Hi there, Alistair Campbell here. Don't worry, I know this episode is titled The Rest is Money, but even though we're approaching the one-year anniversary of the disastrous Kamikwazi Trust mini-budget, this is not an emergency episode where Rory Stewart attempts to defend the economic policy of the current Tory government. Instead, this is just a quick message to let you know that Goal Hanger, the company that produced The Rest is Politics, has launched a new one, a new podcast with Robert Peston and Steph McGovern called The Rest is Money. I've known both of them for quite a long time. Steph, wonderful woman, she's now broadcaster at Channel 4, but for over a decade, she was a business correspondent for BBC News and I'm not sure how many of you know this. She started off as Robert Peston's producer at
the BBC back in the days of the financial crisis and I'm sure most of our listeners will be familiar with Robert Peston, currently ITV political editor before that, economics editor at the BBC. When I first got to know him, he was political editor of the Financial Times when I was the prime minister's official spokesman. I actually mentioned Robert in this week's main episode recounting the time I had the dubious pleasure of appearing next to Nadine Dorries on his show and I think it's fair to say that Robert, Steph, me, Rory, Darren Bent, we've all done more for the constituents of Mid-Beds than Nadine Dorries has over the last few months. Anyway, if you enjoy the broader business and economic themes that we sometimes touch upon
in The Rest is Politics, I'm pretty sure you'd enjoy The Rest is Money. It's all about following the money, charting the latest developments from the world of economics, business and finance, both home and abroad. Just search The Rest is Money wherever you get your podcasts. In our first episode, Robert and Steph discuss whether the British high street can survive, why the UK stock market has fallen from one of the biggest in the world in early 2000s to lagging behind Saudi Arabia in 2023, how cyber attackers target our critical infrastructure like air traffic control and the national grid, and why the French government is paying its farmers 200 million euro to destroy their wine surplus. Anyway, here's a quick clip from The First Ever, The Rest is Money. We're now going to look at, well, you know, an issue that's been blighting, you know, hundreds and hundreds of thousands of people, which is, you know, the collapse of air traffic control. But we're going to broaden it. We're going to look at critical infrastructure. Before we do, can I ask a question? Because whenever something like this happens, your phone normally goes wild. So come on, you'll know the truth. Was it a technical issue? Okay, so look, obviously, I've tried to sort of get to the bottom of this by talking to Spooks, ex Spooks, about whether or not this was a cyber attack. Do you have them saved in your phone as Spook? That would be telling. Now, and I have to say the consensus in that community is that this was a cock up by a traffic control rather than a cyber attack. I suppose the only thing I would say is from long and slightly painful experience is they would say that, wouldn't they? But in the end, having spoken to a lot of people about it, I think this probably was, you know, choose my words. Carefully, some would say it's incompetence and truth is air traffic control do need to reassure us that we need to get to the bottom of why this happened given the disruption. But it looks as though this was a management failure rather than attack. But one of the things that I have been thinking an enormous amount about actually broadly, since COVID is the potential for catastrophe in this country, right? COVID, the banking crisis, these were catastrophic events that we didn't protect ourselves against. Another potential

catastrophic event would be the failure of critical infrastructure. Now, the air traffic control system is critical infrastructure. It caused massive disruption to lots of people. It was bad. It'll have an economic cost as well as massive inconvenience to lots of people. But there are failures of infrastructure that can bring the country to its knees. And the question, therefore, is whether we are protecting ourselves enough against those risks?
