HOUSE OF COMMONS

Foreign Affairs Committee

Oral evidence: Disinformation Diplomacy, HC 703

Tuesday 13 January 2026

Ordered by the House of Commons to be published on 13 January 2026.

Watch the meeting

Members present: Emily Thornberry (Chair); Fleur Anderson; Aphra Brandreth; Phil Brickell; Dan Carden; Richard Foord; Uma Kumaran; Abtisam Mohamed; Edward Morello; Sir John Whittingdale.

Science, Innovation and Technology Committee member present: Emily Darlington.

Questions 248-339

Witnesses

I: Ana Revenco, Director, Moldovan Centre for Strategic Communication and Countering Disinformation.

II: Ciaran Martin CB, Founding Chief Executive at National Cyber Security Centre.

III: Vijay Rangarajan CMG, Chief Executive at Electoral Commission.

HOUSE OF COMMONS

Examination of Witness

Witness: Ana Revenco.

Q248 **Chair:** Last week, the Foreign Affairs Committee heard from FCDO Minister Stephen Doughty, who was here to talk about disinformation. Today, we are going to hear about some examples of disinformation campaigns and the implications for the UK and particularly for the upcoming elections in May. We are really grateful to Ana Revenco, whom some of us met when we did our trip to Moldova. She is from the Moldovan Centre for Strategic Communication and Countering Disinformation, and we are really pleased that she has been able to join us today. Thank you very much, Ana, for meeting with us.

May I begin with a general question? Moldova has been the target of sustained Russian hybrid warfare. Russia has conducted cyber-attacks, illicit financing schemes, fake bomb threats and disinformation campaigns at a really high level, all trying to undermine democratic institutions and processes. The UK has also been suffering cyber-attacks, disinformation campaigns and sabotage from foreign actors. The question I want to ask you is really about your experience. Would you mind giving us a little more detail of the sort of things that Moldova was subjected to? How did Moldova defend itself, and what lessons should the UK learn from your approach?

Ana Revenco: Thank you very much for this opportunity; I am glad to be able to share our experience. As you said, it has been obvious for us, especially in the last four years, when Russia began to act much more openly, in open information warfare—to say the least—in order to regain control over the region and to blackmail both Brussels and Kyiv, and definitely to block democratic development, which also means blocking accession to the EU agenda.

The arsenal of tools that Russia has employed include quite a complex set of tactics. It has used illicit financing, including of political parties and campaigns, and the public endorsement of so-called political initiatives that were nothing more than the proxies of Russian political forces. It has used very intense cyber-attacks—constant, continuous attacks, both in and between election periods. It has used economic blackmail, particularly energy blackmail, for winters in a row. Again, it is about not only the usual one to three months of the active election period but what is happening in between elections.

Here is the first lesson learned: protecting democracies and protecting the democratic integrity of elections means being aware and better co-ordinated, and acting in between the election cycles. There have also been very strong disinformation and information-manipulation campaigns. Russia has been employing at least those five tools of its arsenal in order to dethrone the democratic nature of the elections.

Speaking particularly with regard to the disinformation, information-manipulation and information-interference campaigns, especially when it

came to the parliamentary elections, all the documented tactics have proven that Russia has built a very robust information-war ecosystem. I would dare to say it is at an industrial and professional scale, with all the tactics you can imagine being used, including deepfakes and cheapfakes, AI-generated content, AI-promoted content, networks of thousands of inauthentic accounts constantly engaged in promoting lies and fakes, and all these cheapfakes. We have also been seeing various cyber-generated or facilitated disinformation, like fake official memorandums, letters or Government protocols being circulated, and sites impersonating the websites of state institutions and of the leadership.

Especially in the last electoral campaign, we saw that new tactics have been added as compared with 2024, such as pseudo-opinion polls that have been organised online, which were nothing more than an attempt to inculcate hostile narratives among the consumers, or information laundering through pseudo-media—media houses created online, including in the European space. These are just a few examples. An enormous amount of money is invested into the continuous running of this disinformation campaign—

Q249 **Chair:** Before you move on to the money, do you mind if I go into some of the things you have said in a little more detail? When it comes to disinformation, it is not just that you will get a fake account that pretends to be a person that isn't a person, and that is promoted in an authentic way—it will not just put out a lie but claim that it has a source, and that source itself is dishonest. How are those dishonest sources produced?

Ana Revenco: It is what we call information laundering. It is an attempt to plant apparently fact-based information or messages, including in mainstream media and European mainstream media, but when we take a closer look at the articles or columns, we see that the data has been misinterpreted and taken out of context, with a lack of secondary or opposite opinion, and strongly backed up by many other semi-facts in order to support specific positions.

Others immediately pick up the inauthentic account in order to amplify the message and to create the fake impression that it is true, because one can see the message everywhere. That puts it in the mouths of so-called political leaders, but unfortunately they are nothing more than political initiatives or clones: the same people keep registering various parties overnight, pretending to be political leaders in order to give the impression of a true statement. That was one of the favourite tools or tactics used in the complex FIMI campaigns that engaged all platforms, all social networks, and had the highest penetration in the consumption market in the Republic of Moldova.

We saw instant planting of those messages in numerous groups, in numerous pseudo-media online, self-supporting each other to multiply the message across platforms such as TikTok or Facebook, immediately creating and amplifying artificially the message, as I said, to create the impression on people that something is happening over there to which they have to pay attention. Of course, fear was one of the emotions most

often used to reach people. It aimed to trigger an emotional reaction to the messages, blocking critical thinking.

Q250 **Chair:** May I give you an example from London? Would you identify this as a similar thing? Mark Hill of King's College London did an analysis of Reddit accounts. On those accounts, he saw that London was being described as "dangerous" and "lawless". Those words have been used about London, going up from 874 in 2008 to 258,444 by 2024. On the face of it, that seems to be a kind of organised campaign to use those words about London. Do you recognise that as the sort of thing that you were subjected to?

Ana Revenco: It sounds to be, yes. I do not know the entire context, so I cannot give a more precise opinion, but based on the few things that you just told me, yes. Such cases have the highest potential to drag people into a public discourse that is defocused from the truth. It is not really a fact-based, but a more manipulated public debate.

I will give you a few other examples. For example, in Moldova, one of the priorities of the defence and security sector is to modernise the army. Every time an amendment to the law, or a new strategy, programme or budget is being discussed in Parliament, or a new agreement with a new strategic partner is being discussed between two Ministries, automatically the Russian disinformation campaigns suggest that that is because Moldova is preparing for war, that NATO troops are already on the ground or at the border of Moldova, and that immediately after the pro-Europeans make a gain, the NATO troops will be allowed into Moldova to back up Ukraine, and so on.

You see how a fact-based Government development agenda is being manipulated in order to scare people—that this is only because war is here. The same is happening, for example, with other topics related to migration or demography. They are consciously misinterpreting the data, skipping the data that relates to past decades about immigration or demography rates in order to just focus on here and now, and to try to portray that this is a problem that has appeared only because Moldova has decided to take the European path and to stay connected to people.

Q251 **Chair:** I am so sorry to cut across you, but there are two questions that come from this. First, how do you deal with inauthentic accounts, or accounts that are being inauthentically promoted within an algorithm or a social media platform? Secondly, how do you counter the disinformation? I wonder if it is possible to answer those relatively shortly, and then I will go on to Edward.

Ana Revenco: You will not find a black and white answer, but what we have managed to develop is, first, we have constant actions on documenting the behaviour. We are not looking into the content because, for us, freedom of speech is very important; pluralism of opinion is important. As long as it is an honest and truthful statement, it must be given the right to exist in public debate. But if it is manipulated—talking about the inauthentic accounts and behaviour—our analysts are

documenting this behaviour. Once it is documented, the next step is to raise awareness among the population in order to increase their capacity to navigate in the online space among the news with better knowledge, understanding how to check the source and how to grasp that information.

Q252 **Chair:** How do you do that?

Ana Revenco: Basically, we make public reports of these documented actions. Whatever we can make public, we make public, and we present the reports to the National Security Council. For example, even in the last year, this exposure of inauthentic behaviour and its key elements and tactics were presented in public by Madam President. The technical exposure and awareness of people and society is done, including at the highest level, but this is also shared with the members of the National Security Council, who are notorious leaders, which means that this awareness is being synchronised among all the key messengers. This is part of the StratCom effort as well, but it is only one thing.

Secondly, we created strong partnerships with civil society organisations, dedicated think-tanks, investigative journalists and fact-checkers, and we also regularly have information sharing with them in order to ensure that this information and awareness effort and message is supported by representatives of civil society in order to increase attention and the outreach, and to ensure that this topic is constantly kept on the public agenda so that people are constantly aware of the importance of staying attentive in the information space. We also share the main findings with the platforms in order to increase their responsibility, but I must say that the most challenging exercise is probably getting a more responsible response from the social platforms.

Q253 **Chair:** Did you get any responsible response from the platforms or not?

Ana Revenco: There is a response, but it is far from sufficient. It is more reactive, which means that the harm is already done. When we identify those accounts engaged in a campaign, it means that the harm is already done. Those accounts have already multiplied and promoted deepfakes, cheapfakes, lies and disinformation that have already reached people. Blocking them, taking them down or blocking access in a post-facto manner is generally according to the platforms' rules, but the impact is almost zero.

Chair: The most famous example of that is from your neighbour in Romania with the presidential elections and TikTok, where TikTok eventually did something about it, but only after the presidential election was called off.

I will move on to Ed, as the Committee has a limited amount of time and lots of questions for you.

Q254 **Edward Morello:** When the Committee was in Moldova and Romania, we heard quite a lot of evidence about concerted efforts to undermine confidence in Government institutions, not just during the election, but in the run-up and years beforehand. A lot of that was focused on the

electoral commission and electoral process. Could you talk a little about Moldova's experience of that? I also remember cases where public figures and politicians were echoing some of that narrative in an effort to discredit the electoral process or the electoral commission.

Ana Revenco: You are absolutely right in noticing that. As I mentioned at the beginning, the most important period where both Russia—call it the adversary; the hostile actor; the malign actor—and the democratic parties can act is in between the election periods. That is exactly when actions gain more traction and have the potential to influence people's beliefs. We have mapped Russia's strategy and tactics and worked in an anticipatory manner. We have designed that vulnerable scenario, and based on that we have started to develop strategic communication recommendations and partnerships. Based on that mapped strategy, it was clear that Russian influence or FIMI objectives were targeted at dividing the population, especially pro-democrats and pro-Europeans, to weaken that group both among resident and non-resident Moldovans.

Secondly, exactly as you mentioned, all the actions were put in motion to portray the state institutions as incapable of bringing safety, security and democratic processes. It is the electoral commission—but not only it—that is part of those targeted campaigns. Law enforcement institutions, border institutions, anti-corruption institutions, tax authorities and the Audiovisual Council are constantly part of disinformation campaigns, and orchestrated hybrid-type attacks that drain the capacity of those institutions and test their ability to react. Those include paid protests or orchestrated cyber-attacks on the digital infrastructure of the electoral commission, or tons of fake complaints coming as rain to the Audiovisual Council in an attempt to engage them in fruitless investigations regarding the alleged illegal or harmful activity of some media houses or publishers. As I said, these actions were specifically designed, organised, financed and scheduled to exhaust the state institutions—in order to determine that the state institutions fail or make mistakes, or to constantly raise the anxiety in the population on the capacity of state institutions to secure the democratic nature of processes.

This happened even before the referendum in 2024. It was a constant campaign of using hybrid tools in order to drain people's trust in democracy, in state institutions, in the European path and in strategic partners. It has gone much beyond the usual terms of election campaigns; it has probably been our reality for the last four years, and it is a constant one. It peaks during elections, but even now, as we speak, we register periodical very aggressive disinformation campaigns around various sensitive topics related to Ukraine, to security in the region, to peace negotiations, to energy security and to much more.

