HOUSE OF COMMONS

Foreign Affairs Committee

Oral evidence: Disinformation diplomacy: How malign actors are seeking to undermine democracy: follow up , HC 1823

Tuesday 14 April 2026

Ordered by the House of Commons to be published on 14 April 2026.

Watch the meeting

Members present: Emily Thornberry (Chair); Fleur Anderson; Aphra Brandreth; Richard Foord; Alan Gemmell; Uma Kumaran; Edward Morello; Sir John Whittingdale.

Questions 1 - 91

Witnesses

I: Kanishka Narayan MP, Minister for AI and Online Safety, Department for Science, Innovation and Technology; Talitha Rowland, Director for Security and Online Harms, Department for Science, Innovation and Technology.

Examination of witnesses

Witnesses: Kanishka Narayan MP and Talitha Rowland.

Q1 **Chair:** We are joined by Minister Narayan, the Minister for AI and Online Safety at DSIT, and Ms Rowland, the Director of Security and Online Harms at DSIT. Thank you very much for joining us. Minister, could you explain to us what your day job is?

Kanishka Narayan: Thank you, Chair, and thank you in particular for both the inquiry that you are conducting as a group and for that generous opener. The fundamental thing I would say is that you will know more than any other part of Parliament that we are in a totally new geopolitical paradigm. AI is the central question in terms of capability for the future of our national security, economic security, and trust in our communities and our democracy.

The crux of my job is to make sure we are doing everything in this country to position us to have that capability and build sovereignty as well as prosperity as a result of AI, but to do so in recognition that this is comparable to—if not even greater than—historically big jumps of significance in military, naval and nuclear capability. We need to take AI as seriously as those big jumps when we are thinking about the future of our public policy. I am very focused on capturing the opportunities of AI economically but also making sure that we are doing so in a way that protects our trust and safety domestically, in terms of AI capability.

Q2 **Chair:** There are potential amendments to the Online Safety Act 2023 through the Crime and Policing Bill. Are you dealing with that?

Kanishka Narayan: Yes.

Q3 **Chair:** Are there also potential amendments in relation to the Representation of the People Act?

Kanishka Narayan: If we speak about very specific amendments, MHCLG is of course the Department leading on it, and we are contributing. I am engaging very closely with my colleagues in MHCLG on the question.

Q4 **Chair:** Are the amendments to the Representation of the People Act about deepfakes, or some of them are?

Kanishka Narayan: Yes. Foreign interference as an offence is very much owned by the Home Office. There are some aspects of deepfakes that I am involved in. The question of personality rights, for example, is a question that is very much in scope for my role.

Q5 **Chair:** Sorry, I missed what you just said. Who is responsible for foreign interference offences?

Kanishka Narayan: As an offence, it is owned by the Home Office.

Q6 **Chair:** Does Ofcom answer to the Home Office then, or to your

Department?

Kanishka Narayan: In its implementation of the online aspects of foreign interference as they relate to the Online Safety Act, Ofcom reports to us in the DSIT context.

Q7 **Chair:** In the context of the foreign interference offences, Ofcom is answerable to whom?

Kanishka Narayan: As you will appreciate, foreign interference offences have a series of offline instances. You will be very well aware of widely covered cases, not least those subject to court action at the moment. Of course, the offline cases are not in the ambit of Ofcom, and so they are dealt with by the Home Office. Regarding online cases related to the foreign interference offence, which come under the ambit of the Online Safety Act, Ofcom is responsible for the implementation of that Act, and DSIT is the oversight Government Department for that.

Talitha Rowland: Ofcom is an independent regulator, so it is accountable to Parliament rather than to DSIT. However, DSIT is the sponsoring Department, so we have a particularly close relationship with it and Ministers meet with it regularly. But Ofcom as an institution is independent and accountable to Parliament.

Q8 **Chair:** Okay. Of course the foreign interference offence does not just come from the Online Safety Act, does it?

Kanishka Narayan: No, not at all. In fact, it is the opposite. The elements of foreign interference covered in the Online Safety Act come from the offence but the foreign interference offence covers offline stuff, which is totally separate from the—

Q9 **Chair:** Let us not talk about offline. We are talking about only online. The online offence of foreign interference does not just come from the Online Safety Act?

Kanishka Narayan: Sorry, that is an independent thing.

Q10 **Chair:** There is another piece of legislation and the two of them come together.

Kanishka Narayan: That is right.

Q11 **Chair:** Are you responsible for ensuring that those offences are in some way prosecuted or that something is done about them?

Kanishka Narayan: Prosecuted? Talitha, I am going to have to rely on you to decide.

Talitha Rowland: You are right. The foreign interference offence sits in the National Security Act 2023. That is a Home Office piece of legislation and it is responsible for how that operates. The Online Safety Act creates a bridge, as it does with lots of different offences. It says, "This is an

offence offline. It's also an offence online, and services have to deal with that content." That is a regulatory regime overseen by Ofcom.

Q12 **Chair:** People watching this might be getting a bit confused. Can I perhaps take it to an example? You may know that there were 1,300 bots created in Iran that pretended to be Scottish nationalists. There were photographs of rather handsome young men wearing kilts and expressing strong views about Scottish independence. It garnered a very large number of followers and produced a lot of pro-Scottish independence propaganda. When the internet went down in the summer in Iran, all the bots disappeared. They then came back and, for a while, forgot who they were and talked about the supreme leader and then they remembered that they were supposed to be Scottish nationalists and went back to talking about Scottish nationalist propaganda. They then came offline again during the recent attack on Iran.

Quite clearly, these were created bots, and there has been a lot of publicity about them. Was what they were doing some sort of offence that has been identified—this new foreign interference offence—through whatever the legislation is, through whatever Department it is that is responsible for that bit of legislation? Have they been responsible for some sort of offence and who is taking responsibility for doing something about it?

Kanishka Narayan: On the first question of whether it is an offence or not, ostensibly it feels totally wrong to me. Given the threshold set in the law, which is that you just need reasonable grounds to infer foreign interference, not conclusive proof of it, without pre-empting the individual cases, to me it would feel like there is a pretty significant case for arguing there is foreign interference there.

In terms of who is responsible, when it comes to the foreign interference offence, in that instance the Online Safety Act would be operable, and so Ofcom is in charge of ensuring that platforms are complying with their duties. Platforms have to make sure that where there are reasonable grounds to infer foreign interference, as it applies to UK residents' experiences, platforms are acting on it and not just acting reactively but proactively. When they are not doing so Ofcom is the regulator in charge that is responsible for enforcing it.

Q13 **Edward Morello:** Minister, given what you have just said, do you use any social media platforms?

Kanishka Narayan: I try to limit it but of course I do, yes.

Q14 **Edward Morello:** In your experience of using social media platforms such as X, do you see any evidence that the social media companies are effectively preventing the spread of misinformation and foreign interference?

Kanishka Narayan: The main thing I would say is that the online experience at the moment for me, and I expect for all of you, is not

satisfactory in a couple of different ways. There might be instances that meet the threshold of illegality, and when those happen, we have a system to take action on those. There is a—

Q15 **Chair:** That is what we want to know. What is the system for dealing with this? Who has dealt with the Iranian bots? Who is responsible for doing it?

Kanishka Narayan: When the foreign interference offence as covered by the Online Safety Act applies, Ofcom is the regulator in charge of ensuring that platforms, which have the duty to comply with their requirements under the Act, are taking action. There is a very clear enforcement path there. There is a broader thing, which was just brought up, which is misinformation as well as foreign interference. The reason I have highlighted the distinction is that there is a huge swathe of information that does not quite meet the threshold of illegality but over time and in its volume chronically erodes trust in public debate and the public sphere online.

I am as concerned about that and we have a series of things that we are focused on in trying to tackle that. However, I have to highlight that over a very, very extended period of time, Parliament decided that those sets of cases—legal but harmful cases—were not to be covered in the same way that illegality in the context of foreign interference is. I just draw that distinction—

Q16 **Chair:** I do not want to talk about that. I want to talk about the Iranian bots. I want to talk just about that because it seems to me that there is no argument about this being anything other than foreign interference in our democracy. What I want to know is which Minister is responsible for dealing with this? I asked Darren Jones, and I asked Dan Jarvis at the Joint Committee on the National Security Strategy, JCNSS. I asked them both when they appeared in front of us at JCNSS and they said that it was not them. They said that it was your Department that was responsible for doing it.

