HOUSE OF COMMONS

Business and Trade Sub-Committee

Oral evidence: UK economic security, HC 835

Tuesday 8 July 2025

Ordered by the House of Commons to be published on 8 July 2025.

Watch the meeting

Members present: Liam Byrne (Chair); Antonia Bance; John Cooper; Sarah Edwards; Alison Griffiths; Sonia Kumar; Charlie Maynard; Gregor Poynton; Mr Joshua Reynolds; Matt Western.

Questions 214-234

Witnesses

III: Jamie MacColl, Senior Research Fellow, RUSI, Professor Ciaran Martin, Blavatnik School of Government and Katharina Sommer, Group Head of Government Affairs and Analyst Relations, NCC Group.

Examination of witnesses

Witnesses: Professor Ciaran Martin, Jamie MacColl and Katharina Sommer.

Chair: Welcome to the third panel of this hearing of the Sub-Committee on Economic Security, which is reviewing cyber-security policy in our country. I thank our witnesses very much for joining us this morning.

Q214 **Sarah Edwards:** Thank you for coming. Professor Martin, you have described the "transformation of China's digital attack capabilities" as "the most important change" for western cyber-security in more than a decade. What are the policy implications of this change, and can you describe what you think we need to know?

Professor Martin: Thanks for the invitation. I think that there is one point of history and one of consequence.

The point of history is that, while we in the UK and the wider west have been complaining about Chinese cyber-operations for 25 years, they have all been about data exfiltration. They have just been stealing governmental and commercial information. Those are silent: the organisation goes on to function perfectly normally, so that is strategic damage.

If you have a discussion—I have been in this position, as have others—with a Chinese Government interlocutor and complain, one thing they will say is, "We have never launched a destructive cyber-attack of the type that Marks & Spencer suffered." That is historically true. What has emerged over the last few years, uncovered by the Americans but backed by our Government and the other Five Eyes partners, is a plan and operation code-named Volt Typhoon. The name does not really matter; it is one of the silly names that the cyber-security industry gives those operations.

These operations are essentially what some have called digital booby-traps in critical infrastructure. If you think back to the operations you heard about this morning, particularly M&S—the Co-op was different, as you heard; as Mr Cooper put it, it amputated its leg—it is dozens or hundreds of those happening at the same time. That would be extremely uncomfortable nationally. The then head of the US cyber-security agency CISA, Jen Easterly, used the phrase "everything, everywhere, all at once".

I am sorry for what may arguably be a distasteful analogy, but if you think back to the peak of international terrorism earlier in this century, at one point, the likes of al-Qaeda became obsessed with very sophisticated and difficult operations such as 9/11. That, to some extent, saved us from further harm, because they are quite difficult to do. Then they started doing simpler but devastating operations such as the one that we commemorated yesterday or the one in Madrid.

In cyber, it is kind of the same thing. The Russian operations against Ukraine over the years have been very sophisticated. It takes a year and a half or sometimes two or three years to do a bit of limited destruction to a

power grid. It is possible, but very hard to do. Then you look at the sort of thing that happened to Marks & Spencer, which happens to organisations all the time. The criminals have given nation states a playbook, and that is what Volt Typhoon is. That is the history and context.

There are all sorts of policy implications, but I am conscious of time, so I will focus on one. I heard the chairman of M&S say that you cannot always regulate your way out of this, but I think sometimes public policy has a role, and we are not starting from scratch.

I would argue, speaking only for myself, that we already have a body of law that incentivises every organisation—literally every one—to prioritise the protection of personal data from theft. That is the way our law currently stands. It does not incentivise them to prevent the disruption of critical services.

For critical infrastructure, there is a lot pending from the Government, and that is welcome. However, even in general, it is fiendishly hard to work out which companies are critical and which are not, and which bits of companies are critical and which are not.

The classic case of this is the Irish healthcare system in 2021. The entire national healthcare system collapsed, in terms of scheduling appointments for vital healthcare, but there was no regulatory breach by the public authority in charge. Four days later, the criminals behind the attack released some medical data, and that was a breach of the law. That is crazy, but that is roughly where British law is in a lot of places right now.

The incentives are all wrong, if we are serious about economic security. I am not downplaying the importance of data security, but we have prioritised it at the expense of continuity of service. I believe that hat is wrong.