Q255 **Edward Morello:** We also heard from colleagues of yours in Moldova about quite sophisticated vote-buying efforts and the use of illicit finance, especially funnelling through cryptocurrency. Could you give us some more details of how that played out in Moldova?

Chair: Can we also ask a wider question on the use of crypto in trying to

influence the elections in Moldova? Were you able to contain it?

Ana Revenco: As I mentioned at the beginning, the illicit financing of political campaigns, electoral campaigns and political parties was one of the key instruments in this arsenal. They have been trying to infuse illicit funds through various means. Every time state institutions responded, because it was not only related to the last electoral campaign; it was not only one of the tactics used by Russia to influence the parliamentary elections. We documented the first attempts back in 2022.

It was the attempt to bring in cash via plane—engaging elderly people almost like mules, or priests, or the younger generation, organising charter flights to introduce this illegal money into the country. Every time the state institutions, when documenting these cases, have immediately responded by improving the national legislation requiring more transparency, for example, on bank transactions, to make it more transparent for those who want to bring in money by other means.

That also made Russia's proxies determined to be more creative. What we saw for example in 2024 during the elections was that they tried to introduce money through pre-loaded or prepaid bank cards. These documented cases allowed us to immediately prepare for the parliamentary elections, so changes have been made to laws. I can tell you that was not an easy exercise. It took a lot of effort to explain to people and to partners, and to the Venice Commission and many others, why these measures are important.

That actually brought results, and certain attempts have been stopped, but we have also seen how these responses made them become more creative, which brings me to the second part of the question, about crypto. Part of crypto is that it takes international efforts. No country, including Moldova, can deal with this alone. It is important to conduct financial investigations when it comes to foreign information interference, manipulation campaigns or attempts to manipulate elections.

In this case, it was done only due to international co-operation, including a lot of training and expertise that we received. I can tell you that expertise was also received from UK experts on better understanding how to organise this response. Expert support was provided to our state institutions, including the Office for Prevention and Combating of Money Laundering and the National Anticorruption Centre. That exchange of information and awareness between the institutions of various countries, including international banks and financial systems, allowed us to prevent at least certain transactions and diminish the impact.

One of our conclusions was that the available international legal norms and standards on protecting this type of process are already insufficient. Lots of investments have been made in the past on fighting the illegal financing of trans-border crime, or other types of criminality of organised groups. However, at the same time, they have still not been enough when it comes to the illicit financing of political campaigns and electoral campaigns, which is something that we all need to work together on, and

we plan to put it on the agenda in our multilateral dialogue with our European partners.

Q256 **Chair:** Can I ask you a question about a debate that is going on in the UK at the moment? From your experience, do you think there is any advantage to the United Kingdom in allowing cryptocurrency to be used in our democratic system?

Ana Revenco: It is almost like asking whether technology is good or bad, or whether AI is good or bad. Any development is associated with modernisation, and modernisation without technological progress is impossible. We just need to be aware of the other side of that progress, and we cannot diminish or underestimate the possible harmful effects that it can produce. It is not only democratic actors who are using these technologies and modern models of life for good—we also have hostile actors.

Unfortunately, the way in which Russia has interfered in our democratic processes is only proving that there is another side of this technological process, including crypto transactions, which means that we have to put on the agenda—not only for the public but for legislators—a deep examination of the possible harms and take actions now, before we plan or enter any election processes.

For example, one of the conclusions is that the Central Electoral Commission has already decided that it will extend its structures. It is seeking to create a special team that would be specially trained and equipped with all the relevant methodologies and tools to enable much more complex financial monitoring of the financing of political parties and electoral campaigns, including from the financial, online and crypto perspectives. That is also a conclusion that we came to as a result of the last democratic exercise.

Chair: Unless anyone has any further questions, thank you very much for spending some time with us, and for sharing your knowledge and wisdom. I am sure that we will see you again soon. All the best.

Ana Revenco: Thank you very much. All the best.

Examination of Witness

Witness: Ciaran Martin CB.

Q257 **Chair:** We move seamlessly on to our second witness. I thank Ciaran Martin for joining us in person. Would you mind introducing yourself for the record?

Ciaran Martin: Thank you, Chair. My name is Ciaran Martin. I am a professor at the Blavatnik School of Government, University of Oxford. I was the first chief executive of the National Cyber Security Centre at GCHQ.

Q258 **Chair:** Excellent. Thank you very much for coming and for sharing your time with us. I am sure that you appreciate what we have been doing. We have been looking at what has been happening internationally, and we are quite concerned. We would like to get some reassurance, if possible, that we are, as a country, prepared for any potential onslaught that we might be subjected to. Obviously, Moldova is one of the strongest and most recent examples of a country that has been subjected to attempted disinformation and manipulation from abroad. I will ask you a general question to begin with. What is your assessment of the UK's resilience to hybrid threats? How have they changed over the years? Is there anything that gives you particular cause for concern?

Ciaran Martin: While the past is only a limited guide to the future, we have been worried about foreign interference in our politics and democracy for some time. I would date it primarily from 2016, when the obvious interference in the US presidential election—the hack and leak campaigns—obtained such prominence and exacerbated divisions within an already divided US. It brought to the attention of most western Governments the risk of that type of activity, so that is when I would date the concern from. We are getting to the 10th anniversary of that. Looking at the past, the UK and other western democracies have actually fared better than many of the expectations at that time. We have had multiple, very contentious electoral events in that period. We had the elections of 2019 and 2024. We had losers' consent in both; we have not had any serious US-style division about those subsequent electoral events. That is not to say that the intent has not been there, but it is important to differentiate intent from impact.

I am always very struck by an interview given in September 2020 by Sir Alex Younger, as he departed from SIS—from MI6. He said two things. One is that, of all the stuff he had witnessed in his time in terms of Russian state interference, none of it in the UK had had any strategic effect at all, in his judgment. Secondly, he said that they have proved unable to divide societies that do not wish to be divided, and that social capital and resilience matters. That is not to say that there has not been intent or some significant operations. One of the things that the speaker from Moldova—who faces much greater pressure—brought out very eloquently is that it is not just about elections; it is about the political process in perpetuity.

One of the most high-profile examples of Russian interference in the UK was the stolen letter from the then Department for International Trade in 2019. That was then amplified over the course of 2019 and became a feature in the 2019 general election campaign, about alleged US involvement in the provision of healthcare post Brexit. That was not timed. It became an election issue, but all the covert activity to steal and amplify that document came outside the electoral cycle, so it is important that we are constantly vigilant. In terms of the past 10 years, it has not been as bad as we would have feared. Right now, my analysis of the threat is that the Russians in particular are focusing on former Soviet republics and former Warsaw pact countries. That is where the bulk of their effort is.

There is a choice for the UK state about how much you want to contest that in those regions, as well as protecting ourselves.

There are four tests that I think we should apply or keep things under review on, in terms of our resilience. One is the legal framework. For example, I am not saying this was Russia because we genuinely do not know who did this, but no doubt you will recall that awful, but perniciously clever, deepfake of the London Mayor in November 2023 about the pro-Palestinian march and its clash with Remembrance Day parades. It turned out that it was not an offence to make such a thing, because it was just creating a fake video. There are possibilities to make that an offence under other laws, but, as we see with other issues around social media, there is a constant need to look at how up to date criminal law is, because it is a big deterrent. That is the first thing.

The second and third things are about the functioning of the media in the population. Robust, free media, chasing these things, looking at their validity and so forth, are really important. The third thing is social capital—things like the response. I thought the response in November 2023 from the British political system was excellent. The then Conservative Government sought not to exploit it, and to promote very quickly the fact that it was fake. If you look at other countries, such as what happened in the US in 2016 or in Slovakia in 2023, you see that political opponents of the victims of a deepfake have seized on it and amplified it. It is really important that there are quick mechanisms for debunking it. It is also worth looking at what Finland is doing to teach people, including from nursery school age, how to judge information critically for themselves, because we are going to be flooded with this stuff from now on.

The final point is: what technical innovations can we encourage and, if necessary, mandate? There are things under way at the moment; there are pilots of what we call content credentials. Big platforms have been slow on the uptake, but it is about, where you can, beginning to see the provenance of a video or document—who created it, when was it modified and by whom, and whether that is uncertain or unknown and so on—so that there is more information. Those are four things that we should be looking at.

In summary, it is something we have to be constantly vigilant about. The threat is more to our east at the moment than to ourselves, but it could come back and it has not entirely gone away. We need to be careful not to overstate the impact, because once we start creating a narrative that there is a widespread problem with the integrity of British political processes, we have done the adversaries' job for them.

Q259 **Chair:** I understand that, and I am sensitive to the potential that it would be in the interests of Russia for us to not trust our democratic system, whether or not we ought to. I understand that. However, while we might say that there has not been that much impact on the UK historically, part of the problem is that nobody ever wants to admit that they have been influenced by lies, bots, manipulation, fake videos or fake individuals. Our concern is that it seems to be ramping up. The alarm bells set off for the

Committee when we were talking to Germany. We were thinking, "Oh, it is just eastern Europe," but it is not; it is creeping across.

I will come to a question in a minute, but recently we discovered that when the internet went down in Iran for the second time, 1,300 bot accounts that are terribly interested in Scottish nationalism went dark. This is happening. Attempts are being made to influence British public opinion. The Moldovan witness was saying that that they, the Moldovans, ask, "What are our weaknesses? Where are the divisions? Where will they try to work on us?" My concern is whether we are doing the same. Are we looking honestly at ourselves and where the weaknesses may be, and then at how Russia—or wherever—is reacting to that to try to divide us? Is that work being done and who is doing it?

Ciaran Martin: Let me break it down into two things in terms of the work being done. One is more reassuring than the other, but for good reason. One is disruptive cyber-interference with the functioning of elections. Take Moldova: there is the disinformation campaign, which we have focused on. One thing that did not come out, but is well documented, is an absolutely enormous cyber-attack on the electoral commission of Moldova as the results came in. There were 898 million hits—it is one of the largest DDoS attacks I have ever heard of. What is the purpose of that? That is to disable, I assume, the Moldovan electoral commission from accurately and credibly reporting the results. So that is a cyber-attack. It is not there to sow distrust. It is there to stop something happening.

Since 2017, when I was in office, we have had a programme that was supposed to be under the old Fixed-term Parliaments Act aimed at 2020. We then had the sudden election of 2017, so we did as much as we could in eight weeks and then resumed the programme. In terms of the cyber-integrity of the British electoral system, as you may recall that register to vote collapsed just before the Brexit referendum. It turned out that was a technical fault rather than foreign interference, but you can see the point. By 2019, by that election, things like register to vote were being very closely monitored. There were all sorts of spikes in registration that were investigated to see if that was malicious activity rather than, for example, as it turned out, a celebrity having made an appeal to register to vote and things like that.

Things like the Electoral Commission's protections—you can ask the next witness about that—offer to political parties things about monitoring their systems and guidance to parliamentary candidates and so on. An awful lot has been done on the integrity of even local government and the printing of electoral rolls and voting slips and so forth. There is an awful lot done on the cyber-protection of the electoral process to reduce the risk of what happened to Moldova happening in the UK.

The problem with disinformation is that it is harder. To the aggressor, it is two prongs of the same attack fork, if you like: cyber-campaigns on the one hand and disinformation on the other. It is much harder in defence because it engages all sorts of issues of free expression. It engages the big platforms and the way they circulate things. It is much, much harder

to defend against. I would divide that basically into two phases. There was the phase towards the turn of the decade when the big platforms were still playing ball. Meta, for example, had a huge disinformation and electoral security facility when X, or Twitter as it then was, was talking to you. That is mostly gone, so some of that is harder.