I have written to Ofcom, and I asked Dame Melanie Dawes if she was responsible for the Iranian bots. Obviously, there is more than just Iranian bots but it seems to me that we should have one example and focus on it. What did she say? She said her worry is about the existing provisions under the Online Safety Act. She said, "These are the things that I am supposed to do." She said her concern is that "It's very difficult to prove a breach of the foreign interference offence because the standard is too high and too difficult." She said that she is going to look into it and she will get back to me. She has yet to do so.

She said, "I have to set out above, platforms' responsibility in relation to foreign interference under OSA. However, as you note, the requirement to meet the three conditions in the foreign interference offence is a high bar. We understand that Parliament sought to ensure a balance between tackling foreign interference and the importance of free expression and

legitimate influence activity. As a result, the threshold for platforms having to take action is high, as is the threshold for Ofcom holding platforms to account. None the less, we are working to use the powers that we have to maximum effect." It sounds to me like she is blaming you, or blaming the Government, for not giving her enough power to be able to do what she should do when it comes to the Iranian bots.

Kanishka Narayan: There are two separate questions here. One is the question of who is responsible. You have rightly answered that yourself in that context: Ofcom is responsible for the implementation of the law. There is a separate question from responsibility, which is are the thresholds appropriate at the moment? First, as I mentioned at the outset, the current bar is reasonable grounds to infer, not conclusive proof of foreign interference. By the way, there is not a diminished concern. This is one of the most central questions for our politics—

Chair: It is one of the most central questions for our politics. That is why I do not understand why we are not able to have a senior Minister responsible for ensuring that we are protecting our democracy.

Kanishka Narayan: On the responsibility question, as Ofcom has itself told you, it is responsible for the implementation of the Online Safety Act. I am the junior Minister responsible for it; the Secretary of State is the senior Minister responsible for it. On the question of the legal threshold, which was the second separate question raised in your most recent point, I am very keen on making sure that we are reviewing and looking at where we expanded. I have not seen any evidence at the moment from Ofcom that the low bar I mentioned is insufficient but I will do everything to try to expand that bar if that evidence is there and if it can be an effective way of tackling this challenge that you and I align on.

Q17 **Chair:** Let us put it this way: even if the Iranian bots have not been dealt with by way of the new legislation, if the bar is at the same level presumably there would be an example of foreign interference that had in some way been taken down or dealt with because of this legislation. Could you give me an example of that?

Kanishka Narayan: Platforms have a responsibility to comply with the Act. I suspect there are many cases where they have done so. We do not ask platforms to report every single instance where they have taken action.

Q18 **Chair:** Just one. I want only one. Can the platforms give us—through you—one example where they have taken down attempted foreign interference in our democracy?

Kanishka Narayan: I am very happy to write to the platforms and ask them for data.

Q19 **Chair:** Do you not speak to them on a regular basis?

Kanishka Narayan: I speak to them on a regular basis, and so does the rest of Government.

Q20 **Chair:** Are they spoken to about them defending our democracy against foreign interference?

Kanishka Narayan: I do not ask for data on their internal compliance with the law. The instances of non-compliance and the overall compliance with the legislation are something that Ofcom is responsible for. Of course in this instance, I know they have been in front of you, and I hope they were asked this. I am happy to ask them again in the future.

The other thing I will flag is that the Online Safety Act has been live for materially less than a year. This is not something that has been around for years and years. I want to make sure that it is acting robustly, and we will go further on this question wherever it is required. But this is not something we have longstanding, longitudinal data on.

Q21 **Chair:** I am sorry. It has been around for a year. We have had elections during that year, we have had democracy during that year, and you cannot give us one single example where the platforms have taken down material that has been interfering in our democracy. Do you not think that we are getting a little complacent?

Kanishka Narayan: With respect, the Online Safety Act has been around for less than a year in its implementation of illegal content duties and child safety duties. To my knowledge, we have not had significant national-level elections in that period. That all said, I am as concerned about this question as you are. I am just keen on grounding it in both the fact of the law and urgent action in engaging with the platforms. If you want me to go and seek that evidence then I would happily do so independently too, but we have to make sure that we are proceeding in a way that is grounded in law and where we are.

Talitha Rowland: We know that platforms take down foreign interference content. They publish some of that. I know they gave you some examples. The question is, are they doing enough? That is a question for Ofcom as the regulator to assess. They are doing some but the law now makes that a requirement. Are they meeting the requirements of the law? I do not know. That is for Ofcom to assess, and I know it is looking into that.

Q22 **Edward Morello:** I was just wondering whether you are aware of how many times Ofcom has referred an incident for prosecution? How many times has Ofcom either demanded something be taken down directly, or referred it internally within Government as an example of malign influence, or referred something for prosecution, if that is within its powers?

Kanishka Narayan: I am aware that Ofcom engages very consistently on reviewing risk assessments and compliance of the platforms' duties, especially illegal content duties, which is the subject here. I am not aware

of data on prosecutions or referrals that it has made in the light of illegal instances in this context.

Q23 **Edward Morello:** Are you able to find out if there has been?

Kanishka Narayan: Yes, I am happy to write to Ofcom.

Q24 **Edward Morello:** I ask this question because when we had the Electoral Commission in front of both this Committee and the Joint Committee on National Security Strategy, and we asked how many prosecutions there had been—I would have to check the transcript—but relating to foreign interference in terms of funding issues I think it said there had not been a single case within the last five years. What I am touching on here is that if the Electoral Commission has not seen any evidence, and Ofcom has not seen any evidence, either we are completely overblowing this threat, or—as I suspect—we are not doing a very good job of identifying the threat at the moment.

Kanishka Narayan: It is a really important question you raise. On the question of funding, of course that is separate. There is a live case under the foreign interference offence that you will be aware of in the courts, so I will not comment on that. That is outside the online space. In the online space, as I mentioned, I will absolutely write to both platforms and Ofcom to understand where there have been any instances of referrals. The main thing I would say is that my understanding is the threshold set in the law is relatively low. I am not happy with the quality of information that we are engaging with online, so of course I will keep pressure on Ofcom to make sure that it is acting robustly.

Q25 **Sir John Whittingdale:** Minister, can I ask you about a part of your Department for which you clearly are responsible? I should put on record that I was previously a joint Minister for DSIT and DCMS. Previously, as a Minister in DCMS, I had some involvement with what was then called the Countering Disinformation Unit. I understand that has now evolved into the National Security Online Information Team, which sits within DSIT. Could you perhaps tell us a little about the activity of the National Security Online Information Team and the exchanges that it has had with platforms to flag potential disinformation?

Kanishka Narayan: Of course. As you are very well aware, in terms of Government responsibility DSIT is overall responsible for online disinformation policy. In particular, it looks at the impacts on UK domestic audiences, agnostic of actors. The NSOIT team that you refer to is really DSIT's operational response to information threats, with a very specific focus on a threshold of either public safety or national security threats arising from the online environment. In those cases, the operational team in effect flags content where it does not comply with platforms, in terms of services.

Q26 **Sir John Whittingdale:** Could you tell us how many times content has been flagged on platforms in the course of the last year? What proportion have the platforms then removed?

Kanishka Narayan: I am afraid I am going to have to frustrate your question on this because for reasons of not wanting to give answers on capacity and resourcing of the team—not least to avoid letting malicious actors have a sense of how we are acting on this question—we have tended to ensure that we are clarifying to Parliament and engaging as much as possible on the terms of its operation but not the detail of its activity and resourcing.

Chair: It is a little difficult in those circumstances to hold you to account.

Kanishka Narayan: I have answered a very large number of oral questions and written questions on this particular theme and they relate very much to ensuring the scope of the team's operational activity is appropriate. But as you will appreciate, in this context—as in other contexts of looking at operational national security responses—we tend not to go into the detail of the resourcing question.