Sarah Edwards: That is really helpful.

Chair: Yes, that is an extremely helpful conclusion. Sarah, do follow on—I will have some questions on that line too.

Q215 **Sarah Edwards:** When we are talking about the classification of what is critical, and given what we have just heard from two food retailers, at what point do you think the Government and the security agencies need to see that as a critical infrastructure attack? We had two, and then a delivery organisation was affected as well. How should we quantify that?

Q216 ***Professor Martin:*** I think it is really hard, which is one reason why I think a law that just says that something is critical will be hard. In some areas it is really obvious: in telecoms, there are one or two organisations that are household names. It is probably not fair to name them, but it is pretty obvious who I am talking about. If they go down, we are in deep trouble.

Food is really interesting. We had this during covid; at the start of covid I was still in Government, and all the various agency heads, who were in

charge of various bits of protection, looked at what is critical. Food self-defines as a critical sector, but there is not a single company in the sector that is critical on its own. Food is an example of where it is a very hard thing to do, which is why I do not think that there is some straightforward public policy answer that you can write a White Paper or memorandum about.

It is about some of things that you heard from the previous two panels, about co-operation within the sector and having dynamic exchange with Government, so that you know it when you see it. I do not think that you can say that if the attack had gone from Marks & Spencer to the Co-op and then on to Tesco, Sainsbury's or Lidl, it would have been a critical incident. I am not sure that there will ever be that point, because it depends on what it is. We need to be able to have that dynamic process by which we know it when we see it.

Q217 **Chair:** That is very helpful. You have flagged some of the evolving threats, such as Volt Typhoon from China. What are the other multiplying threats that the country faces in the cyber domain?

Professor Martin: I will highlight three quickly. You have heard about one all morning, which is the enduring criminal threat. I think a specific aspect of that is geography. From what we know in the public domain, the Marks & Spencer and Co-op attacks were potentially done by arrestable, English-speaking criminals. That is actually unusual: if you ask people currently in office, they will say that it is still the minority.

We have the structural problem that about three quarters of the known ransomware comes from Russia, or near Russia, and areas with which we do not have law enforcement co-operation. The traditional approach of sending the police after some people and hoping that you arrest them, even in an international environment, does not work. The police have to think more imaginatively and do disruptions. That is the first thing. It sounds depressing, but there is not a great deal that you can do about the source of that. You can do some really important tactical interventions, and the NCA has been brilliant at that, but that is an enduring problem that means you have to defend.

Secondly, the Russian state and a few others, such as the Iranian state, remain capable. They show restraint—I know that may not be a popular thing to say, but that is what the evidence reveals. Russia did not turn its considerable firepower on the west when it invaded Ukraine, to any great extent; there were some serious incidents in Poland and other places, but we would have been talking about it had that happened to Britain in the last three years.

If you are looking at longer-term public policy, one of the things that has kept us in an uneasy equilibrium in the cyber space—in other words, there has been lots of harm, but we have never been here to discuss an absolute catastrophe of national or global proportion in the cyber space—is the fact that to do something really devastating, you have to be quite good and/or extremely reckless. The small number of powers with the elite

capability are never both of those things at the same time, however much we may dislike some of their Governments.

With the rise of AI-enabled cyber-tools, the cost of being more than a nuisance—a lot of this is nuisance value—and a strategic threat goes down, so more people can do it. You think about the motives and modus operandi of some those groups, and you then think about them with more powerful cyber-tools. Those would be the things that I would worry about.

Katharina Sommer: Can I come in on that point?

Chair: Yes, please—help us to fill out the picture of the threats that we should be foreseeing in the next five to 10 years.

Katharina Sommer: I would add the context of everything being connected these days, and everything relying to an extent on digital technology. As we have heard, that has just broadened the attack surface massively, so there are targets everywhere nowadays. One of the resilient solutions is to go back to pen and paper, which obviously comes with productivity and efficiency implications.

Another thing that we are seeing at NCC Group, and that our threat intelligence team is pointing to, is the convergence of threat actor groups, such as nation states working with cyber-criminal groups, hacktivists being co-opted by criminals and the ecosystem of adversaries coming together to our detriment.