Are we taking a look at ourselves in terms of these types of information? If you look at, for example, disclosures from the National Cyber Security Centre and MI5 and so forth, if you take 2022 and 2023, where they publicly avowed Russian and Iranian hacking campaigns against politicians, which were then designed to leak and twist information? It is clearly something that the security services are watching out for.

In terms of other campaigns, I come back to—I expect you will disagree with this—very carefully trying to delineate intent from impact. Those Iranian Scottish nationalist bots are an interesting case in point. It was me who gave evidence to the Intelligence and Security Committee's Russia report, published eventually in 2020, which said that the first known case of foreign interference in digital was by Russia during the Scottish referendum. That appeared in the report. What was not brought out as clearly was that the quality of that effort was risible, and in terms of the analysis of its impact, it did not seem to have any.

I would encourage objective research into the impact of some of this stuff. The Iranian bots did go offline. What impact were they actually having on Scottish politics? As you say, it is very, very difficult to work out whether this stuff is having any impact. I go back to Sir Alex Younger's point: is this having a strategic impact? It has been tried—absolutely, it has been tried—but impact does not automatically equal intent. We have to be careful about that, even if it is sometimes an unpopular thing to say.

Q260 **Sir John Whittingdale:** Can I press you a little on that? You have quoted Alex Younger saying it has not had an impact. But can you just say whether you believe there have been examples of hostile states attempting, even unsuccessfully, to influence elections and votes? You mentioned the Iranian Scottish referendum bots, but are you aware of any other attempts in the last general election or the two before that where there were attempts?

Ciaran Martin: Yes. I have already mentioned one: in 2019, there was a hack of an account—and this has all been publicly avowed—by Russian state intelligence services. I believe, although I need to check this and may have to come back and give you a note, that it was an exchange between a senior Department for International Trade account and a personal account belonging to the same person that was then hacked. The document stolen purported to speculate that, under the then Government's proposed UK-US post-Brexit trade deal, the NHS would be significantly opened up to American providers. That was then slowly amplified in a very clever way over the course of 2019—there is a report by an organisation called Graphika that sets all of this out—and then ended up featuring in the election campaign, unbeknownst to those using

it in the then Opposition that its provenance was nefarious. That is one clear example.

Q261 **Sir John Whittingdale:** It was a genuine document?

Ciaran Martin: It was a genuine document.

Q262 **Chair:** I know quite a lot about this, having been one of the people who was amplifying it in the 2019 election. We did not know it was stolen, but we thought it was very important that the public knew about it.

Ciaran Martin: There have been other things I am aware of. There is a very good report from Sam Stockwell, who works at an organisation called CETaS, which is part of the Alan Turing Institute. They do some very good reports; they did one on the 2024 election where they looked at both the UK and European elections in certain countries, including France. They found 16 completely fake things in the UK that had some pick-up. His analysis—he might be somebody that the Committee might be interested in speaking to, as it is very good stuff—is that it got some pick-up, but it was mostly in smaller communities where it was reinforcing their existing prejudices, rather than the news-dominating, game-changing discourse that happened in the US in 2016.

That was genuine information—the CETaS report is talking about fake information—but if you think about the impact of the 2016 operation; the Democratic National Committee was plunged into crisis, its chair resigned, and it was all over *The Washington Post* for weeks. None of this reached that threshold. He found 16 significant warning signs in the UK and 11 in France. They did not just disappear without trace like, for example some of the Iranian Scottish bots; some of them have some pick-up and a lot of them disappear without trace. These did get pick-up, but they did not break out of tight and closed circles. There is definitely intent; I am not saying there is not. I know there are different and strong views on this, but that is why I was quoting Alex Younger saying that its strategic impact is not clear. But the intent is there.

Q263 **Sir John Whittingdale:** Were you able to trace where these originated, down to specific buildings in Moscow, Beijing or Tehran and say, "This was a state sponsored activity"?

Ciaran Martin: Sometimes. The best known example of counter-operations against that is something that used to be called the Internet Research Agency in St Petersburg, which was flooding the US with disinformation. That was a follow-up to the 2016 attacks. In 2018, the US was so significantly concerned about that ahead of the midterms that they essentially launched their own cyber-attack on the Internet Research Agency and took it offline. Its capability to produce and amplify that type of fake information was significantly degraded.

Since then, you have got you classic intelligence and detection problem. I have no idea who was behind the London Mayor fake, which was a very serious attempt to undermine stability in the capital. The geopolitics would suggest Russia, but I have no more evidence than that about Slovakia,

which is another area where there was a completely fake intervention. Until the controversial events in Romania, which you have already touched on, the most striking example of a digital intervention that seemed to move the dial in an election, either through amplifying controversy or shifting the polls, was Slovakia in 2023.

I do not know who did that; the geopolitics might suggest Russia, but there are no technical indicators that I know of. You have got that classic problem where you have got everything from knowing that there is a building in St Petersburg where this stuff is coming out of to having absolutely no idea who is behind a particular operation and everything between. We have got some suspicions.

Q264 **Chair:** Are you confident that there have been disinformation attacks on the UK from China?

Ciaran Martin: Yes. China's operations are slightly different. There is a Venn diagram. The bit that Russia does, but that China so far does not, is disruptively hack electoral commissions, or indeed anybody else. It might prepare them, but China has no history of actually taking stuff offline. It has a huge history of spying and so forth, but no history of just sabotaging digital equipment.

China has a different history of influencing—a lot more human activity. There have been all sorts of controversies that you do not need me to go into. It is fake news social media accounts until around 2020. Certainly, when I was in office, there was not that much, if any, of it about. I think they are getting into that game. In 2024, there seemed to be some evidence of China showing some interest in the US, and a tiny bit of interest in the UK, in terms of getting into fake social media accounts.

Some of it was quite poor: for example, an Australian company called CyberCX did a report—I declare an interest because I work with the company—in August 2024 about the US and they showed that there were some fake accounts that were trying to sow distrust and disinformation in US politics. They were not very good. For example, if you replied to them on X, they would give you one of two replies. One was in English, and it would say, "I'm sorry, as an AI generated bot, I am not allowed to reply," and the other was in Mandarin characteristics—which rather gave the game away.

The point being, because I am not trying to sound complacent: it is China, so they will get better. They are getting into this, and then of course, they have this huge swathe of human and hybrid human-digital activity. We know, for example, that they are very good at social engineering—finding people on LinkedIn, for example, and then cultivating them. They are interested in that type. My reading of them at present is that they are more interested in political influencing than in electoral outcomes. Right now—it could change—I do not think they would ever want to be in a position where people say, "China sabotaged the election."

Chair: No, I understand. A couple of people are itching to get in.

Q265 **Emily Darlington:** You are talking about some really classic cases of traditional election manipulation. I am not sure if you are aware of the Science, Innovation and Technology Committee's report into misinformation and disinformation during the riots and the role that state actors played within that. While they did not create it, the evidence shows that they amplified in order to create that environment. When we are looking at how activity is changed, we are looking at material throughout the year, not just in election time, that is created to destabilise the country itself. We are seeing that rise on YouTube and TikTok accounts. Are you involved, or is the National Cyber Security Centre involved at all, in researching whether those have state or non-state actors, and whether they are purely for financial gain or have a more nefarious purpose?

Ciaran Martin: I left Government service five and a half years ago, but I am aware; I am not an expert in the detail of that, but I am absolutely aware. It is a very plausible and credible analysis, because adversarial states would want to exacerbate division in this country. It would absolutely, squarely fall into the remit of the broader security services to try to find out who is doing that and try to take whatever action that needs to be done upstream, if possible, against the people doing that type of thing.

How do you then defend against it? If you cannot stop it upstream, or cannot stop people from remotely amplifying this sort of thing, then in terms of policy tools against it, it is a really wicked problem. It is to do with social media regulation and with the critical analysis faculties of people in the UK. It is to do with all sorts of different things. I think it is a really hard problem. I am sorry not to be more helpful, but it is definitely happening. It will be on the radar of the security services; I have no doubt.

Q266 **Chair:** That is our point: we have seen some of that inauthentic amplification of lies, targeted at trying to divide our society. Our concern is that it may get worse in the future. We wondered if anybody had any answers, or any reassurance that they could give us about whether that could be stopped.

Emily Darlington: And some clarity about which agency has responsibility for that. What is the role of the Electoral Commission? What is the role of security services? Everyone seems to say that this is somebody else's responsibility.

Ciaran Martin: Well, the security services would have two roles. One is to warn people about it and, if necessary, disclose it. That may sometimes conflict with their other role, which is to take action against it, possibly covertly, which they would not declare. That action is perfectly lawful but it would probably, so they could get it all at once, remain secret. For example, the Americans—they have never officially acknowledged this; it has just been leaked all over the media—destroyed a large part of the Russian disinformation infrastructure in 2018. There is a wing of the state for that and it is hard, in terms of public reassurance, to talk about this issue because activity against it would necessarily often be covert.

I am not speaking for the Government—and perhaps members of the Committee will not like this answer—but this is a fiendishly difficult thing to thwart at an open policy level. Is somebody there in the Government as a sort of arbiter of what is true?

Q267 **Chair:** No, we are not talking about that. We are being quite careful not to do so. We are talking about inauthentic amplification. That sidesteps all the arguments about freedom of speech: you can say what you like, but why should you get it amplified on social media so that it is in front of people's eyeballs all the time? The reason that is happening is because people want to divide societies—there is another motivation and algorithms are being manipulated, or whatever.

Ciaran Martin: Yes. That, again, gets to things that are contentious. There are good reasons and bad reasons for this, but we do not have very strict laws, pretty much anywhere in the liberal democratic world, about verifying the origin of accounts. We allow anonymity, both in terms of names—the literal thing—and geographically.

There was the feature that briefly popped up on X where you could say where the account originated from—that shed some light on this. In my view, we do not have a particularly strong record, anywhere in the west, on holding people to account who are authentic amplifiers of fake information, which is another problem. If you look at what happened in Slovakia, it was high-profile Slovaks who amplified it. There are very few mechanisms—other than, frankly, shame and negative media coverage—for handling that. I think the question should be asked, but I do not think we should expect any answers.

Q268 **Chair:** Of whom should we ask it?

Ciaran Martin: You can ask two sets of people. One set is the social media companies, and the other, essentially, would be the Department for Science, Innovation and Technology because this is about the regulation of social media, the Online Safety Act and so forth.

Q269 **Chair:** What about the Defending Democracy Taskforce?

Ciaran Martin: That is just a committee of people who bring lots of different things together in Government for a multifaceted problem. That includes the education of kids in critical thinking and goes all the way through to the security services' covert disruptions.

In terms of policy, you are asking me about a very specific problem: inauthentic amplification. In my view, the only solutions to that would be, first, a much more detailed knowledge base about where high-volume accounts that amplify things come from and secondly, the powers to remove them. Those are two huge policy decisions for Parliament that are way beyond me. Where does that policy brief lie? It lies with the Department for Science, Innovation and Technology, as far as I know. That would be my answer.

Q270 **Fleur Anderson:** My question follows from that. I want to go a little more into where those deepfake images—the intimate sexual images that are

being talked about a lot at the moment—come from. We have seen their use in other countries around and between elections. We fear that there will be more of that, particularly with politicians and their images being used. The scale and difficulty of this issue seem very hard to deal with, but is there more that can be done to know the provenance behind an image and where has it come from, such as through watermarking? Could more be put into the Online Safety Act as it develops? What would you recommend we do so that if someone takes my face and puts it on to an image, I can find out who did that? Is that down to the platforms or the producers? Is it too hard to do if it is done internationally, or are there things that could be done?

