HOUSE OF COMMONS

Science, Innovation and Technology Committee

Oral evidence: Cyber resilience of the UK's critical national infrastructure, HC 559

Wednesday 21 February 2024

Ordered by the House of Commons to be published on 21 February 2024.

Watch the meeting

Members present: Greg Clark (Chair); Dawn Butler; Tracey Crouch; Dr James Davies; Katherine Fletcher; Rebecca Long Bailey; Stephen Metcalfe; Carol Monaghan; Graham Stringer.

Questions 1 - 56

Witnesses

I: Professor Ciaran Martin CB, Professor of Practice in the Management of Public Organisations, Blavatnik School of Government, University of Oxford; Professor Sadie Creese, Professor of Cyber Security, University of Oxford.

II: Siân John MBE, Chief Technology Officer, NCC Group; Professor Awais Rashid, Professor of Cyber Security, University of Bristol.

Examination of witnesses

Witnesses: Professor Martin and Professor Creese.

Q1 **Chair:** The Science, Innovation and Technology Committee today starts its oral hearings on a new inquiry into the cyber-resilience of the UK's critical national infrastructure.

I am delighted that giving evidence first we have with us here in Westminster Professor Ciaran Martin, Professor of Practice in the Management of Public Organisations at the Blavatnik School of Government, University of Oxford. He was the founding chief executive of the National Cyber Security Centre, which was and is part of GCHQ.

Joining us virtually is Professor Sadie Creese, Professor of Cyber Security, University of Oxford. She is founding director of the Global Cyber Security Capacity Centre at the Oxford Martin School. She has been a cyber-security specialist in business and a research scientist in the Ministry of Defence.

Thank you both for joining us.

Professor Martin, give us your assessment of the current state of the cyber-resilience of the UK's critical national infrastructure, both from your tenure inside government and now from outside government.

Professor Martin: Let me first declare all relevant interests. As well as my main job at the University of Oxford, I work with and advise a number of cyber-security companies, mostly in the US and Australia. They are all on LinkedIn. I shall provide a full list to the Clerk.

The one that I want to highlight because it has submitted written evidence to the Committee is a UK specialist company, Garrison Technology, to which I am an adviser. I have a small number of options in it, but that is fully open, so thank you for that opportunity.

Given that it is the start of the Committee's very welcome investigation, it is important that I say I do not think that we are discussing hugely catastrophic loss-of-life risks that you might get from a major terrorist attack or military strike. It is a very serious problem, but it is important to try to diagnose it.

There has been a lot of hype around cyber-risk over the years. People talk about planes falling out of the sky. Critical systems on which people's safety depends have strong safety back-ups.

Many of you may recall, because lots of your constituents were affected, that last summer the national air traffic computers went down. That was not a hostile attack, but that makes no difference if you are a passenger. All planes in the air landed safely. They were delayed and some landed in the wrong place, so there was a lot of disruption and economic cost, but there was no realistic threat to life. When there is a threat to life, you would not get on a plane thinking that if a computer goes down you will

be stuffed; you would want a back-up. That applies to other critical safety systems.

Russia, a formidable cyber-power, has found it very difficult to achieve any sort of cyber-impact in the war in Ukraine. Cyber is used for intelligence, intimidation and so forth. For military effect, as we have seen, tragically, it is traditional and conventional.

There are serious things that we should worry about, and mostly, so far, they have come a little bit from nation states but often from criminals. We saw brilliant disruption of criminals by the National Crime Agency yesterday. They have gone for things like hospital administration.

A serious disruption that has changed my view of critical infrastructure resilience happened in the US in 2021 with a company called Colonial Pipeline. The pipeline went offline—it was shut down. It was shut down not because of a sophisticated and difficult attack on it but because they did a pretty simple attack on the company's administrative systems. The pipeline was fine; the company just did not have the systems to operate its safety rotas, invoicing, etc.

There have been serious problems with healthcare in Ireland, with occasional problems here. The problems is not whether operating theatres work but scheduling operations.

You see that with the British Library, which will never make the top of anyone's list of critically important national institutions, but it is an important national institution and it has been close to defunct for a few years.

That would be my characterisation of the risk. In terms of the who, sometimes we cast the net a bit too widely. Nation states have been interested in doing this type of disruption, but more in preparing and threatening it rather than doing it. Russia does a bit of it. Its offensive cyber-capabilities have been created mainly for political and geopolitical ends.

One significant change to which I draw the Committee's attention is in the Americans' assessment of the risk of the threat from China. If this hearing had been held a year ago, I would have said that China has no history of disruptive attacks on critical infrastructure. It has a huge espionage operation. The origins of its offensive cyber-capabilities are economic—stealing lots of data, and so on.

Earlier this month, the head of the FBI and the head of the Cybersecurity and Infrastructure Security Agency said that China is pre-positioning all over US critical infrastructure. It is not for spying. It is in case: they can activate this to cause significant disruption.

Q2 **Chair:** I can imagine what pre-positioning means, but will you unpack it a bit?

Professor Martin: It is an implant on a network that could be caused for intelligence gathering, although the Americans specifically say that this isn't. It could be used as a beachhead. Cyber is not an easily deployable weapon; you have to get into the network and build out from it. It is very difficult for a President or Prime Minister sitting in Beijing, Moscow or, frankly, Washington to say, "I want you to hit so and so by cyber." That takes time.

If you are pre-positioned—hence the word—that helps. With pre-positioning, unlike other types of cyber, you are trying really hard not to be caught for quite a long time. Earlier this month, the Americans said that China has been lurking in aviation, water, energy and other critical sectors for five years. That is fairly significant.

Then, of course, we have criminals who just want money but will disrupt critical structure.

Q3 **Chair:** Thank you for that comprehensive tour d'horizon.

Professor Creese, perhaps you will add to what Professor Martin has said, and of the infrastructure sectors that count as critical national infrastructure are there any that particularly concern you?

Professor Creese: Yes, and thank you.

I should declare relevant interests. I advise and consult various companies on cyber-security; I can supply details, if necessary.

On critical infrastructure, it was helpful to end the previous answer on pre-positioning. We should assume that that is already taking place in the UK, and I believe that we are aware of it in some sectors.

Pre-positioning, as Professor Martin said, involves getting a foothold on a victim's environment and persisting undetected. That can be useful for a number of kinds of attack, and I want to elaborate a bit on that.

A threat actor might decide it wants to sabotage a system. It might be a criminal, so it might want to sabotage a system or threaten to do so and ask for a ransom. It is a way of coercing money.

It might be politically motivated and want to sabotage a system to demonstrate some form of power or cause terror.

It is a significant concern for us and has been for a number of years. Professor Martin is quite right to note that a lot of concern has been raised about risks that perhaps are not realistic.

It is important that the Committee is aware that cyber-security is not either present or absent. Resilience and security operate across a range. The question is: are we exposed to more risk than is acceptable to us?

There is no doubt in my mind that risk is aggregating. It is a bit like an iceberg. Some of the risk is not observable to us. Other states calling out

pre-positioning in nations that we know may well have an interest in stealing IP or perhaps sabotaging systems should concern us.