The third aspect, which Ciaran alluded to, is the greater availability of capabilities and tooling, particularly the proliferation of commercial cyber-intrusion capabilities. Whereas before it took an adversary days and months on end to develop offensive capabilities, they are now available to purchase off the shelf—some on the legitimate market and some on the dark or grey market. That is a real threat, which is partially why the UK Government has instigated that.

Q218 **Chair:** Just to help us visualise this, Marks & Spencer has just lost about three times the value of the Brink's-Mat robbery: £300 million. How many people would you guess were involved in an attack like that? Is it one, is it 10? Is it 100?

Katharina Sommer: That is an excellent question. I would not want to speculate, but maybe my colleagues would.

Jamie MacColl: I can try to answer. We know from the public record about the retail attacks that it is split into two parts of the criminal supply chain. There is this amorphous group, Scattered Spider, which people believe is mostly young English-speaking criminals in the west. It reportedly gained access to the retail victims, but then used off-the-shelf services from Russian cyber-criminals to deploy the ransomware. We are probably talking about a few individuals as part of the initial access phase, and then there is probably a larger criminal enterprise supporting the actual ransomware.

Q219 **Chair:** Is that dozens of people, hundreds of people or an unknowable number?

Jamie MacColl: It depends on the group. We know quite a lot about some of these Russian ransomware groups because of leaks of internal chat data. One such group, Conti, was very professionalised. There were dozens or even hundreds of people involved in that, with people having professionalised roles and skillsets within the organisation. We call them employees because it was run like a business. In other cases, we may be talking about single-digit numbers.

Q220 **Chair:** Would you add anything to the picture that Ciaran and Katharina set out of the threats that we face?

Jamie MacColl: I would add that on the criminal front, we can get quite caught up in thinking about AI-enabled cyber-crime and how things will change in future. A lot of the criminal tactics we have talked about today have not changed over the last four to five years. They have not had to, because it remains highly lucrative. Our response has not sufficiently changed to force them to change their tactics.

Q221 **Matt Western:** Ciaran, it has now been 10 years since the NCSC was first proposed. It came into being two years later. Is it realising what you imagined, or do you have any frustrations about its reach or how it is regarded by the public sector, Government and wider society?

Professor Martin: It probably had four broad aims when it was set up. The first was to lead and grip national incidents. Just before it was set up, we had TalkTalk, which was the first British cyber-incident to lead the news. The Government machine was absent from that. The second aim was protection of critical infrastructure. The third was giving one-to-many advice to those who would not otherwise be able to get cyber-security advice, such as charities, schools and small organisations. The fourth was to try and fix things that the commercial market would not fix, such as protections for small organisations and small public authorities.

I think you can always do better. Some of the highlights have included the handling of major incidents. I recall the head of Redcar and Cleveland council, which was involved in one of the most serious cyber-attacks in the history of this country, because vulnerable children's services were at risk, giving evidence to a Joint Committee and saying that the NCSC, which had deployed a team who slept in the office until it was done, was the most helpful bit of Government.

There have been other things. For example, there is another typhoon called Salt Typhoon, which is a major Chinese spying attack on the US. In the US, there are zero commercial incentives to thwart such an attack on telecoms companies. America suffered a huge strategic spying breach, but that does not cost the companies anything. Because it was spying, they did not suffer any loss of service or anything like that, so they have no incentive to do anything about it. Because of the partnership that the NCSC built with the British telecoms industry, Parliament passed the Product Security and Telecommunications Infrastructure Act 2022, which

said "Look, if you want us to make these improvements to stop this sort of thing happening, build into the regulatory model." That is a good example of partnership.

As for the frustrations, you will never have the capacity to grip as many incidents as you want. We heard a little bit about that this morning. I am not sure that I would go as far as Australia has gone, in terms of law, but I will give you the example for comparison purposes. The UK system is quite collaborative, by and large, but in the event of a major incident—to use your phrase, Chairman, about public risk in private hands—it is essentially co-operative. Alive to that danger, Australia has introduced what they call a power of consequence management: in other words, the Government can declare that if something is going badly wrong, but the primary levers of it are in private hands, they can essentially take over that aspect of it in the public interest. I do not think that we need to go that far in the UK, because it is generally co-operative, but there can be a messiness about the public-private interaction. Where does the corporate interest stop and the public interest begin? We need to manage that very carefully.