Ciaran Martin: I will try and briefly break that down into two. If someone takes your image and manipulates it, there are ways—which could be accelerated, tested and piloted—of determining very credibly that it has been doctored. It may be obvious, but in terms of fake images and people trying to convince others that you are doing or saying something that you are not, there is also emerging technology, which could be fast-tracked and tested, that allows you to say, "No, this is not genuine—this is altered" and so on.

Who is doing it takes you back into that whole anonymity piece; Parliament is very active in one aspect of that space this week. There are also issues of even keeping up with what is illegal in terms of criminal law. If you look at the medium-term horizon for this stuff, there are grounds for optimism in terms of being able to give people the information that they need to establish the authenticity of information—and visuals and audio and so on—and whether something is the genuine voice or image of this person, or something that has been doctored.

Because of the whole foundational anonymity online, it is less clear if somebody maliciously edits and alters that. You are back to the same issue with the amplification of social media accounts and whether you know which IP addresses that is coming from. Is it somewhere that you can do anything about it, and is it the real IP address or something that is masked? It is still quite easy for people to hide online and do such things.

One of the biggest problems in all sorts of online malevolence is jurisdiction. Ultimately, if you are doing something from the UK landmass, there is a pretty high probability that the British police will find you, but if you are doing something from lots of different parts of the world, there is essentially no chance. You are then into things such as the transmission mechanisms and the obligations on social media platforms to take this stuff down.

The optimistic news is that it should soon be easy enough to tell what is real and what is fake—and we need to move faster on that. The bad news is that it is going to be very difficult to hold people to account for malicious fakes, particularly when they are based abroad.

Q271 **Fleur Anderson:** So social media platforms could say, "This is fake" at the bottom of a post and track it. They could say that something was fake

even if it was very hard to find out internationally where it came from.

Ciaran Martin: Internationally, there is lots of stuff being trialled. As ever, with some of these platforms, you could take a benign view that they are doing their best as quickly as they can, or you could say that they are dragging their feet. Some of them would say that the error rates are currently too high, but there is technology that is proving its worth—the content credentials stuff I mentioned at the start—where it is quite realistic that within a few years, if you go on a social media platform, or anything actually, you could have some sort of label that says, "Completely unaltered image", or, "Completely artificially generated", or, "Based on a real image and modified at 2 o'clock in the morning"—or 3 pm in the afternoon. But it will be probably a bit like Wikipedia where it says "by user xyz!@", and who is that? That is probably the best way I can put it.

Q272 **Dan Carden:** Does the Government have the ability to see which platforms are allowing content, for instance, or misinformation and disinformation from our adversaries such as Russia and Iran?

Ciaran Martin: It is all publicly visible, so the question then is: do the Government know, potentially in ways that the public do not, that that is platform misinformation? The answer to that will be sometimes, if the security services have that information. I am guessing—certainly this is how it was when I was there—that there is your classic intelligence versus enforcement trade-off, so that once you have shot something down, that is your access into it gone.

Q273 **Dan Carden:** Could more be done to use some of that security information to put pressure on such platforms?

Ciaran Martin: Yes, but it does come back to the whole posture that you want to take with regard to social media. There are obviously some very difficult politics with the US at the moment in all of that space, but that is a judgment. Absolutely, you could tighten duties to take stuff down, including at the request of the Government. There are all sorts of policy trade-offs in doing that, but you can do it. The Government are perfectly capable of forming an assessment based on mostly public information, but also potentially some classified information, about which platforms are more responsive to that than others.

A different point is about algorithmic bias—to what extent the various algorithms are configured to highlight those types of things. To go back to the Chair's point about inauthentic amplifiers, amplification is not down to the malicious account holder alone; the underlying factor is bigger, and that is whether the underlying platform is configured to allow that. Certainly those platforms that are incentivised to amplify division probably are—it is pretty obvious who we would be talking about here. You could certainly make an assessment of that, but actually proving how the algorithm runs is harder, because the platforms have no obligation to give it to you.

Q274 **Chair:** I did not realise this until recently, but the bots amplify one

another. They are all connected, so you can put out a message and, suddenly, 400 people allegedly like it, but none of them is your family or friends, that's for sure—they are all John3567 or whatever.

Ciaran Martin: Exactly.

Emily Darlington: And you can buy them.

Chair: And you can buy them, yes.

Q275 **Dan Carden:** On the policy options, you mentioned that we allow anonymity on the internet and then the idea that we could have location of accounts—that we demand of companies that they highlight the location. There are tech challenges to that, I think, but is that something that could be pursued?

Ciaran Martin: I would be sceptical as to its effectiveness. What happened with X, as I understand it—this is not the area of my deepest expertise, which is mostly on actual cyber-attacks—is that X started to say, "Here's where the account was registered", and made that public. Because that information was not previously visible on X, you did not have to bother to disguise where you were coming from, but if you did have to bother, it was quite easy. If you were malicious enough, you could just say, "Well, I am not going to declare this legally and put an Iranian IP address any more, or write 'Iran' on the form. I am going to do something else." That is quite easy, so I would be sceptical about that as an effective tool.

Q276 **Dan Carden:** To change topic, part of the strategic defence review is looking at a whole-of-society approach to the threats that we face. In your experience, what is your assessment of our social resilience to these attacks, the hybrid threats that we face, such as cyber-attacks, and other global threats?

Ciaran Martin: My biggest worry from a homeland protection point of view, if that is what you are asking, is the vulnerability of important economic and social infrastructure to sabotage, fairly medium-sophistication sabotage. To put that less pompously in plainer English, the Jaguar Land Rover attack scared the hell out of me—

Chair: And Marks & Spencer.

Ciaran Martin: And Marks & Spencer, but particularly JLR because of the cost. We can debate them, but yes, they are both really serious. That is mostly because of—what word am I looking for? It is not "benign"—the strategic insignificance of the attackers. They are Russian-based criminals. They have no political agenda. They are looking for money and trying to extort money. For the Marks & Spencer one, some British people have been arrested, but it is people looking to make money. It turns out that they can empty supermarket store shelves, force the Government into a £1.5 billion loan guarantee and knock 0.17 percentage points off GDP growth in September with one cyber-attack. That is an illustration of the vulnerabilities.

A lot of that—Marks & Spencer looks like an exception—is coming from Russian-harboured cyber-crime. There is a set of capabilities from within Russia that could be repurposed for the state. It is obviously a very different country in terms of economic and social profile, but Costa Rica was forced to declare a state of emergency in 2022 because of a cyber-criminal attack. The Irish healthcare system was brought to its knees in 2021. These are all individual attacks. You could aggregate all of those from within Russia, and you are in serious trouble.

I mentioned China, which has no history of sabotage, but it does have something known in the cyber-security industry as the Volt Typhoon campaign. It was identified by the US in 2023, but our Government signed up to look at it, and although there has been a change in the party of government in the US and the UK, both current Administrations in Washington and London continue to assess that China has planted digital booby traps—that's the best way of thinking about them—all over critical infrastructure, except interestingly in healthcare in the US.

The Australians have said they have found similar booby traps in Australia. We've said we haven't found them, but we assume they are probably there because if they are in the US and Australia they are probably here, too. The way I would think about that is 10 to 100 Jaguar Land Rover-type events at the same time. China is assessed to be a rational actor—you may not like what it does, but it is not an irrational actor—so that is not assessed as something that will happen tomorrow, but it may be, if there is serious tension over Taiwan, for example, that we have that sort of vulnerability.

Similarly, if, for example, we end up in a situation where it is falling to European nations to provide sustenance to the Ukrainian effort without the US, and Russia wishes to deter that, there are a series of things. My one biggest fear is that cyber-crime has shown the nation states a playbook for how to make life really uncomfortable in this country.

Q277 **Dan Carden:** It is very difficult: this is to do with our supply chains, manufacturing and reindustrialisation. Which part of Government is responsible for that?

Ciaran Martin: That is DSIT, and a lot of it is dealt with, up to a point, by the Cyber Security and Resilience Bill, which had its Second Reading last week. Interestingly—and I am not criticising the Government here—Jaguar Land Rover would not be covered by that.

Q278 **Chair:** Exactly—Tata Steel.

Ciaran Martin: Well, it's not just because it's Indian owned, but because although it is an important company economically, it is not providing water or—

Q279 **Chair:** I thought it was because the data centre was abroad and the management of it was abroad, and it would be more difficult—

Ciaran Martin: No; it doesn't matter where the data centre is. If, for example, Thames Water had a data centre abroad, it would still be

covered by the Bill. That is my understanding, because it is about the service provision. Although Jaguar Land Rover is very important, there is obviously a difference between coping without a water supply and coping without the ability to produce cars. You have to draw a line somewhere.

On the critical stuff, the Bill is, if anything, overdue—it's good news, but we have to think a lot smarter about things that are very important but not critical, such as Jaguar Land Rover. There is a lot you can do in terms of corporate governance. One challenge, to be provocative in policy terms, is that our regulatory framework for cyber-protection and resilience, like every other developed country, is obsessed with personal data, almost to the point of fetishisation, and does not incentivise resilience.

I have two classic examples of this. One is Jaguar Land Rover. What are Jaguar Land Rover's legal duties? To protect customer data. Who cares? It is a list of people who bought cars. That doesn't tell you very much, and the information that you get from that data leak is mostly available in the telephone directory. Jaguar Land Rover's legal obligation was to protect that, but not to protect a vital economic artery and 30,000 jobs in the supply chain.

The Irish healthcare system was even crazier. The whole national healthcare system went offline and, after four days, the hackers—because they were not getting paid—released small amounts of medical data. It was only then that the Irish health authority was in breach of the law. Irish law has changed since then.

We need to think about what we actually want to incentivise. With a lot of experience, we are beginning to realise that there are some data breaches that really matter and some that are glorified telephone directories. We don't differentiate between the two, and we tell all our organisations, no matter who they are, that personal data is their most important obligation. I don't think it is, and if we are serious about social resilience, we want to incentivise car makers, charities, local resilience groups—everybody—to maintain their services to some extent in the event of a large-scale cyber-attack. I will take a few data leaks if that is the price that has to be paid. That is my little rant.

Q280 **Sir John Whittingdale:** Could you just repeat something? You mentioned the alliance against the Chinese, which could be maintained under—

Ciaran Martin: The codename? The Volt Typhoon. Is that what you are asking about?

Sir John Whittingdale: Yes.

Ciaran Martin: That codename was given by Microsoft, because they were the first company to discover it, but it has been adopted by the Government. It is known as the Volt Typhoon campaign. Essentially, what is strategically important about Volt Typhoon is that you don't have to like China—you don't have to be a China dove—to say that it has never been caught sabotaging anything in cyber-space. It has probably been the

largest data thief in human history, but it has never sabotaged anything. This is preparation for sabotage.

Q281 **Richard Foord:** What are the advantages of the NCSC's public-facing role?

Ciaran Martin: The main one is being able to give guidance—not just saying, "You should do this. This is best practice," but actual, specific information. There was an interesting experiment in 2018, in the early years of the NCSC. I am afraid that, with the passage of time, I can't remember the exact figures. Initially, we said, "There is an interesting nation state campaign against the telco sector," and nobody noticed it. Then we said, "There's a Russian campaign against home routers," and the take-up was very significant. We gave the indicators of compromise and the activity taken. The first advantage is essentially being able to share that threat information.