Q27 **Sir John Whittingdale:** Perhaps what you could tell us is, obviously the content that you flag to platforms is such that DSIT believes it to be harmful and disinformation; are you satisfied with the response that you get from the platforms? Have you found that generally they are willing to engage with you and remove if they share or accept your view?

Kanishka Narayan: First, on the very tight scope of that operational activity, which is threats to public safety and national security, the team has been engaging with platforms and has generally found a satisfactory level of engagement. But I have to stress that this is a very tight scope, and so it does not speak to the broader context of disinformation and misinformation, which I am extremely concerned about. Secondly, what I would personally like us to do more across Government is to engage and find ways of deeper information sharing on disinformation outside just that very targeted, limited scope to be able to take more concerted action, both through the platforms and through Government on this question.

Q28 **Sir John Whittingdale:** But it would help public confidence if we knew a little more about the material that falls within the limited scope you describe because that is likely to be the most damaging and where there is clear public safety risk, for instance. When I was involved in the Department with this unit's predecessor, we were very focused on covid and some misinformation being spread about the causes of covid, which was leading to public attacks on, for instance, mobile phone masts. That is a very specific example where there was real harm resulting from disinformation. Would you be able to produce some kind of report to Parliament setting out the kinds of areas where the unit is flagging to platforms and reassuring Parliament and the public that the platforms are taking adequate action in response?

Kanishka Narayan: On this broader question of raising public awareness of the sorts of threats that we are seeing across Government, I am very interested in what we can do across Government. I have to confess,

especially when foreign states are involved, it is an FCDO lead, so I do not want to speak on their behalf. One thing I am very interested in is how we can raise greater public awareness on the sorts of narratives and threats that are being conducted in online disinformation campaigns. Of course, as you will likely know very well, the FCDO and the Cabinet Office are working on a campaign internationally to make sure that they are shoring up trust and sources of information about the United Kingdom. I am keen on making sure we do more and more of that as well.

Q29 **Sir John Whittingdale:** Obviously, the Committee would not wish you to provide information that is of use to hostile actors. On the other hand, we would wish you to provide information both to illustrate the kind of threat we face and reassure people that the Government are doing something about it. Perhaps you would consider a report to Parliament, or some kind of greater transparency than we have been able to discover at present.

Kanishka Narayan: I am very happy to come back and write, and certainly on a regular occasion brief the Committee on the activities of the team, to the extent we can without compromising on the objectives.

Talitha Rowland: Perhaps an illustrative example that we have spoken about to Parliament before is Southport and the public disorder. Obviously, there was a lot of illegal content circulating. That is not what the NSOIT team is looking at. That is obviously a matter for the Home Office and law enforcement. But there was an awful lot of content, including disinformation that was legal but clearly extremely harmful. What the team did there was monitor trends and narratives. It saw the ones that were gaining proliferation and had an exchange with platforms on an early warning system and specifically flagging bits of content that breached their own terms of service; that is the threshold where platforms set their own terms of service. Clearly, for some companies, that is more expansive than for others. Some services have obviously changed their terms of service over the last couple of years.

What we are doing there is an ongoing dialogue, both saying, "Actually, this narrative is growing traction. It might not be on your platform yet but we're giving you a bit of a heads up because actually, you don't want to see this circulating either," and where we identify those things, referring them and saying, "Actually, we don't think you allow this content on your platforms. Please, would you review it?" That is the ongoing dialogue we have.

That is the sort of engagement we have in an incident, but we also have ongoing engagement because these risks do not just come out of nowhere. They are continually present on an ongoing basis. We look at those trends and narratives that might be getting traction in the information environment that might present a risk factor. It is an ongoing piece that particularly steps up at moments of vulnerability, whether that is covid, Southport or an election.

Q30 **Chair:** After Southport, were there particular narratives that were being

promoted from abroad that you spoke to the platforms about? Would that not be something that you could share with the public so the public are aware of foreign overseas interference?

Talitha Rowland: We did not have any specific indicators of foreign interference in the moment. I know there have been some external reports speculating on that. But yes, that is the kind of thing that we definitely support greater transparency about. Independent research is such an important part of this ecosystem.

Q31 **Chair:** Is it not something that your unit did anything about at the time?

Talitha Rowland: We were focused on the immediate operational engagement with platforms to reduce the threat to the public. That was our focus. As the Minister says, we are interested in what transparency can do in terms of building resilience.

Q32 **Edward Morello:** To revisit the Chair's earlier point about the complexity of the Government ecosystem here, you have talked about the National Security Online Information Team with particular reference to the Defending Democracy Taskforce. Minister, can you just talk us through exactly what DSIT's responsibilities are perhaps for any online viewers starting with your understanding of what the Defending Democracy Taskforce is and does, and then where DSIT sits within it?

Kanishka Narayan: I might start with where DSIT sits so that I can then talk about how we are aggregating the Defending Democracy Taskforce. DSIT's role is focused on disinformation policy very specifically and looking at the impact of that on UK domestic audiences, agnostic to who the actors are in the conduct of any disinformation campaigns. The Home Office's role is to look at state threats policy as a whole and in particular to own the specific criminal offence around foreign interference as an offence. The FCDO's role is to lead on foreign interference and in particular to look at the upstream aspect of other states' involvement in it, especially the impacts felt abroad by UK citizens. MHCLG, you will be very aware, will lead on elections policy, so in times of elections in particular.

The underlying sentiment here is right, which is that the online space is effectively vast. There is a range of different risks from disinformation, which cut across Government departmental design. The Defending Democracy Taskforce was born out of this realisation that we need to do radically better on co-ordinating information, operational engagement, and then policymaking across Government on this question. As I said at the very outset, this is one of the central questions, not just for an individual Department but right across Government. Often the links between offline and online behaviour are very material to the nature of the risk and the action that we should take against it.

The Defending Democracy Taskforce brings us all together, including the police and the agencies, to be able to share information from our respective perspectives and share a sense of what we are seeing in our

operational engagement. Then in particular moments, such as elections, we can stand up institutional vehicles—such as an election cell through the JESP vehicle—to be able to make sure the Defending Democracy Taskforce has a co-ordinated sense of what is happening and is able to oversee in ministerial decision-making how we can continue to act against it.

Q33 **Edward Morello:** You just mentioned JESP, which for anyone online is the Joint Election Security and Preparedness Unit. Does DSIT own that, or is that cross-departmental as well?

Kanishka Narayan: It is cross-departmental. If I remember correctly, is it MHCLG or Home Office?

Talitha Rowland: The joint refers to MHCLG and Cabinet Office. They basically co-ordinate a process, and we play a full part in that process.

Q34 **Edward Morello:** Do you want to talk us through what that process is?

Talitha Rowland: There is an elections cell that when we are in an election period brings together the relevant bits of Government, as the Minister said. We will all be doing our own individual reporting in our own areas of responsibility. In DSIT, we will be looking at risks to the domestic information environment; Home Office will be looking at particular state threat links; Foreign Office will be looking at what particular actors might be doing. This brings everything together. It gets one single authoritative source of the truth, and it decides if there is any action that needs to be done. It provides a process for deciding what that action should be.

Q35 **Chair:** Just before we move on, you talked about the election period: what is the election period? In Moldova, we were told that the election period was nine months at least. Build-up to elections takes a long time in trying to change people's minds.

Talitha Rowland: That is exactly why the Defending Democracy Taskforce is important because it is looking at it on an ongoing basis not just around events. Obviously, around events, there is a particular vulnerability, which means you want to stand up probably something more than your ongoing response. That is exactly the point the Minister is making. This is an ongoing threat. We cannot be complacent. We cannot think it just materialises around election periods, for example.

Q36 **Chair:** I was trying to find out about how long this election cell is up and going, or how long the JESP is up and going.

Talitha Rowland: Around the election period as defined in the law, but I would—

Q37 **Chair:** Is that six weeks?

Talitha Rowland: Yes, but that is not the totality of the Government's response to threats to democracy by any means.

Q38 **Chair:** How long does the JESP work for?