One thing that we need to keep momentum on—this is not just a UK point, in terms of the NCSC; the transition of Administration in the US makes this harder—is about the fundamental problems with the top of the tech stack. What I mean by that is that there are breaches and incidents you will hear about that are Microsoft's fault—there are well-known examples; I am not just picking on them—or the telecoms company's fault or the big data-moving company's fault, and they have no liability at all. You can suffer things because of your upward provider, and that is not covered by any laws anywhere. The previous US Administration was interested in tackling that; the current Administration is not.

We have heard the point all morning about legacy tech and legacy systems, unaccountable software providers and so forth. If we want to make strategic breakthroughs, we and like-minded authorities have to try to make a dent in that, but that will be hard.

Like any picture, it is mixed. I think there is plenty that the NCSC—including in the long period since I have gone—can be proud of, but things are changing, and we really need to grip that strategic tech security picture.

Q222 **Matt Western:** On your point about the tech stack and what is happening in the US, is the EU doing more interesting stuff in that area now?

Professor Martin: It is, and it is early days. So far, unlike other bits of legislation that are controversial in EU-US terms, like the Digital Markets Act, American big tech is not screaming about it.

The legislation is called the Cyber Resilience Act, which is an odd name because it makes you think about recovery from attacks and so on, but it has nothing to do with that. The Cyber Resilience Act is essentially a transfer-of-liability Act, so if the big American tech providers sell faulty products into the European market, they will be held liable for them. It has

only just come into force in its most basic, narrow function, so it is too early to tell, but it does not seem to be at the top of the list of the US complaints about extraterritorial regulation of EU tech. When you talk to EU officials and some of the US tech giants about this, they say, "We think that in 10 years' time we will be here anyway, so we might as well make this work, because it is clearly sensible."

It is a difficult technical challenge. There was a big thing, which Katharina mentioned, around how everything is interconnected. With IoT—internet of things—stuff, it is hardware, so it can be easier to do product regulation. If you talk to Microsoft, they say, "How will you provide an incentive and penalty regime for 90 billion lines of code? Will you find an error in line 54 billion and say 'Right, you're fined'?" It will be hard to do this, but it is one of the critical areas. It is not just about the EU; obviously there are sensitivities here in that area, but Singapore, Australia and Canada are all interested in this stuff too. There is an opportunity to work on what is known in the trade as "secure by design" and try to make progress in this area.

Katharina Sommer: It is probably worth mentioning that DSIT in the UK published its software security code of practice a couple of months ago, which goes into the territory of incentivising—through a voluntary code, at this point—software developers and procurers of software to pay attention to secure-by-design features in their software.

Jamie MacColl: There is a lot of work going on in the NCSC and DSIT, but it is all voluntary on this issue at the moment.

Q223 **Matt Western:** This is a question for you, Katharina and Jamie. As external, independent observers of NCSC, what is your take on the impact it is having across society, business and the public sector?

Katharina Sommer: NCC Group has been a private sector partner to the NCSC from the outset. The way in which public-private collaboration was built into the design of the NCSC—through the Industry 100 initiative, in particular—is pretty remarkable from where I am sitting. It is something that international delegations come to the UK to learn more about—how the NCSC in particular has managed to create a shared sense of mission with the private sector, and an environment in which private sector participants are true partners, not just providers or solution-offerers, in the endeavour of cyber-resilience. That is something to be proud of. It wasn't on the list of objectives that Ciaran mentioned, at the outset, but it is a very happy by-product of the work of the NCSC.

Jamie MacColl: The NCSC is admirable in a lot of ways, and it is probably still world-leading among national technical authorities and national cyber-security centres. Particularly in terms of working on technical challenges that don't have obvious commercial implications for cyber-security, there are very positive examples in which the NCSC has led and has been ahead of industry. One current example of that is preparing for post-quantum cryptography. There have also been a lot of success stories in relation to being measured about potential cyber-threats. I consider the experience

with Huawei and 5G in 2019 to be a good example of that. I know Ciaran probably doesn't want to relive that experience, but the technical assurance that went into that work, and the way it was conveyed to the public and to industry, were very positive.