The second advantage—I wouldn't discount this—is to give some form of public reassurance and to grip national incidents. One of the reasons why the NCSC was established was the response to the first cyber-incident to lead the news in this country, which was the TalkTalk data breach in 2014. There was widespread panic about what turned out to be not that big a data breach, but the question being asked about disinformation was, "Who is in charge?" and the answer was, "Nobody." There was nobody like a chief of police, a chief environmental flood officer, a chief vet, a chief medical officer or whatever to say, "This is who is at risk, and this is who is not at risk." Having that is very valuable. Those are the two main points.

Q282 **Richard Foord:** Has this model been copied by some of our allies? Have we seen the NCSC model picked up elsewhere?

Ciaran Martin: Yes. In terms of the other Five Eyes, the Canadians and Australians have done much the same thing, and the New Zealanders might say that they were doing the same thing before us. As with everything, the Americans have multiple agencies, and they are all bigger, but CISA—the Cybersecurity and Infrastructure Security Agency—was given the task of copying the NCSC's public-facing work, but not its classified work, whereas the NCSC does both.

Q283 **Richard Foord:** What do you make of the reporting and accountability arrangements for the NCSC to the Government?

Ciaran Martin: I think they are a bit weird, if I am honest. They are accidental, like a lot of things that are a bit weird. It is all to do with history. GCHQ reports through the Foreign Secretary, but after the first world war we realised that what was then called the Government Code and Cypher School should protect British secrets, and that was done through the Prime Minister and the Cabinet Office. There was always this little weird bit of GCHQ that did protection of the homeland through the Cabinet Office, but because it was a secret for 80 or 90 years, nobody bothered about it.

Now the NCSC is out in public. It is still part of GCHQ—that is probably a good idea—but the ministerial accountability works through the Foreign Office, despite the fact that it is mostly about domestic protection. In my day, you would have liaised with DCMS—now DSIT—for policy. You would deal with the Home Office for crises, and the Cabinet Office for strategy, which is a bit weird. It was never prohibitively costly, but it is not the cleanest arrangement.

Q284 **Richard Foord:** How would you do it differently, if you would at all?

Ciaran Martin: I should say—even though I am not there any more—that one strength is its accessibility to Parliament. That is a good thing. The fact that it is not cosseted just within the ISC, and it does the Joint Committee on National Security and so forth, is a good thing.

How would you do it differently? My understanding, and this is public, is that MI5 has always had a Northern Ireland wing that has always operationally reported to the Northern Ireland Secretary, even though the Home Secretary is responsible for MI5 as a whole. You might make that a little bit cleaner with the Home Office. If the Home Office are going to be in charge of gripping incidents, then you might make that a little bit cleaner. I am not sure how big a problem it is, but you asked me a direct question about how the accountability works, and I have given you an answer that is a bit messy and weird.

Q285 **Richard Foord:** Finally, you were here for the Moldova session that we had before, so you have had the lead-in with our questions around disinformation. What do you make of the proposal to make a national counter-disinformation centre?

Ciaran Martin: I am agnostic. I think you would need to do a serious piece of work. Setting up the NCSC actually flowed from a change of strategy—I think that is really important. The then Government decided to be more active in cyber. They had been very passive—they were very much like, "Let's encourage people to share information and form forums with the private sector," and so forth. I said that there were direct interventions they could make—not just covert stuff, but all sorts of things. There are digital pollutants, but the market is not incentivised to take them down. The Government should have a unit that will just go and do that sort of stuff. The Government should have a single point of incident management. The Government should have a single repository of advice for critical infrastructure and so on, if it is going to be more active in this space. That was all because of the change of strategy.

I would ask what the Government are going to do, and as we have discussed, there are some really difficult questions in this. If the Government then say, "Right, here is what is going to change," and if putting a single body in charge of that makes sense, then do it. But it might not. For example, it would take in everything from educating people in civics and how to process and analyse information, all the way through to top secret activity by GCHQ and potentially MI6 against foreign

operatives who are doing this stuff. That will be a tough thing to put into a single organisation. That is why I am agnostic.

Work out the strategy. The first question is what is the state's best policy; what does it want to do and achieve, and what is going to change about the way that it does it? The second question is how you organise that, because it could be that you have it in multiple places—sometimes that is where you put hard problems.

Chair: Thank you for your time. We really appreciate seeing you, and the thoughtful way you have given your evidence.

Examination of Witness

Witness: Vijay Rangarajan CMG.

Q286 **Chair:** We appreciate you coming to see us. Could you introduce yourself, please?

Vijay Rangarajan: I am Vijay Rangarajan, chief executive of the Electoral Commission.

Chair: And you were previously in the Foreign Office.

Vijay Rangarajan: A long time ago—about 20 years or longer ago—yes.

Q287 **Chair:** I think it would be right to say that the Electoral Commission gets beaten up a bit. People, particularly politicians, criticise you for not being strong, for not using all your powers or for not acting fast enough. Do you think you are in a better position to be more robust in your approach to combating foreign interference in the future?

Vijay Rangarajan: I think we will be in a better position. We are on a track to do that, but there is a lot of work to do. It needs to be done not just by us but with a number of other bodies, although we have a fairly critical set of things to do. The first thing to say is that Parliament approved our corporate plan last year, which added a whole set of threats, one of which was foreign information, and gave us the money to do something on it. We are going ahead and simply implementing what is in that plan at the moment.

Q288 **Chair:** How many people are you employing to do that?

Vijay Rangarajan: We will grow by about 100 people to do that.

Q289 **Chair:** About 100 people to counter foreign interference in our electoral system.

Vijay Rangarajan: And to do a number of other things. Part of it is about running a large education project that has an element of digital literacy, because we are going to try to reach most young people in the UK before 16-year-olds vote, probably at the next general election.

Part of it is about running a programme for this May's election to identify deepfakes, which we have already heard are coming. They are already there in other elections around the world, and someone has to actually scan for them and do that. We have set up finance, and I have just done the contracting for a deepfake identifier that is going to run.

We are doing a lot of work with international partners, because we are trying to learn from them. Our elections come around every year or so, but there are plenty of international elections where we are seeing the playbook exercised, so we are trying to learn from that and keep ahead of it.

Finally, in terms of our powers, some of the changes that we want in political finance and our investigatory powers will be in the elections Bill, which the Government said in the elections strategy that they will shortly bring forward. We have some quite clear views as to what we think would actually help us to tackle foreign interference there.

Chair: We will probably expand on this through the questions. However, if you feel that we have not covered everything at the end, make sure that you make that clear, and I will certainly give you the time to explain anything else.

Q290 **Emily Darlington:** Picking up on your point about deepfakes, the current legal position is that it is illegal to "make or publish a false statement of fact about the personal character or conduct of a candidate"—that is off your website. Do you think that that is strong enough legislation for deepfakes?

Vijay Rangarajan: It is very old legislation. Like a lot of electoral legislation, it has not kept up with the times, and I think that is an area where we would like to see a more fundamental look at not just the thresholds—there is obviously a balance between political free speech, satire and humour—but how it does not apply between electoral campaigns.

One of the things that Ana quite rightly pointed out was that a lot of the fundamental structure of our electoral legislation is such that not much politics and campaigning happens in between elections. In electoral time, you have long campaigns and short campaigns, and—you are all aware of this—some of it is retroactive in where campaign finance limits and a lot of law applies.

The example I would draw on is one of your colleagues, George Freeman, who had a rather good deepfake made of him apparently—obviously, it was wrong—defecting to Reform. We think the reason why it was not a crime at that point was because it was outside an electoral period; it would have been more likely to be judged a crime had it been in an electoral period. I think that the distinction between being in a campaign period and out of a campaign period is broadly falling away for all the reasons of social media and where the money comes from.

It is also really germane to foreign interference. The groundwork for foreign interference is laid entirely between elections, and then it is activated later on. I think there is a piece of work that needs to be done, and we have started to think about how we actually modernise that part of the electoral legislation itself.

Q291 **Chair:** Are you not working with the Home Office to set up a unit to scan for political deepfakes?

Vijay Rangarajan: Yes, we are—this is the contracting that I mentioned. The Home Office ran a really useful and interesting deepfake challenge, where it assesses all the technological tools, and there is a big range of them, as Ciaran already said. Some of them work, some do not, and some will work better on video, audio or text. We are redoing and building on some of its work to choose a set of deepfake identifiers that will then hopefully run from March to about June.

We are keen to pick up the run-in to these crucial elections in May—obviously, there are incredibly important elections in Wales and Scotland, as well as a whole set of English local elections. Rather sadly, we expect that we are going to see more deepfakes, partly because the barrier to entry for making them has fallen so precipitously that anyone can make them. We have seen them used extensively in other elections around the world, so why would we be an exception? It will be a useful evidence base. As part of this, we are going to create an evidence locker; we will try to capture all the deepfakes that we have, and then we can use them to analyse further. If we find them, we will flag them to the relevant candidate or party—I have had pretty extensive discussions with the parties about how they would like to handle this.

I think that that will create some difficult judgments. In cases of electoral process disinformation, we will come out very strongly and say, "That is untrue and wrong," will flag it to the social media company—we are now a trusted flagger or have various arrangements with the companies—and will ask it to remove that information. We will then probably report back to you and other Committees on whether it does so.

A great example of that was in the recent Irish election. Three days before the election there was an incredibly good deepfake of Catherine Connolly, the winning candidate, announcing that she was withdrawing from the campaign. It was in the context of an—again, totally fake—RTE presentation, saying that her opponent had therefore won, so people should not bother turning out to vote. If that happened here, we would come out very quickly and say, "That's false—she hasn't withdrawn," and we would know that, because we are running elements of this. We would contradict it. Where we will not be able to get involved is in pure campaign information, because no one regulates campaign material itself.

Q292 **Chair:** The problem for women candidates is that, as we know, this is not just going to be about that. That is quite worrying for us. I was just looking up the targeting of Maia Sandu, the Moldovan President. The deepfakes that were put out about her were deeply insulting and highly

sexualised; they were trying to undermine her as an individual. That would obviously have a political impact, but it would not be, strictly speaking, political. Would you be dealing with that?

Vijay Rangarajan: Yes, we are still going to scan for those and flag them, and we would then go to the companies and ask for them to be taken down. We would also go to the parties themselves and other candidates, in some circumstances, to say, "This is completely false and you should not in any way be amplifying material like that." So far, all the political parties have taken a very responsible attitude to that. We would like to see some of that material included, potentially, in the revised code of conduct for political parties.

Chair, you are absolutely right that we have seen—we published a large report on this after the 2024 general election—tremendously increased abuse and intimidation of politicians, both online and offline. It has been very heavily focused on women candidates and ethnic minority candidates—twice or three times as much. The Speaker's Conference did a lot of really useful work on that. We have just done a formal reply, which commits us to essentially implementing all the recommendations that fall to us. One of the interesting points is the interaction with social media abuse, which, obviously, a lot of you get, and a lot of which is horrendous. The Scottish Parliament has been running an interesting experiment to centralise, a bit more, the analysis of social media abuse coming to MSPs. It has already resulted in one successful prosecution, because it was possible to trace back to who was generating it.

It is not a completely atomised, disparate set of people—some people are producing it. If every MSP or every MP separately—poor you or your poor staffers—has to take down, remove or delete this material, it is very hard to spot those linkages. We think that more protections are needed, not least because, fundamentally, this is putting people off becoming political candidates. That is the real threat to democracy that we see. We have flagged this for discussion with the Senedd and with Westminster about how we manage to expand that system.

Chair: I am mindful that this is a pet topic for many of us who are victims of it, and I would ask the Committee to try to keep on track, because we have a lot of other questions to ask. Emily, do you have any more? Then I will go to Fleur.