I would be least concerned about the finance sector because it has been regulated for so long. It tends to have quite advanced capabilities and capacity. It tends to have a workforce who know what they are doing.

It is hard to talk about other sectors as a sector because their capability in cyber-resilience will be variable. It tends to vary according to the outlook of leadership—how much priority have they placed in investing in cyber-resilience capability? Has that organisation felt harm? Has it been subject to an incident? Has it conducted threat-hunting and found a hidden pre-position—cyber-crime or some other threat actor—on its system?

In my experience, organisations that have felt harm are more inclined to take cyber-resilience requirements more seriously and think harder about investment.

Q4 **Chair:** Do you agree with Professor Martin that in some ways the weakest links are administrative systems rather than what one might think of as frontline security systems?

Professor Creese: Partially. My answer would be: you can find the weakest link anywhere. I have been working in the domain for—gosh!—over 25 years or thereabouts. In those years, there have been periods when it has been fashionable to focus on people and process, and periods when it has been fashionable to focus on technology vulnerability.

It is all a potential attack surface. The threats that we face are very good at orchestrating across all these surfaces and you will find weak links in any of them. The strongest position that I always advise organisations to take is to make sure that they are trying to orchestrate across all of them.

Yes, there are weak links in the process but also in the technology.

Chair: Thank you. That is very clear.

Q5 **Tracey Crouch:** Professor Creese, the methods used by cyber-attackers are continuously evolving. We see increasing levels of sophistication being used. Will you expand on the main forms and methods of cyber-attack that threaten the UK's critical infrastructure?

Professor Creese: They will span all attack methods. Generally speaking, threat actors will try the easiest route first—don't get out your most valuable secret weapon, because once we've seen it we can learn how to defend against it—and they work up from there.

You need a foothold—a way in. That will be created by hacking from the outside, finding weak software or hardware that is connected to the internet, crafting a cyber-weapon—an exploit—that finds the weakness

and takes control of the computer. Once you are in, you move around the system and try to find your target.

Alternatively, if you cannot hack from the outside, you find valid access credentials and get in that way. They can be purchased on the dark web. There is a blossoming ecosystem of people stealing or crafting access credentials not to use themselves but to start someone else.

Or you phish—social engineer—or persuade or coerce somebody into giving their credentials away. You can position a piece of malware in an environment and it opens the back door from the inside. Malware would be a piece of software that was acting with malicious intent. How do you get that into systems? You trick somebody into putting it on to their laptop, or via a USB stick—portable memory—or attach it to an email and somebody unwittingly opens a file that installs it.

If none of that works, an insider threat is a big reality. What does that mean? An insider threat is traditionally viewed as a human who has valid access credentials—an employee or trusted partner. They are either coerced into becoming an insider threat—they already have the credentials but are blackmailed into acting maliciously on behalf of a threat actor or organisation—or, in the worst-case scenario, and when it comes to critical infrastructure this would be on the radar, organisations are targeted and people attempt to obtain jobs and from the get-go act maliciously with the intention of opening a back door from the inside.

I think that that probably summarises it.

Q6 **Tracey Crouch:** Professor Martin, how has the proliferation of cyber-capabilities changed the cyber-threat to the UK?

Professor Martin: My view—Professor Creese and others may disagree—is: not a great deal yet. One of the things that are slightly frustrating about the profession is that quite a few of the things that Professor Creese accurately set out are pretty old—techniques, capabilities and exploits that have been used for quite a while. The reason they still work is a combination—to pick up Professor Creese's point about culture and technology—sometimes of weak practices and lack of attention but often legacy IT. There is no cyber-security strategy that you can give an organisation that is using a no-longer-serviced version of Windows.

That is what I would say about general cyber-security and cyber-hygiene for everybody. There are a few things that for an investigation into critical infrastructure are evolving, with threats to watch out for that have not yet evolved but might.

The ones that have evolved a little are quite smart supply chain operations. The best example was espionage, rather than a disruptive operation, by Russia against the United States. It emerged in late 2020 and the beginning of 2021. There is a company that is quite important, if

not well known: SolarWinds. With individual cyber-security you get an update from your supplier: "We have detected a flaw; please update this as it is good practice to do so." The Russians extremely cleverly poisoned the update. Everybody who responsibly used the SolarWinds update for corporate network maintenance effectively downloaded digital poison, allowing access to the Russians. That was quite smart, I am afraid, and it needs attention.

You also used the word "proliferation"—an interesting and valid choice of words. If you are looking ahead—I hope you are—one of the things that have moderated some of the risk to critical infrastructure hitherto is that doing some of the basic hacks that Professor Creese talked about is pretty easy: anybody can be trained and taught to do them.

On more sophisticated operations, the Russians have taken out power plants in Ukraine twice, only for very limited periods. They cost a lot of money and need a lot of skilled people.

The barriers to entry for some of the most disruptive attacks—I take Professor Creese's mild correction of what I said, but it is still a set of risks you have to worry about—are quite high. If that does not remain true—as AI comes in more, perhaps it does or perhaps it doesn't; we don't yet know—and more people can easily acquire more potent cyber-tools, we have a different problem than we have had for the past 10 or 20 years.

We must watch for that. I am not being alarmist because it is not a problem right now. Were the lights to go out or were there a serious attack on central London, there is only a handful of actors who at the moment have the capability to do that. That equilibrium needs to hold. If it doesn't, we need to change our approach.

Q7 **Rebecca Long Bailey:** Professor Creese, you mentioned that risks were aggregating like an iceberg at the moment. What are the common challenges in detecting and mitigating cyber-threats across critical national infrastructure sectors?

Professor Creese: The challenges are not specific to critical national infrastructure, although they may be more challenging because they may be facing significantly more threats.

The challenges in threat detection are: being accurate. There are two different ways, generally speaking. One way is to know what bad looks like and set up systems that will notice when it happens. You need previously to have seen the kinds of tooling or behaviours that have been used somewhere else. If somebody is using an attack tool that we do not understand, we are vulnerable to them.

How do we get around that? We have another kind of threat detection—anomaly detection—that works on an ability to understand what normal looks like. You set up the system to tell you when there are deviations

from normal. They are not necessarily indicative of threat or attack, so they are not as accurate, potentially, as the signature-based systems—I've seen it before—but they do empower you to find stuff that has not been seen before.

What are the challenges there? You might end up with a system that over-alerts. We call that false positives. It is falsely saying, "I can positively say we are under attack in this way."

Why is that a challenge? It is because your security workforce have to investigate those alerts and take action. In both kinds of threat detection, work is generated.

To make that easier and optimise how we use our very limited resources, we in the cyber-security profession try automatically to filter stuff that we know to be bad and not let it get near our systems, or at least know we can ignore it and focus on stuff that is potentially very harmful.

It is very difficult to do. If you are being heavily targeted, more sophisticated attacks will layer. Your system will be faced with a number of different attacks going on. Some of them might be a distraction from the real agenda. That has happened for many years.

That is essentially the challenge of threat detection. The challenge for threat detection, no matter where you sit in the CNI, is that it is more challenging as you are exposed to more threat activity. There is a danger of getting overwhelmed, with very limited security and less resource.

Q8 **Rebecca Long Bailey:** Would you like to add anything, Professor Martin?