Talitha Rowland: It is an ongoing function. It stands up the election cell around election periods, but it works tabletop exercises, for example, running through theoretical examples: "If something were to happen, how would we respond?" It co-ordinates that sort of activity on an ongoing basis.

Kanishka Narayan: The only thing I would add is that in the Defending Democracy Taskforce, we have been talking about election preparedness for the elections ahead, well before the short campaign start as well.

Chair: I should hope so.

Kanishka Narayan: If I recall from memory it has been about four months or so at the very least.

Q39 **Edward Morello:** Can you give us any examples of what a response from JESP might be? What does that look like? What are the levers that you have to pull?

Kanishka Narayan: The range of levers would start with joint monitoring through the election cell, all the individual Government Departments, the agencies and the police. You might have a scenario, for example, hypothetically, where you can do something just through platform engagement and being able to share information, so that platforms are able to act quickly in complying with their duties.

A second type of response might be that you bring something to the Defending Democracy Taskforce. The police and agencies then decide that the information provided from across Government and outside is sufficient to raise the security threshold, and to give particular guidance to the public as well as politicians in terms of their conduct and the level of threat experienced in the country. There are a series of operational responses in the moment through both companies and the security and police forces. There is a separate set of questions, which is also to inform policymaking, so that we are able to ensure that the policy environment is robust to act against these threats.

Talitha Rowland: It is not just about information threats. It is about the whole series of issues to ensure that the elections run successfully, are safe, secure, and the integrity is maintained.

Q40 **Edward Morello:** I certainly understand that. One thing that I am struggling with—surely anyone externally would struggle with—is the nature of the fragmentation: the number of Government Departments involved and independent regulators such as Ofcom and the Electoral Commission. There is also the time period over which stuff is looked at. The Chair has already mentioned Moldova and certainly countries that have experienced high degrees of foreign malign influence and interference in elections talk about the run-up to it starting so long before. Minister, you have also talked about the fact that there is a

crossover between offline crimes and online crimes.

We also have this issue of freedom of speech and the democratic process, and we have seen actors in the UK weaponising Russian talking points to achieve their own political aims. John is just back from Hungary where the entire narrative of the former Government was based on, in effect, Russian talking points. We have seen leaders in the US echoing Russian talking points. A lot of the criticism that came out from this Committee's report on misinformation, from the Rycroft report, has been about the fragmented nature of—

Chair: At the weekend, there was the Mayor of London as well because speaking as a London MP, London has been subjected to the most appalling lies about how safe it is, which have been spread internationally and caused grave undermining of our economy.

Edward Morello: Absolutely. One of the major criticisms from Rycroft's independent review was that there was no one official who could confidently explain to me how the different parts of this jigsaw puzzle come together. I am just wondering, Minister, whether the system that has been built up is fit for purpose, given the range of threats you have identified and the new and emerging threats from AI. Does there need to be a single unifying unit, body, or organisation? Does Ofcom have the powers it needs? Does the Electoral Commission have the funding it requires? Are you satisfied, looking at this smorgasbord of organisations and acronyms, that we have a system that is fit for purpose?

Kanishka Narayan: There is a very large number of questions there. Let me answer directly the one that I feel most strongly about. I do not feel satisfied with the scale of response we have in this country, and have had for some time, on the threat of foreign misinformation and disinformation campaigns and what they are doing to our democracy. That is my starting point. This is one of the most severe threats, and we need to be doing a lot more on it. That is what I have been consistently pushing for, and I have good support from across Government Departments on this question.

Chair: You have good support from us too.

Kanishka Narayan: Which I value very much too. That is the starting diagnosis. On the prescription, my honest sense is that the question of institutional redesign is potentially something to consider but I am much more focused on how we can do both law and enforcement—I will come to each of those in a second—in a much more intense and robust way to tackle this threat.

The reason I say that on institution design is that there are some very unique strengths that each Department and body brings to the taskforce we have: the Home Office is deeply aware through its policing and security apparatus of state-level threats as they operate domestically; the Foreign Office, rightly, is much more aware of both understanding the nature of the threat emanating from abroad and being able to look at it in

the round of our foreign relationships, and make judgments as to disclosure or not in specific instances; DSIT and Ofcom are focused very much on the online environment, and they have built up very unique and distinct strengths in understanding that.

Whether you get better when you push it all together or not is an interesting question that I am very happy to engage with. To me, whether you co-ordinate in a taskforce environment by bringing them together or you set up a very large sum-of-the-parts body, frankly, is not the most salient question. To me, the most salient question is how we can make sure the law is most robust in this? How can we make sure enforcement is robust?

On the law point, in effect, there are three very practical vectors through which we can attack this question without triggering ourselves very materially on deeply held values of free speech and expression. First, to focus on moments of stress and election periods: the British public would rightly expect us to overweight the protection of democracy in those periods, given the values trade-off we have. Secondly, especially when it comes to foreign actors and interference, again, there we have a very clear case for overweighting domestic security and democracy integrity over free expression rights of foreign actors. We can act very robustly there. Thirdly, in empowering users so that they can choose what they want to be a part of.

From next year, as part of the online safety regulatory context, users can opt out of anonymous content altogether on key platforms. I want us to go much further on empowering users, because that starts to avoid this trade-off you might at other times experience between free expression and making sure that we are keeping our country and democracy safe. There is a bunch more to do on law.

You then asked the question of enforcement. Honestly, I still feel that we are very early in the enforcement context of the online safety regime. I will speak about that before coming to the EC. There are clearly instances where I feel frustrated that individual pieces of content that I see stay on platforms, when I feel they are deeply damaging. In some cases, we have taken action to go very far on those. You will have seen that there are non-consensual intimate images. We were able to stand up to a platform and get that content down and have then specified that we are going to put in law a timeline for takedown.

Generally speaking, Parliament had decided over a very extended period of time—I was a spectator in that process—that politics and Parliament should not dictate individual content being taken down. As a result, the focus is instead on systems and processes. On misinformation, that trade-off is even more acute. The idea that Departments can dictate individual pieces of content being taken down would be very challenging from a political point of view.

That is the crux of the enforcement challenge that we have as well. The Electoral Commission is adapting quite a lot to this modern reality of the sorts of threats the candidates experience now; I am sure many on the Committee have. I certainly experience a very high volume of racist content consistently as well, during the election period too. There is more for us to do on how we can support the Electoral Commission to adapt its capability—partly capacity, but actually in large part capability—to this question.

Q41 **Edward Morello:** Some of the most effective examples of countering misinformation and disinformation and foreign influence online that this Committee has seen have been in France, Ukraine, and Sweden: countries that are extremely attuned to the threat, especially from Russia. All three of those have some version of a national counter-disinformation centre that is the focal point within their systems for countering the threat. Is that something that is missing in the UK and that the UK would benefit from?

Kanishka Narayan: I am very happy to take a deeper look at what other countries' experiences have been. As I mentioned at the outset, I feel at the moment that institution design is not really the thing stopping us from going further. It is getting the legal context absolutely right in the light of the changing context of risk, and then getting the enforcement context properly implemented so that we can be very timely with action. But I am very happy to take a look and come back to the Committee with views on it.

Q42 **Chair:** Do you accept that neither the legal context nor the enforcement is sufficient at the moment?

Kanishka Narayan: I would like for us to go further on empowering users when it comes to the context of misinformation and disinformation. That is something thematically that we are very much looking at. Also, not to ditch the law altogether, but the law is new. We are still learning about how it is acting. There is one area—user empowerment—where I certainly want us to go further.

Q43 **Fleur Anderson:** I would like to just pick up on how this would apply in an example, such as the one the Chair shared earlier about London. We have clearly seen disinformation about crime in London and the Mayor of London has called it out. There is evidence that it has come from foreign actors as well. It meets a certain threshold but maybe not the threshold of security that would put it in the scope of the Defending Democracy Taskforce, the Joint Election Security and Preparedness Unit or others.

As you have just said, we are new in enforcing this. We are looking at those thresholds and that disinformation by its very nature is going to be in that grey zone of thresholds and difficult to define. Do you think in the next six months, for example, we will see more of those examples of undermining our democracy through foreign actors being taken on and addressed because of the measures you are putting in place?