Q293 **Emily Darlington:** This is in the same vein, but it is not about me. There are 73 TikTok accounts posting thousands of deepfakes about Keir Starmer announcing controversial policies—obviously, outside the election period. They have names like "BBB UK News" and "Daily Britain News". We are not sure whether these are foreign state actors or foreign non-state actors, and I do not know whether you think we should be treating those differently—many of these reach the threshold for making money. They posted 197 videos in just one week in December and over 6,000 since May.

My question is, is the Electoral Commission aware of this kind of deep-fake

activity? In particular, are they aware that these 73 accounts use real news footage, but AI-generated audio, to announce controversial policies that are not Government policies or party policies? I am only focusing on this because, clearly, Keir Starmer is the focus of a lot of these attacks, but I am sure it is happening to every single party.

You spoke about your skills to investigate. When you talk about taking it down and telling social media companies to take it down, do you think you have the powers to do that? How do you tell whether those accounts are linked to state actors and amplifiers? What real tools do you then have to recognise when there is the use of state-linked and non-state-linked foreign bots to amplify this material?

Vijay Rangarajan: We are aware of this kind of material. At the moment, it is not really covered by anything that we can take down. Where we would immediately go for take-down is where—this has happened—there is actual incitement to violence or threats against politicians. That triggers it instantly, and we will then try to do something about that. What we have been saying is that anyone—

Q294 **Chair:** So whose job is it, then, if it is not yours?

Vijay Rangarajan: I do not think it is anyone's job at the moment—not that I am aware of.

Q295 **Chair:** Really? So you can just put out a fake video, claiming that the Government are putting out some sort of policy, which is not true, and nothing can be done about it?

Vijay Rangarajan: At the moment, anyone would be able to say, that is just the way you have to take down. That is partly because of a long tradition of political free speech. People say very misleading things and they may be completely wrong, and they have a right to be wrong and erroneous and make things up, but where it is a foreign interference operation like that, the powers both in the Online Safety Act and the National Security Act on foreign interference operations—the directed attempts—ought to come into play, but those are for the agencies.

From our point of view, we are actor-agnostic. We do not really mind who is doing the mis- and disinformation. There are two reasons. We do not have the capabilities to analyse deep down the chain of repeated bot accounts, for example. Also, this happens extremely quickly. It will take us, or anyone, quite a while to work out final provenance. What we are much more interested in is the immediate effect of this in an electoral context, where actually you have got to act pretty immediately. Trying to work out who is doing it will take days, weeks, months—whatever it is. In a way, we do not really mind who is pumping out whatever piece of misinformation. We will just act on that immediately in the event. It is quite hard sometimes to disentangle the questions of whether it is a foreign actor, a set of domestic actors, one intermingled with the other or whether it has been triggered by a foreign source but actually generated domestically and so on. As I say, the barriers to entry are very low.

Q296 **Chair:** So the fake Keir Starmer video can be put out now, but it cannot be put out during an election period?

Vijay Rangarajan: It could still be put out during an election period, but if it got any traction and started to go around, we would then try to see whether it a fake video, and then we would try to run through the sort of protocols and rules that we are going to try to develop. Is it something that we should flag for take-down to social media companies? Is it something that we should be flagging to the politicians or parties concerned? Should we be telling the media about it?

Q297 **Chair:** How long would that take?

Vijay Rangarajan: We would have to react very quickly. The Catherine Connolly video got several hundred thousand views within the three days it was up, and there were quite a few hundred genuine interactions with it by Irish voters. This has to be done really quite quickly, which is one reason why asking who has done it is a later question and probably one that others are better placed to answer. We are interested in just actually trying to get it removed as quickly as possible.

Q298 **Sir John Whittingdale:** One of the quickest ways of getting out the message that this is a fake video is, as you mentioned, talking to traditional, not social, media. Traditional media will have an inclination to want to believe things. They want to create headlines and splashes about revelations. To what extent are you able to talk to traditional media before the tabloid press go and splash a story to say, "Hold on a minute—that's actually a fake video"?

Vijay Rangarajan: Exactly. That is one of the things we would look to do in some circumstances. In the Catherine Connolly case, the George Freeman case and others, it has been worth going to the traditional media, really opening it up and then going public. In other cases, there is going to be a balance as to whether you want to give it extra prominence, and that may not be worth it. In some cases where it is clearly illegal, we may go to the social media companies asking for rapid takedown and then not give it prominence in the media at all. We are going to have to work very closely with the people most concerned—those who are the subjects of it—if we detect some.

Q299 **Emily Darlington:** I am conscious of time. A quick question, how does the Electoral Commission monitor spend by political parties on bots or foreign bot activity to amplify or attack parties? It may be different during short or long elections, but this is clearly one of the ways in which we know foreign actors are interfering or creating disunity within the country.

Vijay Rangarajan: We do not have the capability at the moment to monitor large bot networks and so on in the sense of misinformation and disinformation. That is where we are working within the defending democracy taskforce and directly with the agencies and others, and are more reliant on their capability.

Q300 **Chair:** When you say, "We do not have the capability at the moment", are you expecting to have the capability in the future, or are you expecting to

rely on the security agencies to have that capability?

Vijay Rangarajan: We are expecting more to rely on the security agencies for that capability, and for them to then flag to us when they see suspicious activity, in much the same way we do—and which they have done.

Q301 **Chair:** Then what do you do?

Vijay Rangarajan: It depends on what it is. We saw some of this at the general election where there were clear campaigns to try to raise some foreign issues—Israel-Gaza was one and there were several others—which were trying to destroy community cohesion in this country. I think that there were legacies of the Southport riots there as well. Again, people flagged those.

Q302 **Chair:** Then what do you do?

Vijay Rangarajan: We would then make it as transparent as possible. There is a very powerful thing here, which is just explaining to large numbers of people in the country that this is inauthentic and false. We couple that with education, which, as I said initially, we are hoping to do, to give people more of the tools of digital literacy. When talking to our colleagues, particular in Moldova—and we have had contact with the Moldovan electoral commission, the Ukrainians, the Finns and the Swedes and the South Koreans—we see that they are a bit ahead. They face greater threats than we do, but they all put a very strong emphasis on digital literacy and education.

Q303 **Chair:** Before we move on to that, I want to understand something. You have said that in the past, you have noticed armies of bots amplifying lies during the general election, and you identified that and said that it was happening and made announcements. How long did that take and how much pickup was there of what you had to say compared to the original messages?

Vijay Rangarajan: We and others did. Can I come back to the Committee on that? I do not remember the timings exactly.

Chair: I think that it is important to understand this.

Q304 **Emily Darlington:** There is an important point here. The beginning of my question was on how you are monitoring spend by UK political parties on bots.

Vijay Rangarajan: In terms of spend, the standard party spending limits apply. We get statements of accounts by all the political parties after a general election and we regularly publish those—and again, I think the transparency is important. Some of those show exactly what the different parties have been spending on social media in general, but the parties describe their spend in very different ways. That is not just because of their size, but because they categorise it differently. There is an advantage in moving to a slightly more systematised way of categorising the spend by political parties. We are looking to do that as we work through the new

political finance online system with the parties. We do not specifically monitor how much parties are spending on any particular element such as bots or social media at the moment.

Emily Darlington: Do you think they are being honest?

Chair: No, let us move on.

Q305 **Edward Morello:** To follow up on that, the Committee has seen or heard evidence of foreign actors deliberately amplifying messages designed to break down social cohesion. Sometimes those are messages by political individuals or political parties. From the point of view of the Electoral Commission, if a foreign actor is deliberately using its bot network to amplify a domestic message by a politician or political actor in the UK, is that electoral interference, or do we just accept that is how social media and the online world works?

Vijay Rangarajan: I think it will depend a bit on the case. We have had an attempt by foreign actors to try to influence politics in this country. That would be a foreign interference offence operation going on. We have seen cases where political actors in this country have used international events as a way to generate political interest. We all know the issues over the general election. We have seen a number of different tools being used internationally. It is a combination of money, information operations and cyber-attacks all being used by different actors to try to influence things. I am not sure it is a single case of a botnet or a set of information operations. Quite often I think our adversaries are using all three at different times.

Q306 **Chair:** Yes, but we are only interested in one. That is what the question has been about. What we are interested in is what happens if you have foreign interference in the British political system, where bots amplify false messages in the UK and try to divide us, particularly in the run-up to an election. Who is doing something about it?

Vijay Rangarajan: In part, this is what the defending democracy taskforce has been working on. In part, it will be the agencies actually spotting it. It will be allied to financial movements as well. We get things from suspicious activity reports coming in, because you need money, as our Moldovan colleagues set out, to do quite a lot of this. Trying to monitor the use of botnets and inauthentic behaviour in general is something we are definitely looking at. Quite often parties themselves will respond and tell us that something is going on in terms of activity.

I should say it is easier, almost, on some of the social media platforms to see because they are open, like X or TikTok or Meta/Snap/Insta. It is very hard in some of the closed WhatsApp and Facebook groups in your constituencies. That is probably the place where I don't think we can see the mis- and disinformation going on.

Q307 **Chair:** Sorry to cut across you, but let me ask the question again. It is one thing to identify the bot networks and the inauthentic behaviour. We are beginning to hear evidence that work is beginning to be done on

identifying that. We want to take the next step: once it has been identified, who is going to do anything about it?

Vijay Rangarajan: Again, I think it will depend on what it is. If it is on the electoral process, we will do something about it.

Q308 **Chair:** What would you do?

Vijay Rangarajan: Speak publicly. We had a plan in place for the general election. If there was a piece of mis- or disinformation or a botnet attack, for example, saying you do not need voter ID to turn up for the election, and it was targeted at people who might vote one way or another, we would have contradicted that. We had a plan to say what would need to be done or to go on social media or whatever was needed. If there was a particular attack on a party or a set of politicians—again, a lot of this has been very misogynistic—what would we have done about it? We would have called that out. Some of it is about directly countering it. At least during election campaigns we have a voice and would use that to counter.

Q309 **Chair:** You cannot stop it, though.

Vijay Rangarajan: We can do some of it with the takedown. We went to quite a number of the social media companies in the run-up to the '24 general election and asked them to remove some really misleading content. We had several examples where they were saying something completely incorrect about the general election. One of them, rather famously, decided that the general election had happened and said who the winner was.

Q310 **Edward Morello:** We visited your opposite number in Romania, and they took us through in great detail—probably too much detail—the process that they had established during the election to deal with predominantly TikTok accounts. Something was flagged to them, which was the first thing. It was entirely passive. What you are talking about was flagged to them. There was a two-page Word document that was taken away to assess whether that met the threshold for being a deliberate—whatever their rules were—attempt to misinform. It then went for internal sign-off within the Government structure. Then it went to be flagged with the social media company and it was then taken down.

The entire process was taking 24 hours and they were getting thousands of these on any given day. Even they were willing to admit that they were fighting a rearguard action. Most of the time, by the time they are asking for something to be flagged to be taken down, it has already disappeared and has reappeared on a different page and under a different name but with the same information.

Everything you have described to us today seems to be—with respect—a not too dissimilar process. It feels like it is never going to be fit for the speed at which social media works and misinformation and disinformation circulate, so I am wondering whether this is where resources need to be spent.

You talked a bit about digital literacy, especially for under-16-year-olds.

With the greatest respect—I say this quite a lot—I am less worried about the under-16s than I am about the over-65s. Do we need to accept that in the world in which we live, we will never have a solution that is able to keep up with malign actors and the speed at which misinformation and disinformation travel around the world? Are we better off tightening up the legal framework, which you said already has holes in it, and working on a better educated and better informed general public?

