a crisis than the average leader and are more minded to have the organisations help society to prevail in a crisis.

Lord Harris of Haringey: I think participants get a little badge, which they wear with pride. It is a bit like the Légion d'honneur to demonstrate just how they have been selected to do this, they have done this work and they are helping to protect society.

Rois Ni Thuama: To Lord Harris's point about the Finnish example that he used, the Dutch also have a comply or explain; you are not requiring Orville's Bike Shop, for example, to have the same cybersecurity posture as the Bank of England, which might also interest the panel.

Q14 **The Chair:** On a slightly different point, the integrated review refresh puts a significant emphasis on our resilience to hostile state threats. Obviously, everyone will have their own view as to whether our commitments and resources match up to the rhetoric. Do any of you have any observations about that aspect of the integrated review refresh? By the way, you are allowed to criticise the British Government. This is a Select Committee, which is scrutinising the British Government.

Elisabeth Braw: I just did not want to opine on what sort of ministerial portfolios there should be, but I will happily opine about or have an opinion about the integrated review refresh.

The almost unbridgeable gap that we are seeing is that the UK wants to continue to be a free trading nation but with a global footprint for its businesses. But the very nature of the UK is now vulnerability, because hostile states can and are already exploiting it to harm the UK. This is the dilemma that we face after 45 years of globalisation, where expanding the international footprint and making domestic functions and domestic well-being dependent on supplies coming from abroad is a vulnerability all of a sudden. It would require a completely different review to lay out the vulnerabilities that that produces—not just a chapter or one part of an integrated review, but a review independent of the IR to lay out the vulnerabilities that causes and what the Government should do. The reality is that the Government cannot fix that. They can just hope to back up companies that suffer harm as a result of this geopolitical stand-off that we are seeing.

If I can flag up one point in particular, the IR refresh does not address whether we need an additional Pool Re type of organisation to back up companies and insurers that are subjected to hostile states' harm as a result of this geopolitical stand-off. Cyber is covered through Pool Re and there is obviously Flood Re, which does not have anything to do with geopolitics, but do we need additional Re-s, as it were? Can the Government afford to be the back-up for even more potential harm, or should we just accept that companies may have to go out of business due to this geopolitical harm?

Lord Harris of Haringey: Hostile state threats will come in many forms. The whole point about this grey zone warfare is that so much of it is potentially deniable. If there has been a cyber incident, and I defer to Rois Ni Thuama in this, you do not know whether it is a hostile state or an operator who is sponsored by, supported or tolerated by a hostile state. The economic interference may be part of these activities. Again, it may be obvious that it is a state sanction, or it may simply be an instruction to companies of that country that they need to do various things.

In the IR refresh there is a whole section on our democracy in society, and there is to be a defending democracy task force that is focused specifically on foreign interference in electoral processes and infrastructure. I think it needs to have a much wider remit. It needs to look at the whole phenomenon of misinformation and disinformation, the fostering of extremism. The whole objective of this is often to undermine faith in democracy and our systems of government.

We also need to work to rebalance the asymmetry of voice within the wider system, in which social and digital media and so on become a haven for AI-powered bots, conspiracy and extremist groups, all of which are part of this practice of trying to undermine and delegitimise the core electoral systems. It would be very useful to know whether the defending democracy task force is to have that wider remit or something very narrowly looking just at electoral systems.

The Chair: Interesting.

James Ginns: I think the wider remit is the point. We just need to make sure that we keep a view on the full spectrum of risks and not just home in on the hostile state risk.

The Chair: Or at least international terrorism, which has rather gone off the boil just lately. Thank you all very much. We are very grateful to you for your evidence today. It has been a very interesting session.