In terms of potential challenges and downsides, if you look at statements from NCSC leadership and annual reports over the past couple of years, there seems to be a lot of frustration that the guidance and advice they are putting out is not cutting through or being taken up. Generally, awareness of the NCSC among the majority of UK businesses is still very low.

Q224 **Matt Western:** What is your estimate of small businesses' awareness?

Katharina Sommer: I have a stat on that. In the DSIT cyber-security breaches survey 2025, when respondents were asked for their sources of information, 1% of businesses and 2% of charities mentioned the NCSC by name. Awareness of its campaigns is higher, but by name, it is pretty low. That was reflected in the earlier evidence sessions. Within the cyber-community, the NCSC is very well known and incredibly well respected, and there is a community around it, but awareness in the broader realms of society is still relatively limited. There is a role for private sector partners in acting as ambassadors, multipliers and amplifiers, and that is probably currently untapped.

Q225 **Charlie Maynard:** I am one of those people to whom the NCSC is new, so that is helpful. I am getting warm and fuzzy feelings, but in terms of risks and concerns, you have mentioned quite a few and they have been very interesting and useful. What have you not mentioned about where we are going in the future and what we need to be thinking about?

Jamie MacColl: One question that concerns me at the moment, to go back to Ciaran's opening example of Volt Typhoon, is: how is the British state preparing for a crisis or conflict scenario with another state, and what regulatory mechanisms is it creating to give us much more direct control of parts of the cyber-security of critical national infrastructure in a conflict scenario? I am concerned that that work is not happening at the moment, particularly given how much of not just CNI but the cyber-security services and capacities that we have in the UK is privatised.

Q226 **Charlie Maynard:** What is your take on the Australian example and the pros and cons of that?

Jamie MacColl: I have not looked at it in enough detail but reflexively I think it is a good idea.

Katharina Sommer: From what we understand, the forthcoming Cyber Security and Resilience bill will include a power to intervene of some description. Detail is lacking, but I will be very interested to see what that entails and whether it goes some way to address the Australian example that Ciaran mentioned.

In terms of broader concerns, I do not think we have an overarching view of the collective capability that is available to the UK at the moment and

that looks at what is available via agencies like the NCSC, the NCA or intelligence services from the private sector. No one has done the stocktaking exercise as it were and looked at collective capability and how that measures up to what we are likely to see from adversaries.

Professor Martin: There are a couple of things that are worth watching out for. One is what I would call random malicious accidents. What I am referring to there are less responsible attackers unleashing something that is badly coded, which then goes out globally and it is not targeting anybody. We had two of those in 2017: the so-called WannaCry virus, which affected the NHS, and NotPetya, which affected all sorts, including WPP advertising and the law firm DLA Piper, but globally it took out Maersk, the shipping company and so forth. That is one of the risks with cyber: you can analyse threats and so forth, but some of the most important incidents we have had to deal with, to Jamie's point about readiness, have just been malicious accidents. In other words, they were targeting somebody else, but they ended up targeting everybody.

Given that I suppose we are the segue between the recent victims and the serving Government officials. The point that has come up a couple of times today about insurance is really vexed but is potentially interesting for future opportunities. It speaks to the wider problem that a lot of the technology is there for cyber defence, but a lot of the problems are economic, social and quasi-regulatory, commercial incentives and all that sort of stuff.

In 2014, before the NCSC was set up—that dates it—I recall Francis Maude, then Minister for cyber-security, hosting a summit of insurers at Marsh on the other side of town and saying that Britain is very good at cyber-security technically and really good at financial services, including insurance, and that we should be able to put the two together to give us a big shield. For reasons that are nobody's fault—nobody has acted malevolently—it has certainly not achieved its potential.

I know I did not mention it as one of the four priorities, but this speaks to Kat's point about informality. There is strength in the informality about the British system. In the US, everybody is litigating everything, and if you want to do any co-operation between the Government and a company or between companies, they want some legal guarantee. In the UK, people rarely seek that, and it kind of works.