Kanishka Narayan: Yes. The short answer to whether we will see more action and to an extent awareness is on the action front. On the awareness front, I would like us to. Again, I have to concede that the Foreign Office is better placed to make the appropriate judgments on which instances of foreign engagement to make public or not. It is a more rounded discussion around security implications in each instance. However, from my point of view, we need to raise the volume on the public conversation we have about these threats, because it is very central to then building informational resilience in our society through media literacy and wider public awareness of the nature, severity and scale of the risk.

There are some specific things we are doing, which will start countering more and more of the challenge that we saw in London in particular. First, alongside the foreign interference offence, many platforms have terms of service that require them to act to counter scale disinformation emanating and affecting UK residents. Alongside that, as the Committee will be aware, we are looking, through a labelling taskforce, at what we can do to start labelling content that is synthetically or AI generated and how it can help each of us distinguish between information that is appropriate and authoritative or not, and in other cases, clearly synthetic and artificial.

Q44 **Fleur Anderson:** What is that labelling taskforce called?

Kanishka Narayan: It is called the labelling taskforce. We are looking at the labelling of pieces of content.

Fleur Anderson: That will help understand when it reaches legal thresholds or not and—

Chair: It is labelling AI.

Kanishka Narayan: Yes, exactly. My expectation is that an interim report on that will be out by the autumn and we want to make sure that we are moving fast on that. We are also looking at a digital replicas consultation to ensure that where fake replicas are made of individuals—that has a very significant impact partly on those individuals but actually much more widely in terms of public information—we are acting on it. We are consulting on that very imminently as well. Alongside that, the point made around the impact on London's perception internationally is a really important one. In that context, the FCDO and Cabinet Office have either launched or are about to launch a significant campaign to tackle those narratives.

Q45 **Uma Kumaran:** It is good to hear you decisively say that we are not quite going far enough at the moment. When we meet colleagues from around the world, they call this hybrid warfare. It is a really severe term but it is what they call it. They make no mistake about what this is. My worry is that in Britain we have that sense of Britishness, where we are being quite polite about it and it is siloed and fragmented. We are saying

that it is cross-department and we want to embed a whole-of-government approach. It sounds really nice on paper and in theory it works but in practice, as you can see from the questions of this Committee, it is quite hard to follow and feels piecemeal. We asked this question of Dan Jarvis, the Security Minister and chair of the Defending Democracy Taskforce: why can we not have a national centre countering disinformation? I believe our allies in Ukraine, Sweden, and France have it. What is Britain's reluctance?

Kanishka Narayan: The first thing to say is that I could not agree more on the scale and intensity of the challenge. We are experiencing, whether from state actors, proxies, and others, a level of attack on our public information environment that is pretty unparalleled. It is increasingly a really important aspect of conflict.

Uma Kumaran: We all seem to agree on it.

Kanishka Narayan: The diagnosis we agree on. On the prescription, as I said in response to Emily's point, I am very happy to look at the design of the single centre that has been mentioned. I genuinely feel that re-organising Whitehall and institution design is rarely the answer to a problem, and as a civil servant I have seen a number of these things. It is fundamentally about investing in AI capabilities so that we have a much better understanding of this, investing in media literacy, investing to ensure that laws can move at pace to cover new threats, and ultimately making sure that the enforcement is robust. Most of these are questions of either resourcing or prioritisation. Institution design can be an important input but I genuinely do not see it as the primary reason why we are not effective. Frankly, it is too early to make that judgment about effectiveness altogether. I am much more focused on making sure that this country and our politics reflect the case that, if we believe genuinely that AI is the primary fault line of global conflict and warfare, this country is investing in sovereign capability at the level of resource we require in terms of capability to stand up tall on it.

Q46 **Uma Kumaran:** Are you confident that we are doing those things at the scale and pace required?

Kanishka Narayan: As the Minister for AI, I am never complacent about the level of investment that we have in AI. We definitely need to do more and I will continue to make the case for it.

Q47 **Uma Kumaran:** To come back on the London point a few of us have raised, disinformation about London in particular is not isolated. We know it is part of a co-ordinated hybrid ecosystem, which is focused on positioning London as a symbol of Western decline. There are people who benefit. They monetise content, which I want to come to later on in our session, but we know it is being driven by extreme right-wing groups in the UK that are also aligned with Russia. It is another long-standing attempt by Russia to interfere through disinformation in British democracy. What do you think the role of politicians in this country is

who are participating in spreading these state-sponsored lies? We say it is not the Government or Department's job to police content, but should politicians not have a responsibility? Should there not be a minimum code throughout our public life?

Kanishka Narayan: Yes, that is a really critical question. From a personal point of view, I would be very interested in having norms and conventions that apply. As I am sure everyone on the Committee has experienced, I have a sense that politicians are increasingly willing to contravene what would have been reasonable corridors of how we communicate publicly and the way in which we stick to facts.

Q48 **Uma Kumaran:** Do you think politicians should be allowed to use AI to manipulate our images and what we say in the Chamber or in our constituencies?

Kanishka Narayan: The fundamental thing that we are looking at, as I mentioned in the consultation, is personality rights born out of this feeling over the manipulation of individuals' rights to their own personality online. It applies more acutely to public figures and politicians but it applies broadly too. It is a definite problem and we want to try to tackle it.

Chair: We are going to return to this in a minute, I have a few other questions from people before we get there.

Q49 **Alan Gemmell:** The Chair has outlined our serious concerns about hostile Iranian activity seeking to undermine Scottish democracy, particularly in the debate on Scottish independence. The Rycroft Review said there was nothing in the public domain that would allow the general public to understand whether the Iranian effects are down to foreign interference or are driven by something else. What more can your Department do to help people understand what has been going on and the scale of the threat that we are seeing in Scotland?

Kanishka Narayan: One thing I have made a case for is that we need a collective agreement across Departments on where we want to make more information available in the public domain on these contexts. I have to repeat the caveat that the Foreign, Commonwealth and Development Office is very much the lead and understands deeper than any of us what the global assessment is of when they want to do that in instances where hostile states might be engaged. From my point of view, we need to raise the volume on instances of the sort you have described.

Q50 **Alan Gemmell:** Looking at the foreign interference offence, since the law has changed do you think platforms are taking this offence seriously? What changes have you seen to their behaviour and activity?

Kanishka Narayan: The online aspect of it has been live since July, so about 10 months. Platforms have conducted risk assessments that look in particular at the threat of foreign interference. One thing Ofcom has realised is that there are some platforms where the risk of foreign

interference is higher still. In those cases, Ofcom is now consulted on a more robust crisis response protocol and is looking at the impact of recommender systems on amplifying these sorts of disinformation campaigns as well—

Q51 **Chair:** Which platforms are the ones that are worse then?

Kanishka Narayan: I do not think that is something Ofcom has publicised, rightly, in the course of a consultation.

Q52 **Chair:** Why should the public not know which platforms are more likely to be subjected to foreign interference in attempts to undermine our democracy?

Talitha Rowland: Ofcom has published risk assessment guidance, which gives guidance to services on the types of features and functionalities that might make services more high risk. It does not call out particular services but it says things such as, "If you have a recommender system." It looks at the make-up of a service and how those correlate to risk.

Q53 **Chair:** It is not likely to be discussed at the Dog and Duck, is it? It is not something that will get into people's consciousness in the same way as picking up X and seeing lots of Iranian bots pretending to be Scottish nationalists.

Talitha Rowland: The risk genuinely looks different on different services. Obviously, the ones that have a particularly high reach will have particular risks attached to them. We should not discount the risk that smaller services, particularly messaging services or things such as that, can do on a lower scale but perhaps with wider impact. There are different risk factors that contribute to it. Ofcom's guidance sets those out and services have to assess against that.

Q54 **Alan Gemmell:** What are the top risk factors that they have set out? What are the risk factors that you are most concerned about?

Kanishka Narayan: We are going to have to come back to you in writing on that.

Talitha Rowland: A recommender system is obviously a big one because it has the impact. I have it here; it is a very long document. We can certainly write with more detail but virality and scale are clearly a big one.