You must have been into an air traffic control centre as well, because it's incredible when you go into these places, isn't it? And it's hard for people to picture. You know, if you think about it, there's something like two and a half million flights in UK skies every year. And what you've got when you go into these air traffic control centres are people who are basically sat intently looking at screens. So this is so computer based. And that's part of where the vulnerability is, isn't it? But I remember when I went to one of them, I was just amazed because you have to think in 3D when you sat watching the screen, which I couldn't really do. I couldn't, to me, I looked at the screen and I thought loads of planes are about to crash into each other. But this person obviously
was so well trained and intently staring at this. But, you know, I remember them saying that they have to have quite a lot of breaks because of this. They can only sit looking at that screen for so long before they have to leave. And they're encouraged to have naps of its night times and things like that. But the fact, my point being is the fact that it's so computer based means that that is a vulnerability, isn't it? All our critical infrastructure is now based on network computers. And, you know, that means if there's a bug in the system, could be an accident, that's, you know, that can cause a big problem. And if, as I say, a bad actor, well, let's go back to the WannaCry Worldwide Attack, which caused mayhem for the National Health Service in 2017. You know, huge amounts of... Reminders what happened again? So in 2017, huge amounts of the NHS's computer systems were brought down by a cyber attack. It was known as WannaCry. This was a global attack. And actually, the NHS systems were down for days until they found, you know, what's known in the trade, the kill switch. So we've had experience in this country of the damage that this can do.
Now, on the plus side, the government has become more aware of these risks. And every two or three
years, it publishes a book which goes through all the potential catastrophic risks that the country might face. This is the National Risk Register. The latest one came out just a few weeks ago after Parliament rose. Actually, it didn't, in my view, attract as much attention as it could.
Now, one of the risks that it categorizes as the most serious is what it calls the failure of the National Electricity Transmission System. And I want to read what it says about, I want to read you what it says about this. It says, a nation by loss of power would result in secondary impact across critical utilities networks, including mobile, internet, water, sewage, fuel and gas. This would cause significant and widespread disruption to public services provision. We're talking about the NHS here. Businesses and households as well as loss of life. And it also says that if the electricity transmission was brought down in the way that it fears could happen as a result of a cyber attack, the restoration of critical services may take several months.
So we are talking about a risk that is not just going to cause us inconvenience for a few days, but can actually undermine the functioning of the economy. I don't know in the end how much weight we put on these things, but it also puts a probability on the risk of this kind of, you know, collapse. And it says there is a risk of between 1 and 5%. So that's a 1 in 20 risk of this system going down. That sounds scary. And so you just have to assume, if there's a 1 in 20

risk, that they are spending whatever it takes to protect us. Because we saw in the case of the collapse of our banks in 2007, 2008, and we saw in the case of COVID, that risks that were, you know, would have been considered roughly the same, something like 1 in 20 happened.
And we weren't prepared for the banking crisis and we weren't prepared for COVID.
So we just got to hope that actually, they have put in place serious contingencies for this already.
So this to happen, we're talking about something like the national grid having a cyber attack, aren't we? Well, the national electricity transmission system is indeed, it's another way of looking at the national grid. Yeah. So to explain what that is, this is basically the company that manages the network and distribution of electricity that powers all of our homes and businesses. And it's a very complex system. You know, I think you've actually been in the game in the control room. And it can see where the power is going. If there's too much power going in one place and they haven't got enough supply, they're able to shift it from other bits of the country. It's a complex and important operation. Honestly, it looks like you're on, you know, in Mission Impossible or something like that when you go into the national grid control room. Because, I mean, when I was last there in the chief executive, you've just got this massive screen that's constantly monitoring how much we're consuming, which obviously changes at the course of the day. It shows the amount we're generating. And their job is obviously to try and balance this up. It shows the breakdown of where the power is coming from, which is obviously interesting actually in terms of where we're relying on our sources of energy. And then they predict how much we're going to use. And what's interesting, you say that point about, are they prepared for this? They've got quite a lot, the national grid put out quite a lot about what they're doing around cyber security. So for example, they've said over a 24-hour period, their cyber security teams identified 1.1 million emails, all attempting to reach the national grid email address. 