Building on that, I will give you a specific example in insurance. About four years ago, the insurance industry went down globally as a result of the NotPetya attack. It went down this complete rabbit hole about what was an act of war in cyber-space, even though it was pre-invasion of Ukraine in terms of where the phrase "act of war" comes from in insurance history; we did not have any of that. When it came out, it was written in a language that neither the Government nor the cyber-security industry understood. There was no reason for that.

Given that the UK is actually quite collaborative in cyber-defence attitudinally, you should be getting together the insurers, the experts, the

academics, the Government people, the cyber-security industry and the big corporate victims and saying, "Look, here's what the last 10 years of revealed history have shown us. This is what nation states do. Here are the incredibly murky and incomprehensible grey areas between nation states and criminals hosted by those nation states. How are we going to get a workable insurance model out of this?" We have not quite had that conversation. If you are interested in public-private collaboration in the interests of UK economic security, that is a really strong area of potential, if we get it right.

Q227 **Chair:** As a quick side point, the recently published national security strategy talks about how quickly the country may need to move from co-operation to competition to crisis. The National Cyber Security Centre was a novel institution that brought together the public and the private sector around the cyber domain. Do you think it is a potentially useful model for thinking about economic security more broadly?

Professor Martin: If you adapt for different incentives and sectors, yes. At the risk of making myself sound ridiculous, my early Government career was in the Treasury, where there is almost an attitude that the private sector is amoral and exists to generate revenue for the Government to spend. If you work in something like cyber-security, you realise that, of course, major corporations—the people you have spoken to this morning, particularly M&S, as a listed company—have to make money and make returns, but if you approach them sensibly on issues of national security, they instinctively want to be in the right place and to do the right thing, and they will give you the co-operation that you need. Sometimes, we overcomplicate that dialogue. I think I overcomplicated it in my early days in office, because there is, again, the question of where public risk starts and private risk ends. There is always going to be a big overlap. You can sit around writing a memorandum about that, or you can actually go and do stuff.

Cyber is quite a technical subject. It was seen as quite important but not widely understood, and it wasn't a political fault line. We had quite a lot of space to engage with big business. To their enormous credit, they did not seek legal protection for doing it. We said, "Look, if this gets lawyerly, we'll have to call it off, because we can't do it." I do think that there was a very strong attitude, interestingly, for a country where a lot of chief executives are not British nationals, that that did not really matter. If you went to a big corporate that was chaired by someone or had a CEO who was not a British national, they still often wanted to do the right thing. Obviously, you had to exercise prudence in what you shared with them. But yes, I do think there is a model that can be replicated, subject to adaptations, for other sectors.

Q228 **Matt Western:** On the point about how businesses interface with the NCSC, how good are they at using the cyber threat intelligence and assessment in making decisions, and how effective is the NCSC in informing that process?

Katharina Sommer: It sounds like an easy question, but it is quite complex, because it depends on the maturity of the receiving organisation and what it can and cannot do with it. Depending on that level of maturity, different kinds of hand-holding mechanisms are needed.

Relatively mature organisations will receive a threat assessment from the NCSC. They might have in-house threat intelligence teams who can go through the intelligence cycle and enact whatever needs to be done on the basis of the actionable intelligence they received. Smaller or less mature organisations will struggle with that.

Ciaran pointed to the lack of resource or capacity on the NCSC side. That is still a struggle, because the information is being put out there into the ether for something meaningful to be done with it, yet a lot of receiving organisations see it and think, "This seems really important, but what exactly is it that you'd like me to do?" It goes back to there being a role for more mature private sector partners, whether they come from the cyber industry or from big businesses, to be the bridge between what the NCSC is doing and saying, "Here's what you need to do. We'll do that translation layer and make that intelligence actionable for a less mature organisation."

Professor Martin: I will try not to overcomplicate this. There are some brilliant examples. There was one in 2018—a while ago now, in my time—where a North Korean group well known for being the most accomplished monetary cash thieves in global cyber, the so-called Lazarus Group, had a go at the City of London. The NCSC detected anomalous activity on the SWIFT system and spread it out to the banks, and 54 banks that were under attack blocked all of it. But, to Katharina's point, that was 54 of the wealthiest institutions in this country with the strongest capabilities.