Professor Martin: That was comprehensive. I have one example on Professor Creese's point about detecting anomalous behaviour that might bring it to life a little bit.

We correctly see electoral protection as part of the critical infrastructure. As politicians, you will recall better than I do that during the EU referendum the deadline to register was extended, by mutual agreement, by two days because "Register to vote" collapsed.

As far as I know—being head of the National Cyber Security Centre at the time, and this was the Government's assessment—that was simply because of wrong profiling of the number of people who would be interested. The system collapsed under weight of numbers; more people than expected registered to vote at the end.

Given the concerns around electoral protection, we stepped up a whole bunch of efforts. In the 2019 election, we watched "Register to vote" very closely as the deadline approached. I believe that the deadline—forgive me if my recollection is faulty—was a Wednesday at 10 pm. On the Monday evening at about 8.30 we got an alert because the profile we expected was about 3,000 people using "Register to vote" about 49.5 hours before the deadline. Suddenly, it spiked to 48,000. That was a big

deal, but we spotted it immediately, in a way that we were not able to back in 2016.

That stood up an emergency conference and so forth, and ultimately had it been hostile foreign activity the option could have been briefly to suspend the service. It turned out on closer examination that Stormzy had sent out a tweet encouraging people to register to vote, which led temporarily to a sixteenfold spike in use of the website.

From a cyber-security point of view, that is a really good story. It shows that something weird is going on but you spot it immediately. You don't automatically say, "Let's take it down." You do the analysis and get the explanation.

All the time there is what we call large-scale credential stuffing, where by brute force—as Professor Creese said, that is guessing passwords and so forth—people say, "Right. I have a bunch of emails and a bunch of passwords. I will try this network and see how many I get."

It is being able to notice that anomalous behaviour and say, "Something weird is going on." That is how that works in practice.

Q9 **Rebecca Long Bailey:** Professor Creese mentioned the varying capability across critical national infrastructure sectors. Do you agree? Would you pinpoint any specific sectors that need to receive more support from Government-led cyber defence organisations? How much collaboration is there between operators of critical infrastructure and Government-led cyber-security organisations?

Professor Martin: "Variable" is the word. I would split it into three. As Professor Creese said, the financial sector has been an exemplar for a while. For all sorts of reasons, regulation started earlier post the crash. It fits very well with the post financial crash concepts of operational stability—cyber, and so on. Banks' general regulation runs off the premise that you can't stop every loss of money but need to be able to stop systemic risk, and that is very good for cyber-security. Since 2012, the Bank of England, in collaboration with the sector and the NCSC and its predecessor organisation, has worked well to get a model of regulation that works for the industry.

Towards the end of my time—I think this is a big improvement—we started to do that with telecoms. The Product Security and Telecommunications Infrastructure Act passed in December 2022. Its parliamentary passage was dominated by debate about Huawei. That is basically applying the same principle.

In a sense, it was suggested by the telecoms companies. One of the problems we had with telecoms companies was that regulation was based on lowest consumer prices, and, when we were in the EU, no roaming charges. There were no regulatory incentives or penalties to do security. There are now, and they are quite good.

Those two are good. Finance is better because it is longer established; telecoms are getting better.

It would be useful to probe in terms of Government and three and a half years out of date, but telecoms and, in particular, finance are different from energy and water. Telecoms has a lot of it, but energy and water have big, hard infrastructure. As a result of NIS2 and legacy EU rules, there are some obligations, but from what I have seen from the regulators and lead Government Departments there is considerably less, certainly in the public domain, about how that partnership works, how the regulatory approach works in energy and water, and given the vulnerability of those sectors and the sheer amount of intrusions we have seen all over the world and here in the UK, I think that is worth probing. I might be wrong, but I think it is worth probing.

In category 1, I would have finance and telecoms as good examples, and, in category 2, I would have energy and water as being worth exploring.

Then there is everything else—day-to-day life. Top of the everything else category, which is a big one, would be NHS administration. With NHS critical systems, in individual hospitals there would be no off button for operating theatres. The NHS suffered a reasonably serious incident in 2017, which was an accident. The North Koreans were trying to rob a bank, essentially, and they wrote some really bad code. As the code was so badly written it looked for destinations that it was not supposed to get and infected organisations in more than 100 countries, including—

Q10 **Chair:** This is WannaCry?

Professor Martin: WannaCry. The NHS has done a lot to try to improve that, but if you want to get big enterprise software systems in lots of small organisations—the NHS is an aggregation of small organisations—that will be some work.

The Joint Committee on the National Security Strategy did a very good investigation into the ransomware and criminal problem, but it is interesting to look at what happened in Redcar and Cleveland council, where they were locked out. There were manageable problems like delays to refuse collection and stuff like that, which you can work around for a few days without any great inconvenience—it is not very nice, but it is not a threat to anything. We had to send a specialist team because the children's services database was locked out.

That is my very important third tier of pretty basic stuff that we cannot forget.

Q11 **Rebecca Long Bailey:** Would you like to add anything, Professor Creese?

Professor Creese: No, I thought that was really excellent. I can't improve on that answer.

Q12 **Graham Stringer:** I should like to go back to your comprehensive introduction, Professor Martin. You said that systems are very good where safety is important. There were reports in the newspapers at the weekend of a six-car pile-up because the system for detecting things going wrong in the middle lane on smart motorways had gone wrong. I do not think you are complacent, but it is a bit complacent because those critical systems in aeroplanes and on motorways are not that good in many cases, are they?

Professor Martin: Certainly, that case is very concerning. I think that one of the reasons we do not have autonomous vehicles running around the roads at the moment is that we do not have the safety model right yet. As the smarter technology comes in, it will be really important that we do not let them out on the road until we have the safety model worked out. We all know that autonomous vehicles work. We have seen the videos; but at the minute—I am not a transport expert, but this is how I understand it—the people who would be responsible for saying they are safe to go out on British roads say, "If you are going to use an autonomous vehicle, you must be a qualified driver ready to take charge of the wheel, sober, not working, not watching TV and not asleep." So it is kind of pointless having an autonomous vehicle.

There will be cases such as the one you mentioned. It is really important not to look at cyber-security on its own. Any system is quite complicated and you have to look at the applied use and the whole range of vulnerabilities, whether of railways or cars. Smart motorways are an interesting and quite problematic case in point.

What we did 25 years ago, although it was mostly in software, which is a sort of accidental mistake that we are paying for every day, was to let ourselves become dependent on a bunch of software-based technologies, without thinking about security as they were being rolled out. We have to stop that, with the more applied technology that we are dealing with now; I think we are doing it with things like driverless cars, and we certainly are with the use of AI in medicine, and so forth. That is where we really need to be going. Cases like that are worth highlighting because they show, sometimes, where it may not be working.

Q13 **Graham Stringer:** You talked about resilience in the systems and protecting the systems. In terms of critical infrastructure, is it sensible to go back to previous, non-digital, non-computer technology as a reserve for what we are doing? It seems to me that you can put a certain amount of protection on all the digital computer systems, but there will be somebody who gets through the system. Should we have, as a back-up, older systems that are not computer-dependent?