Q55 **Alan Gemmell:** Do you have an idea of the type of spend and resource that platforms are putting into monitoring and assessing this risk?

Kanishka Narayan: We do not have a precise number on foreign interference specifically.

Talitha Rowland: That is one of the purposes of putting it in law. We knew that the major platforms had already done some stuff on this before the foreign interference offence was in law. What it does in law is say that this is not optional and your level of resourcing must be

commensurate with the threat. Ofcom is having its own discussions with platforms. What will happen for the major services in the coming months is transparency reporting. For those larger services, Ofcom will be able to require them to publish transparency reports. Ofcom has not set out exactly what it will require yet but it could include instances of illegal content and how they are dealing with it. Foreign interference might be a candidate, for example, but transparency to the public by showing what they are doing and what it has resulted in will be quite an important part of that.

Q56 **Alan Gemmell:** Do you have a sense of the total Government spending or allocation on monitoring or responding to foreign interference threats? Could you share that with us in writing?

Kanishka Narayan: We do not have a global number but we can certainly come back to you with as much as we can.

Q57 **Alan Gemmell:** That would be helpful. With what you have seen so far, do you have concerns about the operationalisation of the foreign interference offence?

Kanishka Narayan: Offences as a whole are being tested in part in a live case in the courts, as you will be aware, so I am reluctant to comment on it here. The main thing I would say is that I approach it with a genuine degree of curiosity over how recent it is and therefore what the lessons are. I would not pre-empt the judgment on this question but it is a live question and one I am paying close attention to.

Q58 **Alan Gemmell:** On your ideas about further user empowerment, what do you think about ungeotagged content or content where users cannot find out the location of the sender or the originator of a message? What more can we do about that?

Kanishka Narayan: We have to look at that carefully. One of the challenges, particularly when it comes to very sophisticated state actors, is the ability of those actors to be able to move and use legitimate VPN technology to evade most tags on location, which is pretty significant. The two areas I am very interested in are the ability for users to efficiently opt out of anonymous content in a standardised way and for users to have as much control as possible over the algorithms that are driving their particular content feeds.

Q59 **Alan Gemmell:** Do you feel, at the moment, that you are in a position where you need to review the foreign interference offence? This Committee is concerned about its workability in practice, particularly in establishing that the action was instructed by a foreign actor. Do you feel there is a need to review the offence right now and that the thresholds you have described are workable?

Kanishka Narayan: We are seeing a live instance of the offence being operationalised through a court case at the moment, so I will not pre-empt the answer as to whether the offence is sufficient or not. I very

much welcome the Committee's thoughts on it. As I mentioned, the specific threshold evidentially is to have reasonable grounds to infer foreign interference rather than conclusive proof to do so. Whether that is sufficiently low or not is a question we are still getting evidence on.

Q60 **Chair:** We have had a lot of discussion about Ofcom and its role. Ofcom has greatly expanded its job due to the Online Safety Act and foreign interference growing, so are you confident that Ofcom has the necessary funding and resources to effectively regulate this space?

Kanishka Narayan: Ofcom has had a very significant expansion of its budget in light of its new duties over the course of the last year. The Secretary of State and I have met Ofcom consistently to press it on whether that resourcing has been sufficient to carry out its duties. We have heard nothing to suggest there is a resourcing challenge but I am under no illusion that we will have to continue to review it, given the recency of the entire enforcement regime, to make sure that that continues to be the case.

Q61 **Chair:** Is it your view that its funding is adequate because its funding has gone up and it is not complaining about it?

Kanishka Narayan: The funding has gone up materially. I cannot find the exact numbers to hand but the funding has gone up very significantly. At no point have I been told that there is a capacity challenge. On the other hand I appreciate that what we are experiencing in terms of outcomes online may not always satisfy us. As I mentioned at the outset, there are aspects of law in particular and judgments in some cases that Parliament made around focusing on systems rather than individual content that frustrates us all. We have to separate those two sets of questions.

Q62 **Chair:** Ofcom still has not come forward with codes of practice concerning foreign interference risks and it is obviously important for Ofcom to be able to regulate. It needs to have the codes of practice because it gives expectations on how it expects platforms to behave and how platforms are to detect foreign interference or mitigate what is going on. It is still not happening. Is that because Ofcom does not have the resources, or because it is too complicated for it, or because it is only nine months on and it is only reasonable to expect it to have more time?

Kanishka Narayan: Ofcom has recently consulted on further safety measures, in particular for platforms at risk of foreign interference threats. I would expect to see the codes emanating from that consultation as soon as possible.

Q63 **Chair:** When is that?

Kanishka Narayan: I could not give you an exact timeline but as I said—

Chair: Give us a general timeline.

Talitha Rowland: The autumn.

Q64 **Chair:** The autumn? I have started to realise that these seasons can be quite elastic. Can we maybe have it instead by 30 October, which presumably would be the end of the autumn?

Talitha Rowland: It is a decision for Ofcom but we can certainly relay that Ministers are very impatient for the outcome.

Kanishka Narayan: We have communicated to Ofcom on at least one formal public occasion that we want it to go further and faster on enforcement as well.

Talitha Rowland: The thing I would just say on the codes is that it obviously has produced their first iteration of codes. Although it does not specifically have dedicated measures on foreign interference, there are measures that look at how services can deal with illegal content across the board, many of which are highly relevant for foreign interference.

Q65 **Chair:** Many of which are not. I am sorry to cut across you but we are trying to be quite disciplined about looking at foreign interference. I appreciate that work has been done, particularly in relation to children and that sort of dreadful content, and we are not criticising that. We are not talking about that. We are talking about foreign interference in our democracy, and the codes that we are interested in are those.

Talitha Rowland: Yes, and several of the measures are absolutely relevant to foreign interference and services should be taking action on them now. There are more to come. The other thing that Ofcom has indicated is that it does not consider the evidence base is fully there yet in some areas. As that continues to evolve, the codes can iterate. There is no need for further legislation; that is an ongoing iterative process. We are very supportive of Ofcom doing that and doing it in a rapid and agile way.

Q66 **Uma Kumaran:** I mentioned the monetisation on platforms point earlier, and I appreciate you do not have the data on specific outlets but do you think we should be allowing the monetisation of deliberate disinformation and misinformation? If we are saying that it is not for Departments to police it, then should we be okay with its monetisation? Should Britain not more robustly defend our democracy by putting laws in place to stop the monetisation of the spreading of disinformation?

Kanishka Narayan: We should absolutely do everything to stop disinformation and misinformation persisting on these platforms. Some is in law at the moment through the foreign interference line of attack and some is through measures that we want to continue to take and empower users against it. To answer the crux of the question: it is absolutely not acceptable for platforms to not take action in the face of disinformation and misinformation. On top of that, to profit from it is obviously horrific.

Q67 **Uma Kumaran:** The algorithms we have seen push certain types of

content and that is what is then being monetised. The Greater London Authority published its own research showing that London is the target of online narratives portraying the city as unsafe and other things. Lots of these accounts were professionalised bot farms in Vietnam and Sri Lanka, countries that have sympathetic actors to Russia. This is business; this is money now. On a foreign affairs side, we should be asking some Ministers if they are going to be raising it on a diplomatic angle. With these platforms, whether Meta, X, or TikTok, should we not be legislating to stop the monetisation of this particular type of content?

Kanishka Narayan: We have to be very clear that algorithms are already covered where risks emanate from them in terms of foreign interference and illegal content under the Online Safety Act. It is not the case that algorithms and their impact on the overall harm and risk are not covered in the legislation. They absolutely are. Platforms have a responsibility to ensure, where there are algorithms, data, or they are supporting content, that the harm vector is the way in which the legislation works. If they are harmful offences in the law then they cannot be allowed.

On top of that, there are two things that are really important and we want to do more on. First, deeper access to understanding the algorithms from a transparency point of view for researchers and secondly, to ultimately have deeper control for users over the algorithms that drive the news feeds that they see. Those are the two areas in which we are hoping to make even more progress.