Vijay Rangarajan: I think I agree; it is about all of those at the same time. It is also about developing technological tools to try to stop material where we find it; asking parties and political actors to use, for example, the imprints regime and label material correctly; and then developing what Ciaran referred to, which is the provenance checks that are going to be needed. It is going to be all of those at the same time. But I think you are right: we will never achieve a state where there will be no mis- and disinformation or attempts made. What we are trying to do is reduce the impact of those to the absolute minimum.

I agree with what Ciaran said earlier; I don't think at the moment any of the UK elections we have seen have been significantly affected by that. However, the threat is now rising, and rising really quite sharply, so I think we have to invest now to get ahead as much as we can, both with the technology and with the legislation. We have to invest on all three limbs—the money, the information and the cyber-attacks—at the same time, because in a sense, people play all three against our democratic system.

Q311 **Chair:** Just to stop the social media attacks we are going to get if we allow that statement to go unchallenged, there is a minority of people who believe that a tight election like Brexit may have been influenced one way or the other by outside influence. I do not necessarily sign up to that, but I think that challenge needs to be put out there.

Edward Morello: I also do not want us to have to get to a point where we have a suspended election in order to decide that now is the time to start acting. This is what has happened in other countries.

Vijay Rangarajan: Can I just flag one area? Again, Ciaran mentioned it, but I just want to go into a little more detail. It is one where I do not think our legislative toolkit is sufficient at the moment, and it is algorithmic bias. What if a social media company were to preferentially and in a politically biased way amplify one set of posts and suppress another set of posts? They are a private company; they probably could do it. It would have potentially a significant effect. I do not think anything in our current legislative toolkit would enable us or anyone else—this is partly a result of old electoral legislation, which needs updating—to take any action against that, and that really is a concern. In other areas, we at least have things we can work on and, indeed, are doing, but this is one where I do not think we yet have an answer.

Q312 **Fleur Anderson:** You mentioned the Defending Democracy Taskforce, and there is the Joint Election Security and Preparedness Unit. When the

Minister was here last week to talk to us about this, he talked about the ways in which various structures across Government look at disinformation. You have talked about your remit really being around election times, and maybe it should be between those times as well, but how joined up are those systems and structures? Are there any gaps that you can make us aware of?

Vijay Rangarajan: I think they are joined up, and the working relations are really good and quite intense. It has been interesting, from discussions in Sweden and Australia in particular, to see they have set up very similar bodies. They have looked at centralised bodies in some cases. They have tended to go for co-ordination mechanisms, but with a much more rapid pace, which is what the DDTF has now evolved into, and I think they are finding them useful and enough. I was very interested in the Swedish Psychological Defence Agency—and we met them—because they are doing some work on whole-of-society resilience to mis- and disinformation campaigns, but they still have not moved away from having a large co-ordination mechanism, because mis- and disinformation touch almost everything at various points. That goes all the way from the very high-end agencies to what happens in schools. So, a tremendous variety of work needs to be done across the whole of Government and society, and at many levels in the UK, including at devolved and local levels.

I think it is more about co-ordination, and the DDTF has been very useful in doing that, which has been good. It is beginning to focus on the May elections, and on sharing some of the international examples of where things have and have not worked—a proper learning mechanism on what FCDO and others can bring from what they see internationally. That has helped us a lot.

Q313 **Chair:** In speaking to the Finns, we found that because Finland is right by Russia and has always had to accommodate Russia, the population is much more open to the suggestion of foreign interference. Part of our problem in the UK is that the public are yet to understand the extent to which there is at least attempted foreign interference in our electoral system and democracy. I quite understand why perhaps some people with some insight feel that we do not want to overstate it and undermine our democracy, but we have to balance that with the fact that our democracy might be being undermined. We have to get to the sweet spot there and make sure that the public are properly informed. I do a "bot of the week" on my Twitter account, and I just get other bots arguing with me, telling me that they are not bots. It is completely ridiculous.

Vijay Rangarajan: We very much agree. We have to flag the issues and then actually act on them. It hopefully also comes with reassurance: flag the issue, show we are acting on it and reassure people that their votes do count and are counted properly.

At the moment, we are seeing real worry about deepfakes in our public polling—around 70% of people are worried about that. Some 69% say that political mis- and disinformation is a problem, but they have high levels of trust in the actual voting process and the outcomes of the elections. That

is partly because we are still paper-based and very local—it happens in your constituency, you know the people, and the candidates are up on stage. That is much harder to attack, in many ways: when people have local support.

Q314 **Chair:** The advice we were given very strongly was not to change that.

Vijay Rangarajan: Absolutely. That would be our position.

Q315 **Phil Brickell:** Mr Rangarajan, the Elections Act 2022 introduced the requirement for a strategy and policy statement. I believe the commission is firmly against that requirement. Can you explain to the Committee why that is the case?

Vijay Rangarajan: You are absolutely right. The Government can designate a strategy and policy statement, which then goes through a parliamentary process. That can be used to guide our work. As Parliament passed the relevant legislation and set a strategy and policy statement, we have of course obeyed it, looked at it, reported to the Speaker's Committee as we need to and taken it into account. We have taken a lot of other things into account.

Fundamentally, our concern is that a Government—maybe not the previous Government or this Government, but a future Government—could use a mechanism like that to ask us to act in a politically biased way. That possibility in and of itself threatens the trust in the Electoral Commission. If we are not seen as completely politically unbiased and impartial, we have a major problem.

We have said, and our chair has said on several occasions, that we would prefer to see repeal of the provision for the strategy and policy statement. We are completely open to any forms of accountability to Parliament as a whole: to the Speaker's Committee, to Committees like yours and to anyone else. The issue is when a single party in government can ask us to do something that could have a party political implication.

Q316 **Phil Brickell:** I really want to dig into the risks around cryptocurrency donations in politics. Can you briefly outline those risks, as the Electoral Commission sees them at the moment?

Vijay Rangarajan: We are seeing the beginnings of parties being interested in taking crypto donations. That is not surprising, given the amount of growing crypto providers in parts of our economy that could in the end be quite a major part of the financial system. The issue we see is that it is very hard to know through some of the crypto providers who the ultimate donor is. As a mechanism to obfuscate where the money is coming from, crypto can be very good. It can flow from wallet to wallet, and while you know which wallet it is in, you just do not know who controls or owns that wallet in the end. We have seen, in some of our investigations, money flowing internationally through crypto exchanges and ending up in British bank accounts. Fundamentally, it is about applying exactly the same principles that we would apply to all the other things that get donated to parties, whether that is artworks, time or

printing services—you name it. I gather that crypto is defined at the moment more as an asset than a currency under HMRC and FCA rules.

We are shortly going to put out some interim crypto guidance to make some of these points. The parties need to be able to properly check that the donor from whom they receive the money is a permissible donor. We are also engaged with the crypto providers, particularly some of the ones used by the parties, to check whether they can actually give that kind of assurance. I am not yet convinced that they can, but we will work with them to see whether they will be able to. This might evolve as you get more FCA- and other UK-regulated crypto providers. It is definitely a risk, and the fundamental risk is a party accepting an impermissible donation coming in through crypto and not being able to track back to who the donor is.

There are two other areas where we are also concerned, one of which is the use of crypto in crowdfunding. You then have hundreds or thousands—or even more—of very small donations coming in via crypto, some of which may be impermissible. It is very hard to return those, so we will be advising parties not to accept crypto as part of crowdfunding.

The final part is a new threat coming into our discussions with both the crypto providers and the national security world, which is the use of AI plus crypto plus crowdfunding. You can disaggregate a large donation into a very large number of tiny donations, and then reaggregate it using AI in the UK. That would be a method of evading the controls that we have. The things that we hope are coming in the Bill, particularly on the "Know your donor" checks by parties, are really important to help manage that particular risk. We must also be sceptical and make sure that any use of crypto can obey electoral law.

Q317 **Phil Brickell:** The commission's guidance, which you mentioned, is going to come shortly. Can you say any more on timelines? In particular, are we expecting that it will be published before the local elections?

Vijay Rangarajan: Oh, yes—well before the local elections.

Q318 **Phil Brickell:** I want to ask a couple more questions on crypto. You have touched on wallets, and you have touched on ultimate beneficial information on the source of donors and whether that is permissible. Can you say what your assessment is of how far back through crypto transactions political parties would have to go to determine whether the source of the donation is permissible? If potential donations can be disaggregated into smaller items using AI, how far back might parties have to go?

Vijay Rangarajan: The parties themselves are the ultimate risk owner on this. We will give them quite a lot of guidance—we have not started writing it yet because it depends on the Bill and secondary legislation, but we will then give them some guidance.

Q319 **Chair:** Sorry; I do not understand that. Did you say that the parties themselves are the ultimate risk owners on this?

Vijay Rangarajan: Yes. They have 30 days to accept a donation. If it is impermissible, or they have reason to think it is impermissible, they need to return that donation and not accept it, and they then need to declare to us that they have returned an impermissible donation.

Q320 **Chair:** What if they just keep it?

Vijay Rangarajan; If they keep it and there is then a challenge, or we notice it—we obviously scan through the donations that they get—we will run an investigation and try to find the ultimate source of that donation. If we find that the ultimate source of the donation is impermissible, pretty well all the party officers involved have committed criminal offences.

Q321 **Chair:** Will you have sufficient resources to do that? Will you be able to guarantee to the British public that money coming through crypto will never be from foreign sources?

Vijay Rangarajan: It could be from foreign sources; at the moment, we allow money from foreign sources to come into the UK—this is part of the overall tightening up in the Bill. We can track back through crypto at the moment, and so far we have been able to. We have also expanded the number of investigators that we have, because some of this is more difficult. I think it is very hard to give an ultimate guarantee. It is about the risk, and the parties will be asked to assess the risk of any impermissible donations coming in.

Q322 **Chair:** It is a risk to not just the parties but British democracy that Russian money might end up affecting our elections.

Vijay Rangarajan: Absolutely, yes. We very much want to see a tightening of the company donation rules. Before we get on to crypto, the main money coming in at the moment from foreign sources is potentially via foreign companies. Tightening up the rules on company donations—so that only companies making sufficient profit in the UK can donate to a political party or candidate—seems to us essential. At the moment, it is just any company doing business in the UK, and that could be a small subsidiary of a very large international company or an office set up for that reason.

The second critical one is unincorporated associations, which have already been mentioned. We really need to tighten up the unincorporated associations hole. At the moment, it means that two foreign nationals can set up an unincorporated association in the UK, and it is a permissible donor—full stop. That really needs to change.

Q323 **Phil Brickell:** I agree with that sentiment, and we have exchanged correspondence to that effect previously. I want to go back to crypto. The intention is that there will be guidance that outlines to the political parties how far up the blockchain, in essence, they need to go to determine whether the source of the donation is permissible. My next question is quite a specific one. Is the commission aware of the wallet addresses that are used by the three political parties that currently accept crypto donations?

Vijay Rangarajan: We have been talking to the parties that are thinking about accepting crypto donations quite extensively, and which providers—

Q324 **Phil Brickell:** Sorry—the three that already accept crypto donations are Reform UK, the Homeland party and the Other party. Do you have the wallet addresses? Are you able to oversee those at the moment, or is that going to come in due course?

Vijay Rangarajan: No, we do not hold their wallet addresses. We are asking them, when they accept crypto, to immediately assess it and transfer it into fiat currency, so they should not be holding crypto for a long time. It comes in as a donation—it is a few thousand pounds. It is immediately assessed and sold, and then it sits in their accounts.

Q325 **Phil Brickell:** But there is a risk there, isn't there? The parties that receive donations in crypto currency have to swap them into fiat currency, as you say, but these instruments are very easy to manipulate in terms of how volatile their value can be. If parties are not able to, or do not, swap the donor cryptocurrency into fiat currency, there is a risk that that could be manipulated. If you do not have oversight of the wallet, what assurance can you provide us that you will know the true value of the cryptocurrency donation that is made?