Professor Martin: Professor Creese and I have got through the first 40 minutes of the hearing without using the dreaded phrase, in cyber-security, "It depends"; but I need to invoke it now, because it does depend.

There are some sectors where what you say does not make sense. I am thinking of the Government, or previous Governments—Oliver Letwin, for example, was assiduous about it in the Cabinet Office—looking at the resilience. That would be about any threat; it could be a physical threat, a bomb, a power cut or a physical attack on undersea cables. In the case of the financial sector, printing banking records is impossible, so for that sort of thing you need to think about back-up data centres, or back-up for whatever it might be.

There will be other areas: as far as I understand the matter, although it is for the sectoral experts rather than me to answer on it, air traffic control is not a bad example of where the back-up system is fairly old school and pre-digital. The important thing for any organisation, and particularly a critical organisation—Professor Creese is probably more expert on it than me, so it would be worth hearing from her on it—is what to do if you lose the network. If the answer is that you go back to a pre-digital system, fine; if it is that you go back to a reliable, completely external digital back-up, that is fine, too. There could be a number of answers, depending on the sector.

Q14 **Graham Stringer:** Professor Creese, do you want to add anything?

Professor Creese: Yes. In fact, I believe it may have been WannaCry where some of the local GPs did failover on to paper, so we have examples; but I agree with Professor Martin and will, unfortunately, invoke "It does depend."

We should be mindful that for some organisations and some sectors it will be easier than for others. If you previously had a process that was not digitised, and you have now digitised it, the chances are that someone in the organisation might recall that process, and that, in fact, even if they do not, reverse engineering back to paper will be possible. Because it went one way, it may be possible to reverse it.

In other organisations that are inherently digital, which perhaps have built their business around being on the internet, the processes will look a little different. They will be built inherently around digital, so it may be trickier to create paper-based alternatives; but it will not necessarily not be worth doing it. There may well be specific areas where we need redundancy and failover. That is where the safety mentality helps security.

The two come together. Obviously, if you are not secure and you are in a safety-critical organisation, that lack of security might mean that you are subject to malicious attacks. We use security to protect safety, in some examples. We can also use safety, and its consideration of how you keep things running and how, when you fail, you need to do so in an elegant fashion without loss of life or gradual degradation, or that kind of thing. Those ways of thinking are also very useful in cyber-security and cyber-resilience.

To end on the example of smart motorways and driverless cars, if a driverless car were to detect that it was under cyber-attack and was doing 70 mph on a motorway, the right response would not be just to shut everything down, because if the vehicle stopped very suddenly it would be likely to cause one of these pile-ups. So there is a need to think about the safety-security interface and, in the general area of AI machine-learning, controls like threat detection, where we do not have specialised products in the marketplace right now.

Q15 **Graham Stringer:** Should we keep our old-fashioned, wire-based telephone system?

Professor Martin: Agnostic: again, I would be interested to hear from telecoms experts. There is resilience built into the way mobile networks are constructed. We saw that in 2017 or 2018—I am sorry, but I cannot remember which. Ericsson built a lot of the infrastructure and its O2 infrastructure accidentally went down. When you are looking at the resilience of critical infrastructure you have to remember accidents. IT systems fail all the time by mistake as well as by malicious acts. For users of O2, there were a few complete withdrawals of service, but for the most part there were slower, more stuttering services that went on to other networks.

One thing that you try to do is make sure there is no single off-button. The telecoms infrastructure legislation dealt with this, and it also applies to things like smart meters. There are various bits of the network that will survive in the event of a digital attack.

I honestly would not want to venture a yes or no opinion in answer to your question. It is worth posing it to telecoms experts, because it will be a cost-benefit analysis of how expensive it would be to keep it going just for resilience and latency reasons versus the likelihood of the risk that all the different bits of the digital telecoms network would get taken out at the same time.

Q16 **Graham Stringer:** You covered pretty comprehensively in your introduction the threat from nation states. I think I am right in saying that you did not mention North Korea. Is it possible to estimate quantitively the increasing threat from other nation states?

Professor Martin: Quantitatively is hard. A quick overview has Russia as the classic political threat with a history of disruptive activity in critical infrastructure. For China, there is no history, but the Americans are now saying they are more than poking around. Iran and North Korea both have limited history of disruptive attacks and not so much recently—although some. Iran's attacks have mostly been regional—not just Israel, but more localised.

North Korea has done disruptive attacks. There was one on Sony Pictures in 2014. As well as leaking celebrity emails, they destroyed quite a lot of Sony infrastructure and wiped a lot of value off, making things much

more difficult for the company. They have done less of that, because the North Koreans are now, in the words of the US Government, the world's first state-sponsored cyber-criminal. They are focusing on trying to get money out of the global financial system, so that is where their threat has been focused for the last few years. That is where WannaCry, a misfiring attempt to do that, came from.

That is an overview of the state threat, which is very similar to what I would have said in office five years ago, so there is a stability there. The big change, to go back to the exchange with Ms Crouch, is about whether in the future someone will buy their way to the top table. North Korea and Iran are not as good as Russia and China. They just have a higher risk appetite and some capabilities that are sort of middling rather than elite. Other countries could buy their way to middling capability and potentially if costs to entry get a bit lower it is a question of what their risk appetite is. So it is stable, but it needs watching.

Q17 **Chair:** Briefly, on the example of driverless cars, or autonomous vehicles, which we have been talking about, there is obviously a lot of regulation on whether the sensors work and can detect a pedestrian stepping out into the road, and that sort of thing; but clearly, as you pointed out, there is a separate set of threats or risks around deliberate cyber-interventions. Who should approve that? Who should regulate that? Are the transport authorities capable of doing it, or is there a need for, as it were, a separate button to press to validate, or not, the cyber-resilience?

Professor Martin: My view—and this is more a view as an ex-practitioner; Professor Creese may have a different view, as a much better academic than I will ever be—is strongly that that should be sectoral. It goes back to the exchange with Ms Long Bailey. If you set up a cyber-regulator, the use cases are so different.

Going back, and drawing on my time at the National Cyber Security Centre, we did have exchanges—they were, in the early days, with finance, because they were the most mature—in which we would say, "Cyber best practice looks like this." Frankly, some of the Bank of England team would say, very honestly and constructively, "Fine, but that is unaffordable for banks and will just not work in a bank." It has to work in the environment. If you think about what running a big bank is like, versus running a very complicated energy system, a big university or the NHS, it is very different. To come back to Professor Creese's point about merging security and safety, the safety expertise tends to come from within the sector.

It can go wrong. In the American experience, post the Colonial Pipeline case that I mentioned earlier, there was heavy criticism of the new regulations about pipeline security and so forth; but I do not think a cyber-rule as opposed to sectoral rules that are applied in the use cases would make sense. Others disagree.

Q18 **Chair:** I thought you just said there should be a central capability.

Professor Martin: No, a sectoral one.

Q19 **Chair:** Sectoral, not central. I see. That is very clear.

Professor Martin: They should be advised by the centre. That is what the National Cyber Security Centre did and does, but the rules should be set sectorally.

Q20 **Chair:** That is broadly consistent with the approach that is being taken to AI regulation, for example, where it is deemed that sector regulators, rather than a central regulating capacity, have the best chance of doing it.