Q68 **Uma Kumaran:** The London School of Economics has similarly shown that the model of paid subscriptions played a massive role in fuelling the Southport riots by legitimising and pushing particular accounts that were spreading false statements. We have that research. Is your Department looking at any of that? We have international evidence of this happening in other situations but I am giving you an example of a domestic situation.

Kanishka Narayan: The one instance of an operational response within the Department that is public is the Southport event, where we were very engaged on online narratives, focused on public safety and national security concerns, and engaged very closely with the platforms on it.

Talitha Rowland: I do not know if it is helpful to you as it is not quite the same thing but it is linked to advertising related to harmful content. Online advertising is a matter for DCMS, but we have been working extremely closely in partnership with it to look at whether we can introduce greater transparency into that system. At the moment, lots of advertisers are inadvertently funding some of this content because the transparency chains in the advertising world are quite opaque. We are working with its Online Advertising Taskforce to see if there are steps we can take to address that. It is slightly different but it is linked.

Q69 **Richard Foord:** How often does DSIT meet with major platforms such as

X, YouTube, TikTok, and Meta in relation to foreign disinformation?

Kanishka Narayan: We meet the platforms relatively regularly to talk about online safety as a whole, including very much foreign interference. Some data is public but we are happy to point the Committee to the engagement disclosures that we have made in this context.

Q70 **Chair:** What does relatively regularly mean?

Kanishka Narayan: If you take the Department as a whole, which was the subject of the question, I would be surprised if it was not on a fortnightly or monthly basis at the very least.

Talitha Rowland: My team meets platforms at official levels on these types of issue weekly at the moment around elections but on a really regular frequency.

Q71 **Chair:** The question was about foreign disinformation. How often is the Department meeting the platforms to talk about foreign disinformation?

Talitha Rowland: We cover information threats because that is our brief, some of which will obviously be about foreign interference.

Q72 **Richard Foord:** As a result, what changes have been made? What improvements have been made to protect against foreign interference?

Kanishka Narayan: I would not like to claim any attribution from our meetings for the impact but platforms have had to carry out risk assessments to understand the risks of foreign interference. The team has been working with them in operational contexts and has engaged with instances flagged to them as well. Generally speaking, Ofcom is the primary responsible party to understand the ongoing compliance of the platforms with the very tough illegal content duties they are subject to in the legislation.

Q73 **Richard Foord:** The Foreign Affairs Committee published a report recently on disinformation, and in that report we called for the Government to require social media companies to make their algorithms transparent. What do you make of that?

Kanishka Narayan: I am very interested, as I mentioned previously, in how we can make sure there is research transparency so that we have a greater understanding of data as well as algorithms in the content that we see. I am also interested not just in transparency but user control and agency over the algorithms that drive the content that we see. Thematically, I am very supportive of it.

Q74 **Richard Foord:** What about requiring platforms to produce annual reports on the detection of state actors being engaged in interference, say through amplification? Would you like to see the platforms producing annual reports on detection of state actors?

Kanishka Narayan: The platforms have some transparency reporting at the moment and we still need to do more, at the very least in information

sharing between platforms and across Government on the nature and source of the risks. Whether we should enforce particular standards of platforms reporting and attributing is a more open question. I want to make sure, as with Government disclosures, that while we are raising the volume on this question, which is critical, we are doing so in a responsible way where we are allowing our national security, policing, and security apparatus to react more broadly in a robust way rather than just jumping to disclosures in all instances.

Q75 **Richard Foord:** We talked about the social cohesion strategy earlier, which requires Ofcom to publish summaries of platforms' transparency. Ms Rowland, you suggested this may require platforms to publish data around foreign interference but you used the term "candidate". Foreign interference data was a candidate for publication. When might we know if the data that is going to be published by Ofcom will include foreign interference data?

Talitha Rowland: What you were just asking the Minister about could be within the scope of those transparency notices. I am not sure of Ofcom's precise timings off the top of my head, but the law says it is a matter for Ofcom but obviously the Government can make representations.

Q76 **Richard Foord:** The same question for you, Minister, in relation to the access by independent researchers to the algorithmic data. When might we see Government or Ofcom implement that in compliance with the Online Safety Act?

Kanishka Narayan: It is a really important thing, which I am focused on. I expect we will see a formal consultation on this question soon this year and action as quickly as possible straight after it.

Q77 **Richard Foord:** Do you have dates or a timeframe?

Kanishka Narayan: I cannot give you an exact date for the launch of the consultation.

Q78 **Chair:** Do you have a general date?

Q79 **Richard Foord:** Or a season?

Chair: Or a season?

Kanishka Narayan: I am reluctant to give you seasons that then expand beyond the logical constraints implied. At the earliest opportunity that we have a date, we will come back to the Committee on it.

Q80 **Chair:** I was thinking about you being Minister for AI. One thing we are told is that, when it comes to foreign disinformation and abuse, algorithms are abused by bots that amplify one another's messages. Those bots are likely to be greatly increased by the use of AI. Platforms will be even more vulnerable than they were before to their algorithms being abused by AI creating lots of these bots, which all copy one another. Are you aware of that? Is a particular strategy going to be—or

perhaps it has already been—put together to deal with the abuse of algorithms by bots created by AI and promoting lies about our democracy?

Kanishka Narayan: It is a really significant question. In this domain and more broadly we are seeing, in terms of information risks and online safety, the volume of instances of attack potentially rising. In some cases, the severity is rising because of the ability of malicious actors to automate the malicious activity altogether. There are two things in terms of a response. One virtue of the legislative context that we have is that it is not technology-specific. Whether it is the algorithm, data, or the AI agent that carries out the activity, the legislation says, "Let us look at the harm and tackle it regardless of which part of the technology stack the risk emanates from." In that context, there has been some assurance.

The second aspect is not related but is applicable here too. There is a sense that the legislation at the moment does not cover some AI chat bots that might be implicated in attacks, including attacks where people are, for example, engaging to understand where they can carry out illegal foreign interference activities. We are now legislating to close the loophole and make sure that we have the powers to act robustly so that the scope of AI tools is very much in rather than out of the legislation we have at the moment.

The final thing I will say is that the law is a very important vehicle, but the central question for us is how quickly we can build up our domestic capability to understand and then counter the risks that AI in particular offers here. One thing I am proud of is that the AI Security Institute in Government is the only lab globally that has pre-deployment access to core models to be able to understand the risks that AI agents might pose in a range of situations. What we need much more of, both in Government and across, is even deeper resourcing of our capabilities to understand and then act against AI emanating threats on foreign interference.

Q81 **Sir John Whittingdale:** Minister, you have referred several times to the Government's examination of the introduction of personality rights. I very much welcomed the section in the AI and copyright document recently published, but while the document sets out in some detail the deficiencies in the existing law and raises the possibility of exploring that option, it seems to suggest that there is not a great degree of urgency or there is an implication that it is going to take some considerable time to even decide whether such a right is necessary. Would you accept that what we have been discussing this morning illustrates why it is really important that we get some protection against digital replicas as part of disinformation on the statute book as quickly as possible? Can you give us some indication of the timeline attached to that?

Kanishka Narayan: First, I would very much echo the Committee's view on the importance of this question. I have seen that there are some legitimate uses of digital replicas but clearly, in our politics and more

widely in terms of commercial exploitation, we have seen a number of instances where personality rights have been contravened and digital replicas have been deeply harmful. That is very much the motivation for the action we want to take.

We set out a big response on AI timing and copyright more broadly relatively recently and, as part of that, said we will be consulting on digital replica in terms of regulation and policy action very soon. My view is to try to do it at the earliest opportunity. The one seasonal concession I will give on this question is that I hope we will do it in the summer.

Chair: The summer finishes at the end of August.

Q82 **Sir John Whittingdale:** That is a step forward, but I am not entirely clear what is going to happen by the summer. Are you going to produce the result of the response to the consultation document, or simply launch the consultation, or—

Kanishka Narayan: You will be more aware than me given all your experience. We will be consulting on a range of ways in which we can best protect individuals' rights without contravening appropriate free expression values when also tackling digital replicas. We will do that as a precursor to then being able to take action on the appropriate path.

Q83 **Sir John Whittingdale:** Would your ambition be to include this within a future AI-built one? When is that likely?