Again, a lot of this comes back to economic, social and commercial incentives. What you can't do—we used to do this and to some extent we still do; not just us but other states as well—is to take medium and small businesses and expect them to be able to do something that a Government or a very large corporation is able to do. That is not fair. While in one respect the statistic about 2% of small businesses or charities or whatever knowing about some of this stuff might sound depressing, there is a part about realistic expectations.

In terms of really important sectors, finance and telecoms are mature and strong relationships; energy, certainly in my time, was not—I do not know if it has changed—and nor was water. There were other critical sectors that were much less mature. When you get further down into smaller organisations, you have to look for different solutions.

It is striking that, even in the United States, nobody has made money—serious money—selling cyber-security to small businesses. It baffles venture capitalists and so forth. We have been at this for so long. You can ask the same question over and over again. Maybe we should look for a different question and a different answer, and that is, just make the stuff

they use a bit more secure and help them out when they are in serious trouble.

There was an example in my time. There was a small documentary maker, which has since been bought by ITV so is part of a large company, but back then it was 25 people in Northern Ireland. They were making a documentary about the North Korean Government. They attracted the attention of the same people who in 2014 famously took out Sony Pictures because they didn't like the move "The Interview". I don't think there is any public policy framework you can construct that can easily protect a documentary-making company of 25 people from the North Koreans. You just hope and expect that those cases are relatively rare and you send the Government in directly to help them, and you make the tech they use as good as possible, so the North Koreans have to work a bit harder.

It is different solutions for different bits of the market. We need to get better at the top end, bringing everybody to the level of finance and telecoms, but as you go further down the economic pyramid—

Q229 **Matt Western:** We heard from Marks & Spencer and the Co-op. Were you surprised or reassured by what you heard about their experiences?

Professor Martin: I am very sympathetic to what they experienced. They didn't go into details, so Jamie and I are just going on what has been reported. One key entry point for M&S is that, unusually, fluent, unaccented—they did not sound foreign or second-language speakers—native English speakers deceived the helpdesk. That is arguably, preventable, but you can all understand the sort of tensions and trade-offs in how that happens. Then, once they were in, it appears that the techniques used were very sophisticated, because they were looking like a normal user. It is sometimes called living off the land—you look absolutely normal. That can be very hard to detect.

I am not critical about the recovery time; it is perfectly normal to take that length of time. But I am worried—this comes back to the point in the exchange right at the very start—about what it says about national vulnerability. M&S can and have looked after themselves; they have made their announcements, they are still trading well and so forth. But the criminals have given us a playbook here: you can disrupt an iconic British brand with some effort, but effort that is comfortably within the easy reach of adversaries. What is also in easy reach of state adversaries is to do this on multiple occasions at the same time. That is the worry.

Jamie MacColl: On the threat intelligence aspect, I would not underestimate the extent to which the state and NCSC are dependent on the private sector for a lot of the threat intelligence that it consumes. Obviously, NCSC benefits enormously from GCHQ's signals intelligence collection and, I guess, more forward-facing cyber-operations that the UK conducts. But in terms of the intelligence generated from incidents, which is a lot of the threat intelligence that the private sector produces, we are very dependent on large US cyber-security vendors to generate that.

Chair: John, do you want to nail the insurance question? I think we have covered a bit of it.

Q230 **John Cooper:** Yes. Professor, you talked about insurance and made quite a powerful argument for convening Government, private industry and insurers, and drawing them together as we face this threat. Jamie, in 2023 the Joint Committee on the National Security Strategy used evidence from RUSI to warn that there was a difficulty in the insurance market, with "demand outstripping capacity and insurers raising premiums and setting tougher conditions for coverage". I presume that that situation is only going to worsen, with big claims coming through, as we have heard. Where are we with that, and what are your thoughts on the idea of convening some sort of pow-wow about the insurance situation?

Jamie MacColl: I did a lot of research on cyber insurance from 2020 to 2023, and I think that market conditions have changed since we gave that evidence. My understanding is that the market has softened again, so that some of those market conditions have essentially reversed. That means that it is easier to obtain cyber insurance. But it is interesting that a company the size of Marks & Spencer could only—based on media reporting—obtain coverage that covered a portion of its losses, because the market is still not offering very significant coverage.

Conditions have improved in terms of being able to obtain coverage. The downside of that is that, if the market is softening, insurers will perhaps not be asking for security controls across all market segments, so they will not necessarily be driving up security standards in the way that we would hope insurance might.