0.7 of them, million, were recognised as potentially malicious and therefore blocked from entry. And obviously the rest 0.4 were deemed as safe. But that's incredible that proportion of dodgy emails essentially. You know, the other thing to bear in mind, okay, is some of these risks are the direct, when I talk about, you know, national critical infrastructure, some of these risks are directly the responsibility of the government. So the NHS will be a case in point. But quite a lot of our critical infrastructure is in the private sector, take a bank. So again, the National Risk Register looks at the risk of a cyber attack on a bank or a financial market, okay? Now, again, obviously, resilience against either a cyber attack or failure is something that any business will take seriously. And it is obviously something that the government will take seriously. But, and this is the thing where I wonder whether or not, you know, whether you're in the private sector, the public sector, you've got your priorities right. On any given day, what you're most obsessed with is, are you delivering the service as best you can to customers? You know, are you essentially, if you're in the private sector, supplying the services that are going to bring in the cash today, that are going to pay your wages, generate your bonus and all the rest of it. And there is a natural human temptation, and we see this in business, and we also see this in government, that if there is a risk of catastrophic failure, but it looks quite small, you think, oh, well, I'll spend the money on protecting us from that tomorrow, because I want to invest today in getting as many people in through the door or providing as many operations on the NHS rather than making the systems as robust
as we possibly can. We are bad culturally at making those long-term decisions, spending money

for the long term against a risk that seems remote. And we can see the failure and the costs of that, as I say, in the banking crisis, where we didn't put in place the relevant protections ahead of time. We can see the failure of that in the way that we didn't protect ourselves. This is what that great national inquiry into COVID-19 is looking at. We did not protect ourselves against the risk of a pandemic in the way that we should. And so this is the beginning of a conversation on this programme or the end of a conversation. You know, one of the things that we're going to have to look
in the course of this series is our businesses is the government spending the money now to protect us against these catastrophic risks. And I'm afraid to say, I just don't have a confident answer to that, partly because quite a lot of people who've been at the heart of government have consistently said to me that government is too focused on the short term, what's going to win them a general election, what's going to stop the public accounts committee criticising them, because one of the problems with spending a lot of money on a risk that never materialises is people then say, well, you wasted all that money. I don't know if you remember, a lot of money was spent on protecting us against a flu epidemic that never came. And people got criticised for spending that money. Well, actually, I think that was the right mindset.
But it's working out which area to spend it in as well. I talk to a lot of small businesses and for them, they haven't got the money because of all the other pressures at the moment in business. And B, they have no idea what it is they're trying to protect themselves against, because the thing we all know about these cyber criminals is they're incredibly sophisticated. It could be very hard. What do small businesses do? Do they have someone who's set aside solely to do that? And how does that person even know what's to come? And the other sort of complicated area in all of this is we know a lot of cyber criminals are in Russia. And actually, there have been cyber attacks by essentially gangs, basically planting ransomware. So for example, there have been NHS attacks this year. It looks as though these are... Hang on a minute. There have been NHS attacks this year. What are you on about? For example, there was a reported attack on computers linked to Manchester
University where they were holding a lot of data on patients, right? And this came from Russia. And the point one is making is that there is a huge amount of technical expertise in Russia. There are a lot of criminals in Russia. What we don't know is how much of this attempt to extract ransoms by Russian gangs is sanctioned by Putin, sanctioned by the state. When I talk to the intelligence
services and people in that area, they also are constantly on guard for an attack more explicitly, not by sort of freelance criminals, in a sense, underwritten by Putin, but more directly by the cyber arm of the Russian intelligence service. And in fact, truthfully, there is some surprise, we haven't seen more from Russia in that sense, trying to basically bring down our infrastructure. But the fact that we haven't seen it yet doesn't mean that we're not at risk. It is something we have to be wary about. Do you reckon the Russians are using the data they managed to get about us to from this BBC hacking incident that we've both had letters about? Well, yes. I mean, so one of the other, you know, attempts to extract money effectively blackmail was this, again, worldwide attack on a number of big institutions. One of the institutions that was attacked was the BBC. I haven't worked at the BBC since the end of 2015. So quite a long time now, they managed still to extract quite a lot of my personal data. Yeah, and me as well. You've got the same email and letters from the BBC. I was with Angela Rippon when she got her letter too.

So if you enjoyed that, you want to hear the first episode in its entirety, just search The Rest Is Money wherever you get your podcasts and click subscribe. Make sure that before you do so, you listen to the latest Rest Is Politics and even more important, make sure you tune in to Leading on Monday, where Rory and I sit down with the Liberal Democrat Party leader, Ed David. It's a really good episode, not one to miss. Have a lovely weekend. Bye-bye.