Briefly, Professor Creese, on that: I think you nodded when I drew the comparison with AI. Do you think that is consistent?

Professor Creese: Yes, and of course AI is particularly challenging. The international community is grappling with it. I would just add that the reason we have to embed this at the sectoral level is that we need a stronger leadership. We need cyber-resilience to be in the DNA of our organisations. That means it must be in the DNA of the boardrooms, as financial risk is.

It seems to me that the only way to do that is to embed it into the sectors; but we will also need some kind of strong oversight that has the power to enable change, to ensure that that sectoral regulation is happening.

I am involved, as I am sure Professor Martin is, in a number of international bodies that are thinking about, for example, the governance of AI. These challenges are being discussed there, too, but my guess is that this is where it will end up—as it should, because, for example, there are certain environments where you could over-regulate and impact on or deter innovation in a way you would not want to.

In other use cases, or other sectors, it is critical that there should be strong oversight and regulation, because human life is at risk. We cannot assume that all examples are the same. For that reason, and because of the necessity to get leadership properly engaged, I wholeheartedly agree with Professor Martin that it is important for it to be done at sectoral level. I would argue that you must definitely strengthen oversight.

Chair: That is very consistent with the AI discussions that we are having.

Q21 **Carol Monaghan:** Professor Martin, last year the BBC showed a "Panorama" programme. I think the title was "Is China Watching You?" It highlighted the use of particular CCTV systems in Government Departments. Are we or the Government naive in our approach to cyber-security?

Professor Martin: I don't think the Government is being naive in its approach to cyber-security. You mentioned the way in which different bits of hardware came on to the market over time, before, perhaps,

Governments in the west clocked it. This goes beyond hacking and is partly about selling hardware into the UK market: it meant that quite a few of these things ended up in the UK and many similar countries. It is worth being realistic about what some of these things can do. For example, there is a lot of mirth and cynicism at the minute about a story that emerged in the cyber-security press about an apparent hack of 3 million IoT toothbrushes; it turned out not to be true, but even if people have internet-connected toothbrushes that does not get you very much.

Q22 **Carol Monaghan:** A sparkling smile, maybe.

Professor Martin: Exactly. A camera is a camera and it depends where it is.

Are there areas where there is probably unreliable kit, still, in places where it should not be? I think yes, and we probably woke up to that a little late. Since the late 20-teens there have been various programmes. Some of them have been covered in the media and no doubt you as MPs have had memoranda about them—about toughening up a bit.

One of the reasons it matters that we should be more careful about this in future is that, having been on the board of GCHQ—which obviously I cannot say too much about, but which is an intelligence-gathering as well as cyber-security organisation—there was an acute awareness of the limitations of some of this stuff in terms of what one camera can give you, but also of the fact that if you have hundreds or thousands of cameras someone has to make sense of that. If a camera is just looking at a pavement all day and not much is happening, how do you get anything useful out of that?

That becomes a long-term strategic risk, however, if some of the predictions about the power of AI come true. There is a distinction between what you might call mass surveillance and mass spying. They are not quite the same thing. Mass surveillance could be gathering an awful lot of data that nobody has the capacity—either computing or human—to look at and make sense of. That is mass surveillance. You are gathering lots of stuff and maybe you can find something.

With AI you might—it is something we have to watch out for from China—be able to turn that into mass spying, where you can run a programme and say, "I have 3 million cameras all over the UK"—or the US, or wherever it might be. "Can you analyse this for me and find out something interesting about this person, using facial recognition"—

Q23 **Carol Monaghan:** You are talking about many cameras. If we narrow it down, surely there is the opportunity, if you are that way inclined, to target particular cameras that are showing something more interesting than a piece of pavement.

Professor Martin: Indeed; and that is why you have gradations of risk and should be very careful about what you have on sensitive sites, and so forth.

Q24 **Carol Monaghan:** Is enough attention paid to what we have on sensitive sites?

Professor Martin: I am aware that more is being done. In the Departments where you would expect it, such as the Ministry of Defence, there have been quite a few initiatives recently. I do not know, if I am honest, how much assurance that would give, but I do not think it is something that is being completely ignored. That would be unfair.

Q25 **Carol Monaghan:** Thank you. Professor Creese, I saw you jotting notes during that. Do you have anything to add?

Professor Creese: Yes, I thought they were excellent answers. I had some other insights that I wanted to offer. I recall that many years ago one of these IoT cameras was hacked and used in a distributed denial of service attack as part of a botnet. I would say that the point about some of these devices is that it is not just their primary functionality that is at question. Every one of those devices, if connected to the internet, is a potential platform. That does not mean we should not have them; but we need to be aware of that.

Sometimes devices can be more targeted platforms. For example, it might look like somebody's toothbrush, but it depends on the computing capability. A toothbrush is in someone's home, vehicle or office and, if it were possible to compromise it and pivot onwards, that would be a potential way in.

I agree with Professor Martin. There is no evidence of the toothbrushes being used for that right now, but we have to be eyes-open. Any device with computational capability and connectivity capability is just another part of the attack surface that we need to be concerned about.

When it comes to cameras, that can be challenging. If you were an organisation in a sensitive site and somebody managed to gain access to the footage from the cameras because they are IP-enabled and connected to the internet in some way, you could generate some kind of pattern of life on that site. It might help you to predict good times of day to attempt a physical attack; it would help you to understand who goes in and out, who passes by and who may work there. You could then use social engineering to try to compromise the individual to find a way in. As with any kind of data collection capability in any system, we would say that you need to consider the cost-benefits in terms of the risk and potential opportunity benefits. Do not collect data without good use or put instrumentation into your environment without good reason, because it can be a source of attack surface and can be compromised; and if you are collecting data that is just another piece of data that you need to protect.

We would use that advice in all environments: medical or health records, no matter what, it is good practice. I do not think you are wrong to be

concerned, but that does not mean that the business case for having the cameras does not outweigh the possible risks.

Q26 **Carol Monaghan:** Are there alternative camera systems that could be used?

Professor Creese: I am not an expert on this but I would say that over the years camera systems will increasingly be built with connectivity. I do not know if you have tried to buy a smart TV without a camera for your living room recently. That is quite hard to do. Many years ago, if you were concerned about chip sets in personal routers being manufactured in certain parts of the world, you would have found that they were generally manufactured in one part of the world. The issue of whether you can develop resilience through thinking hard about alternative sources for the manufacturing of hardware or software is challenging. It is a really good point to focus on when it comes to a cyber-resilience strategy for the UK—thinking about those kinds of questions.

Carol Monaghan: It is 1984, 40 years on.

Chair: We will now have to ask for brief answers, as we are running out of time, such has been the interest in your answers so far.

Q27 **Dawn Butler:** Thank you both very much. Professor Martin, thank you for highlighting the role that Stormzy played in the general election. In his song "My Presidents Are Black" he says he is going to keep out of politics, so hopefully he will listen to this session and know that he played a vital role.

Are there any other areas that we should be concerned about in regard to our democracy and politics, and cyber-security?

Professor Martin: Yes, I will be as brief as I can. I think the important thing in terms of electoral protection is trying to just map out the different bits that could be vulnerable, based on experience and on consulting experts on how elections work. You all know better than me that these are hundreds of local events that aggregate into a big national one.