Q231 **Chair:** So there might be some market failure that requires a bit of state intervention.

Jamie MacColl: I am not sure I would go so far as to say that it is market failure; it is just how a private market reacts to market conditions. When the market experiences losses, it will need to ask for more controls to reduce losses. When the conditions are opposite, it does not. The insurance market is not going to be a silver bullet in solving cyber-security, which is how a lot of people have historically treated it.

Q232 **John Cooper:** Do you think the market itself is in a reasonable shape, and that there is no need for the Government to intervene to put money in? I am thinking of things like when the Government stepped in and provided cover for private buildings when the IRA had a bombing campaign here in the UK. Even if you do not think that we are at that point yet, do you think that there is a way of the Government using insurance companies to incentivise better controls and systems to protect against this kind of thing?

Jamie MacColl: On the first question, I do not think that market conditions are at the point where we need a Government backstop in the way that we did with Pool Re. I do not think we are experiencing a market failure where organisations cannot obtain cyber insurance in the way that they could not for terrorism and property damage. There is still room for

the market to grow organically, and I do not think that we need that kind of intervention. Ciaran may disagree.

Professor Martin: I am not sure whether I would go so far as to say that it is a market failure, but maybe I am being overly semantic. I certainly would not say that it is market that is fully working in the public interest. We are not in backstop territory, but—this comes back to having, as a first step, a proper, serious cross-sectoral dialogue—I think there are a number of problems. I mentioned an example about how nation states insure threats that still rumble on.

Going back to data harm versus disruptive harm, Marks & Spencer has been very clear about how much disruption cost it, but when you are insuring for data losses, what are you measuring? We have struggled with that. Jamie may disagree—we will have to cauterise this debate at some point—but my impression, having talked to a lot of customers and insurers, is that when things go wrong and insurers look for more, some of the things can be a bit compliance-heavy: "Have you done this risk assessment, and that one?" That actually under-incentivises.

There are some good technical tools that companies can use. Take the M&S example of living off the land and looking like a normal user. There are some very powerful internal tools that people are now adopting that say, "Okay, hang on. That looks like a normal user, but it is a little bit weird what they are doing at two o'clock in the morning." How do you incentivise having some of that good stuff? I do not think you have to reach straight for the terrorism-style Government backstop yet, but I still think there is scope for technocratic improvements in the current system. That is unusual for the UK, because, as others have been kind enough to say, under the NCSE's leadership, in lots of other areas of cyber-security there is a strong partnership environment, where you can convene and make improvements. I have not quite seen it completely work in insurance yet.

Chair: We are almost out of time, but I will hand over to Charlie Maynard.

Q233 **Charlie Maynard:** Following up on Jamie's comment about it being dependent on what the private sector tells the NCSE, or whoever it may be, people were talking earlier about mandatory reporting. I want your take on whether you think that should be regulated so that private companies have to report if there have been breaches.

Jamie MacColl: The Government just ran a consultation on ransomware specifically, and one of the proposals is that UK organisations would have to report a ransomware incident. There are still questions to be worked out around what the threshold would be. Personally, I would expand that to all malicious cyber-security incidents; I do not understand the logic of just applying that to ransomware. The fact that we can have a publicly listed company in the room today, and we cannot get a clear answer out of them about whether they paid a ransom or not is a bit telling of the current reporting environment that we are existing in.

Chair: Well spotted.

Q234 **Charlie Maynard:** Any other points of view on that?

Professor Martin: I think it is one of those rare instances of public policy that has very little downside to it. Sorry to keep mentioning Australia, but I worked for free helping the Australian Government two years ago with their strategy. They have just introduced it, and it has been in place for two months, and the sky has not fallen in. The capabilities of the NCSE and the NCA are national assets, and anything we can do to strengthen them helps. It is not just about the situation that Jamie talked about, but about having a richer dataset where you get towards those hidden events—that will help strengthen them at very little cost. It is not a huge bureaucratic burden on the affected entities, so I do not see the case against it.

Chair: Most accidents have to be reported. We are out of time. Thank you so much to this panel for a brilliant set of evidence, which was illuminated and alarming at the same time.