Vijay Rangarajan: They will have to declare the cryptocurrency donation. This will be part of our guidance—actually, I think it already is. They will have to declare the cryptocurrency donation as a non-cash transaction, cash it immediately and declare the value of it. That is clearly something that their auditors can audit and we can look at as well. But you are right that the volatility means that it needs to happen immediately.

Q326 **Phil Brickell:** You talked at the start of your testimony about increasing the number of staff at the commission. When it comes to cryptocurrency, one of my concerns is around the capabilities that the commission might have. You will need somebody who understands how cryptocurrency works, and you will need somebody who has an understanding of electoral law. Those are quite specific requirements. What assurances can you provide the Committee that you are able to attract the staff with a level of expertise that means you can understand the risks as they present themselves?

Vijay Rangarajan: We have quite an expertise in electoral law already, and that will continue. We are indeed recruiting people who can track back—we already have people who can track back—through crypto. The third thing that is crucial, Mr Brickell, is incredibly close working with people at, for instance, the FCA, because they are the deep experts in the future of crypto and how things are going to evolve. That has been very helpful, because they can point out some of the future risks that I have already mentioned. We will continue to do all three of those.

Q327 **Phil Brickell:** I have a final question. On 7 October 2025, I wrote to you in my capacity as chair of the all-party parliamentary group on anti-corruption and responsible tax, on a separate issue: reports in *The Guardian* about Wafic Saïd, a Canadian citizen who is resident in Monaco

and ineligible to vote in the UK. Reports were made at the time about donations that were in the name of his wife, but those are inconsistent with Downing Street and civil service logs, which said that the then Prime Minister Boris Johnson had a "Political meeting with Wafic Said (donor)". I am yet to have a substantive response from the commission. At the time, I urged a full investigation into those irregularities, which seem on the face of it to be in breach of electoral law and to be potential foreign interference. Are you able to give me any assurance that I will hear from the commission soon?

Vijay Rangarajan: Yes, you will hear from the commission very soon. We have done a full assessment of exactly that. It has involved going to talk to the various people involved, which is why it has taken a bit of time.

Phil Brickell: Thank you.

Q328 **Edward Morello:** Yesterday, the Joint Committee on the National Security Strategy was taking evidence on crypto, foreign donations and crypto donations. It became clear through the evidence that an ecosystem is required in order to scrutinise this—you touched on some of it, such as the FCA or the potential for only using UK-registered exchanges. A skillset is required in order to do proper forensic analysis of the entirety of the blockchain and all those things.

At the risk of sounding like a massive Luddite, my takeaway was: "Should we not just ban crypto donations until such time as we are able to put the structures in place, rather than what at the moment feels like a rush to try to build something, because of political pressure from some quarters by people who want to be able to take them?" What is the view of the Electoral Commission? You are obviously being mandated to work out a framework, be it legislative or regulatory, to deal with this, but would your preference simply be just to ban it, or to put a moratorium on it for x amount of time until we are ready?

Vijay Rangarajan: We broadly agree that the system is not yet good enough to obey electoral law with the clarity and transparency that we want. That is why we are working with the parties. The reason why parties want to take crypto, and may do so increasingly in the future, if it becomes a very large part of our economy, is that London is a financial centre, and the ambitions of successive Governments have been to grow the UK as a crypto centre. To then cut off political parties from using it would also mean that it would fall outside our regulatory remit. People would trade lots of crypto, put it into fiat currency and then transfer it to the parties, whereas we would quite like to be able to look at how far down the blockchain we can go and where the money is actually coming from. Rather than ban it at the moment, I think what we would like to do is set very clear rules and guidance for parties about what is acceptable. That is very much about implementing PPERA 2000 rules on donations.

If necessary, some kind of statutory guidance might need to be produced by us, probably with other agencies, and then agreed through Parliament. That would then bind parties or candidates to accept only certain kinds of crypto. I think that as this evolves, we are likely to see a big spectrum

emerge from quite safe providers—probably more fiat and more UK-regulated ones—right the way through to the real wild-west crypto providers. We will need to be able to say to parties that some of these are legitimate, and some the parties can rely on, as a way to say that they have indeed checked far enough down, but that, in other cases, there is such a high risk that they should not use them. I think that we will probably look to do several stages now: the interim guidance and potential statutory guidance, if needed, later.

Q329 **Chair:** Again—I am another Luddite, I appreciate—I still do not understand. I listened very carefully to your answer. You gave an answer, but at the end of it you said that therefore it would be wrong to ban crypto. I am still not clear why we can't just ban it. Why can't people give money to political parties that is much easier to trace than crypto, when we know that cryptocurrency is the Russian currency of choice when trying to undermine democracies?

Vijay Rangarajan: Partly because for political parties at the moment, our financing regime allows parties and candidates to accept many things other than money: artworks, services in kind, buildings, foreign trips. There are all sorts of areas where politicians accept things, rightly, in order to do their job, and we do need a well-financed political system. We are not saying, "Take all money out of politics." There needs to be money—

Q330 **Chair:** I am not saying that; I am saying crypto.

Vijay Rangarajan: But in this case, if crypto becomes a significant part of our economy—

Q331 **Chair:** But it hasn't yet.

Vijay Rangarajan: No, but that is why we are looking ahead at the very rapid evolution of this and trying to think, "What should the rules be in order for this to be accepted?" I completely accept your point that at the moment some of it is real wild-west stuff and the tool of choice to evade financial controls, but that is why the FCA is doing such a lot of work on what a properly regulated crypto market should be. That is really our position: if it is acceptable for parties to get money from many different sources, to single out crypto as particularly more difficult than gold, cash or anything else—

Chair: I do not think that many political parties are accepting donations in gold.

Q332 **Phil Brickell:** On this point, you mentioned earlier in your testimony that you receive suspicious activity reports.

Vijay Rangarajan: Yes.

Q333 **Phil Brickell:** Presumably from the FCA.

Vijay Rangarajan: Yes. When it thinks there is something we should know about, we have been shown those.

Q334 **Phil Brickell:** So at the moment, parties are receiving crypto donations, or are able to do so. Have you received any suspicious activity reports from agencies around crypto being received by political candidates, individuals, or parties?

Vijay Rangarajan: I don't know all the SARs that we have received. I don't think there have been any specifically on crypto; they have more been where large transactions have triggered the anti-money-laundering provisions. It is a slightly open system, but it happens particularly when you have a politically exposed person involved, because that does then tend to trigger some of the anti-money-laundering provisions, and that tends to be people who are receiving donations, if they are politically exposed. The threshold becomes quite low then for those. I do not think we have had a SAR that has come in because of a large crypto transaction.

Q335 **Edward Morello:** To take a development that has happened in the US, if a politician—it would not be me because I would not know how to do it—or a political party set up a memecoin, for example, how would that sit within the existing regulatory framework? If anyone could purchase that, then am I having to look at where those purchases are being made and declare them, if it is a tradeable asset that I am profiting from? How does that work?

Vijay Rangarajan: I probably need to give some thought to how that would work in our system. My initial thought is that it would sit under the usual holding of any asset, so would be declarable. Particularly donations would be declarable for people who are buying it. The issue is—we have mentioned this already—the thresholds for transparency. If there are lots of micro-donations, they tend to fall below the thresholds for publication.

Q336 **Edward Morello:** But they might not be permissible.

Vijay Rangarajan: It could be permissible, yes. One of the issues that we have seen is that the increase in the transparency thresholds over the last couple of years has reduced actual transparency, particularly in some areas of the UK, because most donations are under those transparency thresholds. We had a massive falling off of transparency on Northern Ireland donations, for example, because the threshold went up to more than the vast majority of those donations. We do think that there is something to look at there—the actual declaration. There are some cases, and maybe those are such cases, where it is worth declaring pretty well everything in them. We are certainly, when it comes to crypto, saying, "Be very careful of crypto and micro-donations," for the reasons I gave. It is too easy for impermissible money to sneak its way into that.

Q337 **Chair:** I appreciate that I do not really know what I am talking about on this, but from what I have read, is there not a suggestion that there is a risk that AI can fracture a crypto sum of money into lots of micro-donations, which therefore makes it even more difficult to follow?

Vijay Rangarajan: Yes, the combination of AI, crypto and crowdfunding altogether is really difficult. We have to think hard on that.

Chair: Okay. We are back to a safe place with Phil, who does know what he is talking about.

Q338 **Phil Brickell:** Given that disaggregation risk, is there not an argument to say, given the Government have yet to ban cryptocurrency, given the commission is going to bring forward guidance, and given three parties have already said that they are accepting, or open to accepting, donations, that the commission might look again at the exemption of individual contributions to political parties under the value of £500 from any checks, and bring that threshold down to accommodate the risk that you can disaggregate a very large crypto donation into lots of £499 donations and face no requirement?

Vijay Rangarajan: Exactly. I think it is about aggregation and bringing down some of those thresholds. A lot of these are set out in electoral law itself; it is not in our power to shift some of those. In some of these cases, I think we are probably going to need to reduce some of the thresholds.

Chair: We have a couple of other topics. I am mindful of the time. We had some questions we wanted to ask on the Speaker's Conference report and on public trust in elections. Is the Committee happy that we have covered that sufficiently? [HON. MEMBERS: "Yes."] Are there any other questions?

Q339 **Fleur Anderson:** Can I ask one? To put together some of those things, we heard in the Moldovan evidence—we have also seen this in other countries—about the increased activity in foreign interference, potentially, and threats between elections. We have covered this a little bit, but what would it take to increase your remit to be able to look at them substantially and take more action? You have said there is going to be a short-term trial for a few months of more active work around deepfakes, leading up to the May elections, which is very welcome, but what happens after that? Does your remit need to be changed? Would that need to be done legally? Would it need to be done by Parliament? Is it resources that would stop that? What would you need to be able to increase your remit to cover the whole of the period between elections, as well as elections?

Vijay Rangarajan: To cover in between elections, particularly when it came down to campaigns or spend in between elections, that would require legislative change. That is definitely set out in primary law. There is a resource issue as well. We are trying to use the resources that we have, and they have increased thanks to the corporate plan and the three Parliaments all funding us to do this. But were we to actually get into looking at political material used and, for example, AI-generated material, that would be a big resource constraint.

I think the single biggest set of changes, which is in the Government's election strategy, is extending our remit to cover independent candidates as well. We think that is necessary because we are beginning to see the interplay between regulated parties and candidates and unregulated candidates being quite unfair.

The third area where a tremendous amount of work is needed is in cyber-defences. The commission had a cyber-attack attributed to the Chinese.

We have now recovered from that, and our cyber-defences are now really good, but our cyber-threat is enormous. We had over 60,000 attacks on election day. We quite often run at hundreds of attacks a day. At the beginning of November there were 4,422 login attempts, to try to get into our systems, and almost 2,000 phishing attempts.

We are not the only ones; all the political parties are going through this as well, as are the electoral management system suppliers and local councils. It is about investment to build the cyber-defences of our democratic system, which we would say is critical national infrastructure. That is where I would be investing quite a lot of money. The tools and techniques are all there, and we have now implemented all of them to get ourselves to Cyber Essentials Plus, which is about the highest standard. We need to, to recover from our previous attack, but I think it has to be broadened out to the whole system now.

Chair: Thank you very much for taking the time to come to speak with us, and for giving us such full answers. I think you have undertaken to write to us on a couple of issues that you were not able to give us all the details of. We look forward to hearing from you on that, and indeed, if anything else comes to you now that you have finished giving your evidence, please feel free to write to us. Again, thank you very much.