The Government offered political parties networks and support if they wish; obviously it has to be done voluntarily. That was in response to what the Russians did to the US in 2016. The first intervention was stealing a bunch of documents from the Democratic National Committee and from the private emails of a key Secretary Clinton adviser. We gave guidance to parliamentarians and local authorities, for running the election safely—compilation of the electoral register, printing of ballot papers and that sort of thing. In fact, registering to vote in the British system is one of the few nationally centrally run services in the election, so you end up doing lots of outreach and protection to other organisations. Media is another one.

That is, in a sense, to prevent hacking. Of course there is now the problem of disinformation, AI and deepfakes, and so forth, which are a

slightly different problem. We have to do a lot of work with the platforms. Twitter, sadly, has abandoned content moderation to all intents and purposes. That is more difficult. Facebook, actually, whatever criticisms one may legitimately make of it, takes it very seriously and tries to remove things as efficaciously as possible.

One thing that I think the UK political system has done well, and better than the US, is the cultural reaction to fakes and hacks. When the US was hit, the media ran with it and candidates made hay with it politically. If you take the deepfakes of, say, the Mayor, the security Minister was out there immediately saying, "This is a fake. Don't circulate it." When there was exposure of campaigns against Members of Parliament and others, parties came together and said, "We are not going to use this material." I think that is a very important point on electoral protection. So the whole tapestry of the election system needs to be looked at.

Q28 **Dawn Butler:** Professor Creese, what is the difference between sleeper cells and pre-positioning?

Professor Creese: Well, I am not the expert. Perhaps Professor Martin will give you a better definition; but sleeper cells are essentially pre-positioned groups of individuals currently not activated. I guess you would find an example, or a corollary of that, in cyber where people have pre-positioned and may not be doing something; but often they will at least be checking that the heartbeat connection is still working, periodically. My understanding of sleeper cells—I am not the expert—is that that might not be the case.

Q29 **Dawn Butler:** Professor Martin agrees with you. My last question is how concerned we should be about computer repair centres.

Professor Creese: A fascinating question. I will deal with it in two ways. Functionally, allowing somebody to repair your computer gives the opportunity to install something. So theoretically that would be a potential point at which somebody could get some malicious software on to your system. Do I believe there is a significant threat or risk of that, currently, in the UK? Personally, I have not seen enough evidence to say that it is a big concern; but functionally it is a potential risk that should be assessed.

Q30 **Dawn Butler:** Professor Martin, do you have anything to add?

Professor Martin: A great answer. I would share the assessment. I think people have to make risk assessments. If you are working at some of the organisations I used to work for, you do not go to computer repair centres, out of an abundance of caution. I think Members of Parliament might want to take sensible steps so that they know it is reliable and trustworthy and has a good record.

To go back to the sleeper cells versus pre-positioning comments that Professor Creese answered expertly, in more sophisticated operations there is often a combined human-digital element. You might have an

operative working for a foreign intelligence service on the ground in the UK, potentially looking to get into a critical site—maybe to get a job there, or whatever. It is not that common, but at the top end of the threat you need to worry about that human and technical interaction.

Q31 **Dr Davies:** Professor Martin, could you tell us briefly about the organisation of governance structures in the UK for dealing with cyber-security and the resilience of national infrastructure, and their role, in general terms, in responding to cyber incidents?

Professor Martin: I will do so as quickly as I can. It is governed by the National Security Council, chaired by the Prime Minister. There is a sub-committee that deals with critical infrastructure, which used to be called the sub-committee on threats, risks and hazards, but I do not know whether it still is.

There is no single policy Department for this. In so far as there is, it is probably the Cabinet Office. Some of the governance of cyber-security policy issues is a bit messy. There is a certain inevitability about that because it is so cross-cutting, but it might do with a bit of looking at. The model is made up of the National Cyber Security Centre, part of GCHQ, which is the single source of advice but is not a regulator and has no regulatory functions whatsoever, and the sectoral regulators—the Bank of England, Ofgem, Ofcom, etc.

Q32 **Dr Davies:** My second question is about the extent to which attacks are being reported and recorded. Do the public and indeed the agencies and the Government have a clear idea of what is going on?

Professor Martin: It is not as clear as it might be. It is difficult. France passed what you might call a very widely defined law, with incredibly onerous duties to report cyber-attacks. You get statistics that are a bit ridiculous—for example, "This bank faces 58 million attacks a day." In some respects that is true and in other respects it is nonsense. What is a cyber-attack? That is quite difficult.

In critical sectors, thanks to the 2017 EU network information security directive, which still applies to us, there are disclosure obligations on critical infrastructure companies, so it is better for critical infrastructure-designated companies.

Q33 **Dr Davies:** Professor Creese, do you have any thoughts on that?

Professor Creese: I agree wholeheartedly with Professor Martin. Going one step further, I would imagine that one of the more challenging spaces is when thinking about supply chains. Interdependencies between organisations have always been challenging. We are moving towards quite complex supply chains—dare I say, ultra-large-scale infrastructures. Understanding the level of risk, based on reporting from multiple organisations, and putting that together into a bigger risk picture is probably a capability gap that we need to look at for the future.

Q34 **Rebecca Long Bailey:** Professor Creese, what are the most pressing policy considerations for the Government as they aim to strengthen the cyber-security and resilience of critical national infrastructure?

Professor Creese: Gosh, that is a big question. I would be looking at a number of things, including how we ensure that there is strong leadership across our organisations that inherently understands cyber-risk. There is a policy consideration there. More needs to be done, because they set culture and investment, and we cannot leave it solely to regulation, so we need to think about incentivisation of behaviour, too, in other ways.

The other piece must be around understanding how systemic risk might be emerging and the supply chain risk issues—at least to get visibility of it in the first place, on which we can build business cases for new policy interventions.

Q35 **Rebecca Long Bailey:** Professor Martin?

Professor Martin: I am conscious of time. I am not prescribing where we might end up, but the issues to look at include reporting requirements that have come up. It is worth checking that they are in the right place.

We have not discussed the issue of criminality, but it is a big problem and potential. The Government should look seriously at the issue of the legality of paying ransoms because it is currently encouraging more.

I have mentioned that the energy and water sectors could do with a bit of a look, and I wonder whether it is worth the Committee and the Government thinking about what a general duty of resilience looks like and how it applies to different sectors. Taking the example of the Colonial Pipeline in the US, it had a regulatory obligation that, if the pipeline was shut down, for whatever reason, it had to be back up and running in seven days. As long as that was the case, it was fine. That is a bit of a weird regulation, but there should be a way of requiring every public authority and organisation that is in some way critical to look at what happens if you lose access to the key network, and how regulation, if appropriate, can incentivise a better response.

Q36 **Chair:** Thank you very much indeed, both of you, for your evidence. I have one final question. We have been talking about internet of things-enabled toothbrushes. There are current, more connected devices, such as smart speakers and Alexa devices, which listen to what is going on in a household. Do you think they present a risk? Perhaps to crystallise that, do you both have them? Given that you work in security, you may have a higher bar, but would you advise your relatives who are not in the field to have them?