Kanishka Narayan: I will get in particular trouble with the whips if I commit to a legislative vehicle for a hypothetical regulatory action.

Q84 **Fleur Anderson:** Is it possible to do this on our own as the UK, or is it an international problem with a blurring of lines especially when we are talking about foreign information? We have gone to many countries in our inquiries and we have seen this happen in so many places and in similar ways, yet every individual country seems to be trying to tackle it. Is it possible for us to tackle it? Does there need to be more international cohesion to take on the platforms, create alternative and trusted sources, and to make a real difference?

Kanishka Narayan: I feel very led as a witness on this question. I could not agree more. One thing that has been really valuable about this process for me is getting a slightly deeper understanding of what other countries are doing and the risks they are experiencing. I am conscious that my foreign office colleague, Minister Doughty, has engaged very deeply on the experience of Moldova in particular, which we can learn lots from. The overarching answer to your question must be yes.

Q85 **Fleur Anderson:** The follow-on from that is: is there enough join-up in Government to be able to do it? Is there enough ability for the foreign disinformation knowledge that comes in from the FCDO to join up with your information? We have already mentioned the Cabinet Office, the Department for Education, and DSIT. Which Department will say, "We

now need to take this internationally and try to tackle this in a different sphere?"

Kanishka Narayan: Operationally, the Foreign Office. My colleague, Minister Doughty, has been very engaged with international engagement on the operational details on policy around disinformation—particularly around elections—that is owned by DSIT. I have engaged with a series of our allies across Europe, Australia, Canada, and beyond on policy responses to it. Ofcom does a series of international engagements with other regulators as well. I am hearing, and feel to be true, that we probably need to make sure that the Defending Democracy Taskforce is focusing explicitly on the international co-ordination point even further and I will take that away.

Q86 **Fleur Anderson:** We have heard that this is a hybrid war. It is a threat. In no other sphere of defence do we sit alone and not work with allies in step. We create organisations of allies to work together. That is part of the recommendations in our report.

We have seen how media literacy has been built in to other countries. We saw lifelong and system-wide national policy in Finland, where very young children learn this through play all the way up the different ages. The Government published A Safe and Informed Digital Nation media literacy plan in March, which was good to see. It does not explicitly talk about disinformation and foreign information but talks about being alive to misleading content. What do you see as the ways in which you can tackle disinformation, making our population in Britain much more aware about it and able to counter it?

Q87 **Chair:** The other question is: who is taking responsibility for it? We have been confused when asking this question as to who takes responsibility. The Department for Education seems to take upon itself a bit, the Electoral Commission has a responsibility for it, and presumably you guys have. It is very hard for us, coming in from foreign affairs and seeing the importance of ensuring that there is increased media literacy, and trying to understand what the British state is actually doing. That is our frustration here.

Kanishka Narayan: On the responsibility question, I have been very firm in my job by making sure we have a robust media literacy action plan focused on online harms and feel a pretty strong sense of responsibility on that question. Of course, I engage very closely with the Department for Education as schools are a really important vehicle as to how we can engage young people in what we want to do on media literacy. That feels appropriate.

In terms of a specific focus on foreign interference, one way in which DSIT thinks about this is that we are not at all specific to the type of actor conducting things that are risky and lead to online harms. Whether it is a foreign interference instance or a domestic misinformation and disinformation campaign, what we are primarily focused on in the media literacy context is to say, "How can we build the deepest sense of

resilience across this country in separating fact from fiction and in understanding the sorts of risks that online misinformation and disinformation pose?"

One thing I am taking away from this conversation as a whole is this feeling I have that we need to raise the volume separately to that, separately to how we help people build that cognitive resilience in separating fact from fiction online. We also need to think about what we are doing in raising the volume on the particular risks associated with foreign interference from a wider policy context. The reason why the media literacy action plan does not focus on a specific source of risk is that we are focused on building the deepest mitigation that we think applies across risks rather than specifically.

Q88 **Fleur Anderson:** The Committee has found in its report that a culture of secrecy and over-classification surrounding state-linked disinformation campaigns can run counter to that turning up the volume. There are examples of where it is happening and where it is called out. In other countries we have seen that they have specifically said, "We have traced this example of a social media post back and this is where it comes from," which has been very powerful in turning up the volume that you talk about. Do you agree with this Committee that there is a culture of secrecy and disinformation? Would you support our recommendation that, where examples resonate with the public, the Government and the national security community should declassify some information relating to foreign information, manipulation, and interference?

Kanishka Narayan: On the diagnosis of this, the Foreign Office, the agencies, and the security context make a judgment on a case-by-case basis. I genuinely do not feel sufficiently informed on each of those judgments to say whether there is a broader culture where they are making those judgments consistently on the wrong side. I will not comment on the diagnosis—

Q89 **Chair:** I think you should. We have and we would like your help. We think that the agencies could find more Iranian bots. They could find more examples, which is a really good way of educating the public. We feel that there is understandably a culture of secrecy, but politicians need to push the agencies and say, "Give us more examples because the public need to understand that our democracy is under threat."

Kanishka Narayan: On prescription, I feel a very strong urge that we need to turn up the volume on this and I will continue to push for that wherever it is feasible and appropriate.

Q90 **Fleur Anderson:** The volume needs to be turned up because foreign state actors are manipulating democracies in other places, and we can see that happening here. They are undermining our way of life in ways that are very subtle and sometimes not very overt. So making them overt is very important but it means a change of culture.

Another question about the media literacy plan: why are there no overt

actions for social media platforms? There are 27 actions at best. I love to see an action-oriented report—we all do—but there are no overt actions for the social media platforms and what they are going to do. We can play our part. They need to play their part in media literacy and that link to political literacy as well. They could be contributing more financially towards the media literacy work that we do in our country, which was also recommended by the House of Lords Communications and Digital Committee.

Kanishka Narayan: Platforms absolutely have to do as much as needed to engage on media literacy. I will say three things on this. First, the legal context in the Online Safety Act means that not only do they have to assess prospective risks but they have to consider mitigations—including media literacy interventions—that can mitigate those risks. There is a legal duty on platforms to specifically make sure that they are doing that.

Secondly, Ofcom has had a three-year media literacy strategy as part of the Act. It has been working very closely with platforms on it, and my understanding is that the best practice principles on media literacy as a function of design in products, rather than ad hoc interventions, is something that a series of the platforms have committed to. I expect them all to comply with it and invest in it accordingly, having committed to those principles of design.

Thirdly, Ofcom is consulting on where platforms can go further. My view is very clear on this; platforms have to play a significant role. They have to put money behind it to make sure they are complying, not just with their legal duty and the principles that they have signed up to so far but with the change in context and what that implies for the level of resourcing of media literacy.

Q91 **Fleur Anderson:** We highlighted in our report that Ofcom has a specific duty, but in a letter Ofcom wrote to the Joint Committee on the National Security Strategy it said that it was not its role and it did not have a specific duty on media literacy. There is some confusion by Ofcom. As a result it could be said, and maybe it is because of social media platforms lobbying on this, that you have gone a bit soft on the social media platforms in the media literacy plan. There should be more work by them, and Ofcom should be enforcing it, but it does not feel that is its role so something may be missing.

Kanishka Narayan: I am always keen on asking the platforms to do much more right across the waterfront but in particular on this question, which is central. I am surprised to hear that Ofcom feels it is not responsible for media literacy. It has a strategy on media literacy. I have pushed them many times on media literacy, so I will be very keen on clarifying that the next time I see Ofcom.

Chair: Another impact of giving us more examples, such as the Iranian bots, is that it holds these social media platforms to account because it embarrasses them when there are obvious examples and they have not

done anything about it. I am afraid it embarrasses the Government when we show the examples and are not sure that the Government are doing anything about it, but the media platforms ought to be doing it too. That is why one of our recommendations is that we have more examples and the public are properly informed.

Does anybody have any other questions? No. Thank you ever so much for coming. We are very grateful to you for giving us your time. We will write to you and remind you of all the promises you have made of all the information you are going to give us and we look forward to it. It has been a very interesting session. Thank you.