Professor Martin: I do, and always have had. Smart speakers have been around for a while, and I have not come across any compelling evidence that they have been used in that way. Professor Creese may know differently. I have never discussed top-secret activity in my home anyway, just because of all the things that would be there. We need to be

aware of smart speakers, but, apart from some extreme circumstances, for people who are very vulnerable and so forth, where we need to be very cautious, they are fine for most people, and I would include MPs in that.

On IoT generally, Professor Creese made a really important point about looking at footage of CCTV cameras. It is important to remember, in answer to Ms Monaghan's question, that where it is made—China, principally—is one part of the issue, but it could be made in Catford and there would still be footage that could be hacked into, so I would not get overly fixated on the country of origin. It is part of the issue; obviously, it is easier to implant something made in China, but you can still hack into some of this stuff. I would not get too sensationalist about some of the IoT risk.

Q37 **Chair:** Professor Creese, would you like to talk about smart speakers?

Professor Creese: Asking if I have a smart speaker is a little bit like asking for my password, so I will not comment on that. Do I advise people to have them? I would say, if you are a person in a significant leadership position where a threat might have an interest in targeting you to coerce you into doing something, or threaten you so that you would do something that could harm your organisation or your family, any devices that give away how you live will make you more targetable. I would advise people in those kinds of positions, where they may well be targeted, against having these things in their environment, just as I would advise against putting a camera up in their living room. It potentially gives an attacker more information about them that can be used to craft targeted attacks. But, as Professor Martin said, that does not apply to the vast majority of people.

Chair: That is very clear and understood. We are very grateful to you both for your compelling evidence this morning; thank you very much indeed.

Examination of witnesses

Witnesses: Siân John and Professor Rashid.

Q38 **Chair:** Siân John is chief technology officer at NCC Group, which is a commercial company advising others on how to deal with cyber-security threats. Siân has worked in cyber-security for 25 years, across strategy, business, risk, privacy and technology. She is also chair of the techUK cyber security committee and a member of the Cyber Security Council's strategic advisory board. Thank you for coming today.

Professor Awais Rashid is professor of cyber security at the University of Bristol. Professor Rashid is head of the Bristol Cyber Security Group and director of the National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online. He is also editor-in-chief of the Cyber Security Body of Knowledge.

Thank you very much indeed to you both for coming. You have been kind enough to listen to the evidence that we have heard. This is the first session of our inquiry. I am particularly keen to hear from you both on the current level of cyber-literacy in the UK among the general public and those people who need to know—there may be a distinction between the two.

Siân John: I declare that as well as being on the executive committee at NCC Group I have shares in Microsoft, where I used to be a senior director.

We have a problem with literacy in the country generally, and this refers back a bit to the previous conversation. There has been a tendency to see cyber as the thing that is done by somebody else: you do the implementation of a system and then other people respond. Sometimes, it is almost like a point of pride to say, "I don't do computers, so I don't do cyber." Actually, as technology sits in our day to day, the reality is that we need to have some skills.

I have some statistics with me. Only about 30% of businesses have board members or trustees who are explicitly responsible for cyber, and many of them lack the knowledge. We really need some form of literacy, from young schoolchildren right the way up, as digital becomes very much part of our lives, whether as social media, smart speakers, in cars or the technology we all own. We need to understand the threat and the risk that comes with that, as well as the opportunity. It does not mean that you do not do it; it just means that you make an informed decision about the risks, just as you would in crossing the road. It is the same thing in literacy.

There are two sides to that. One is about asking what you need to do to be secure: how do I do cyber-hygiene? People at home must keep things up to date; it is not an option. You must make sure you think about what you are saying in front of your smart speakers, and make sure that you are using strong authentication. In business or in government, when you are doing investments, for example, you have to ask: can I afford to keep this up to date and in a good state? Am I making the appropriate investments to manage the risk and threat that comes with that, as well as the opportunity?

The other side of the awareness thing is talking about provenance—informing ourselves about how to recognise what good information looks like. It is quite hard to spot disinformation but we should maybe have a healthy amount of scepticism. That applies to disinformation, to getting a link that asks you to click on it that is phishing, and to somebody from India claiming to be there from Microsoft to fix your computer.

Q39 **Chair:** Thank you very much. Professor Rashid, I put the same question to you on literacy.

Professor Rashid: Before I start, I should declare that, in addition to my position at the University of Bristol, I am involved in a number of collaborative research programmes with industry, and I advise various research programmes. Most significantly, I am founder and director of a company called Hacktonics, which provides specialist training for cyber-security for critical infrastructures.

Following on from what has been said, the challenge is that a lot of the narrative or understanding about cyber-security is that it is things that other people do, and they get in the way. Most of the narrative, as we see in our daily lives but also via the media, is driven by this kind of fear, uncertainty and doubt—FUD, as it is called quite often—where bad things happen and they are always in the news. There is no clear understanding across a large part of the population about the role that cyber-security plays in making a positive difference to our lives.

For example, we do online banking every day, and most of the time it works perfectly fine because the systems are secure and we can trust them. We went through a pandemic using online systems because we could trust them. But we often see security as something that gets in the way and, as a result, we do not necessarily engage with it as something that can help us do our work more effectively.

That translates into the kind of statistics that Siân John mentioned. We have a lack often at senior level in organisations but also, at an individual level, we do not want to engage with cyber-security.

Chair: Thank you very much; that is very good.

Q40 **Graham Stringer:** You have answered most of my question about a national literacy programme—what it encompasses and why you think it is necessary. Who would be responsible for implementing such a programme, and how much do you think it would cost? Would it be a cost on the public purse, or would you imagine the private sector paying for it?

Siân John: There is a mixture of areas. In the early years, for children and people in education, having that as part of the education system is important. That includes training teachers to keep them up to date with the latest that they need. When you get into the adult world, there has been a number of online security and safety campaigns over the years—Get Safe Online being one from a few years ago. The challenge is keeping that going and engaging.

In the private sector, there are plenty of security companies out there that will do education, but the danger is, are we doing that appropriately, or is it spreading fear, uncertainty and doubt to sell a product? Some of the best online education has come from organisations such as banks. We have done good educational adverts and engagement in systems. In reality, it is a partnership between the public and private sectors.

I do not know for certain how much that would cost; I would not want to answer that, but it could be achieved reasonably by a partnership between the public and private sectors sharing educational insights.

Professor Rashid: I would add that there is a difference between what we want more widely across the population and the subject matter at hand here: the security of critical national infrastructure. There, we require very specialist knowledge and capability in building systems that are secure but also defending current systems that have a range of insecurities. I have been working in this field for a very long time and I can say with fairly high confidence that, at the moment, that level of knowledge and capability is lacking across the workforce. We have built very good capability to defend what we would call regular IT systems and built a knowledge base around that, but in building a knowledge base around securing other kinds of systems that are deployed in critical infrastructures there is a serious gap at the moment across the UK workforce.

Graham Stringer: Thank you. My apologies: I have to go.

Q41 **Stephen Metcalfe:** Do those serious skills gaps, particularly in critical national infrastructure, exist across the whole picture, or are there specific specialities that we need to look at? How can we go about addressing that shortage?

Siân John: There are two sides to it. Genuinely, we have a shortage of cyber-security skills in the profession. The latest Government stat says that we are something like 11,200 people short in cyber-security.

When it comes to critical national infrastructure, particularly operational technology, it is not as easy as taking cyber and IT people into the OT world because you need to have the engineering understanding of an operational technology environment; it is a very different approach and way of thinking from IT.

There have been plenty of failed attempts—particularly going back to Stuxnet in 2011—when IT security people have got into OT and said, "We know how to do this," but they do not know about the engineering, the safety systems and the approach, which is why providing security expertise to people with an engineering background is better. Sometimes, it is easier to train an engineer in OT about cyber than it is to give a cyber person all that experience on OT.

Going back to what Professor Martin said, a lot of the threats to critical national infrastructure and operational technology come in via the administrative systems and the management information. Part of the connectivity now is to get management information. If you want to do renewables and smart grids you need analytics. To do analytics, you are, in effect, connecting up to IT, and that is where we genuinely have a skills problem in running IT.

Q42 **Stephen Metcalfe:** We have identified the problem and you have given us some of the potential solutions, but this is a field where we are going to need a continuous pipeline of people to come in to provide us with the security that we need. How do we encourage younger people to consider this as a career? What are the right stepping stones that mean that they do not have to commit too early but they will have the foundations if, at some point, we can attract them into the sector?

Siân John: I will share one of my bugbears. Try to get away from the image of somebody in cyber wearing a hoodie, eating pizza and sitting behind a computer. It is a very varied profession with lots of people with different backgrounds. Some are extremely technical—we have talked about engineering, detection and response capability—but there is also policy-writing and looking at the entire architecture. We need to make people realise that this is a profession, not a job, and there are many different specialisms within that profession.

We quite often push it down the computer science route, which is one route in, but it is not the only one. In fact, the people I work with in cyber range from computer scientists, economists and zoologists to people who left school aged 16 and worked in shipbuilding. There is no core person, so we need to go back and look at what aptitudes we need, rather than particular skillsets. But computer science and engineering will help, particularly in the OT world. We need to make cyber a more endemic part of what we do, increasing cyber-literacy just as we are trying to increase financial literacy. With that will come an understanding that this is not a scary, special thing that people in hoodies do.

Q43 **Stephen Metcalfe:** That is a good point. What is the role, therefore, for industry and Government education? Maybe they are aligned; maybe they are separate.

Siân John: It would be good if the Professor could come in on this as well. The UK has been a very good example of how to do this. Since the national cyber-security strategy and the founding of the National Cyber Security Centre, there have been things like the CyberFirst scheme, the cyber apprenticeships and bootcamps to encourage people to retrain in cyber from other worlds. We probably need to do more connecting between the cyber industry and things such as the IET and the engineering organisations so that, effectively, we basically bake cyber in as something that you learn alongside everything else. It is about demystifying it and making it easier to do. The UK has been a very good example in how to do that, and now, from an industry perspective, we need to step in and help provide those early career opportunities and the ability for people to train on the job.

Q44 **Stephen Metcalfe:** Professor Rashid, do you have anything to add to that?

Professor Rashid: I agree. Over the last 10 to 12 years, we have made huge strides in this country in this area. However, I would also add that

we need to lower the bar about accessing this information and helping people, particularly the young, understand cyber-security. Again, the challenge is how it is seen as an adversarial relationship. I am very aware that many schools, for example, would prohibit learning about what we call ethical hacking. You cannot understand how to defend systems if you do not know how hackers are going to compromise them.

As a result, young people often learn it from other sources. Programmes like CyberFirst are a great way to teach people about what cyber-security can bring but also what their role in this could be. We have to take away some of that mystique. It might sound like a strange thing to say, as a professor of cyber-security, but I really think that we need to change the way we think about cyber-security. We should encourage young people to learn about it from very early on so that they consider where they fit in this picture. They may not become cyber-security professionals, but when they go into their other jobs, this will be embedded in their psyche. It will become part of how they think about things.

Q45 **Stephen Metcalfe:** Where we do want to attract them into the sector, and they want to become specialists in cyber-security, is there an issue around diversity within the sector? If so, is there something we can do to improve that?

Professor Rashid: There is a significant issue with regard to diversity in cyber-security. There is a historical issue with gender balance and lack of women or wider genders in the field. CyberFirst has done an extensive programme of work, with the CyberFirst Girls Competition, but, of course, we need people from more diverse backgrounds to come into cyber-security, not just people from different genders. Therein lies a big challenge because sometimes socioeconomics come into play. There is the usual cliché: "People like me don't do cyber-security."

I lead a doctoral programme and within that we have had quite significant success in improving our gender balance—in fact, we are perfectly balanced—towards more women in the programme, but also in getting people from many diverse backgrounds, including socioeconomic and neurodiverse backgrounds and people with different protected characteristics. This is because of how we talk about cyber-security. There is scientific evidence that women and people from what you would typically consider ethnic minority backgrounds are much more attracted to particular fields if they can see it making a difference to the world. As Siân John said, this is not about hacking for hacking's sake; it is about how we can make a difference to the world. That really makes a difference.

Siân John: There is one area where we are very diverse. As a profession, we have a higher level of neurodiversity than many others. There are certain specialisms, such as security operation centre analysis. These people are trying to detect threats by looking at events and spotting patterns, or trying to do penetration testing or ethical hacking. It tends to

attract fairly neurodiverse individuals, because a very strong level of focus is a good differentiator.

We have wider issues. Cyber is seen as a subset of IT and IT has a diversity issue; cyber takes that to the next level, particularly on social, economic, gender and ethnic diversity. We need to drive that more fully. It is about having more examples of people who are there and using language that is much more engaging for people.

Q46 **Stephen Metcalfe:** You talked about engineers with OT experience. For the record, could you explain what OT is?

Siân John: It is operational technology or industrial control systems. Maybe Professor Rashid is better placed to come in on this. When we talk about cyber-physical systems connecting physical things to the internet—quite often, not the internet but a network—that does not happen magically. What you have is operational technology that connects it. Let us say it is a wind turbine or a medical scanner. There will be the bit that is doing the medical scanning or the wind turbine and effectively it is the operational technology that works it. OT effectively describes the entire ecosystem where that sits.

One characteristic of it is that often you have a piece of equipment that is designed to last 40 years connected to a piece of digital equipment designed to last for five years. That is why we get this legacy. When you get this from the manufacturer, the manufacturer will often say that, if you want to upgrade the PC section of that, it is not stand-alone; you have to upgrade the entire wind turbine, which is on a 40-year investment plan, or you upgrade the PC element. It is not quite a PC; it is more complicated than that. You will upgrade the technology element much less often, and that is why you have legacy operating systems and legacy networks, or what are called protocols. Protocols are used to allow communications that do not allow a lot of the modern security.

Quite often, to avoid fear, uncertainty and doubt we get all scary, but for the past 25 to 30 years as an industry we have been advancing cyber-security capabilities. If you are running 25 year-old Windows XP you do not have the latest Windows 11 security capability sitting in your system, and that is the same whether it is Unix or Windows. That is the reality. Operational technology effectively refers to that big back end. It is sometimes called the industrial internet of things, and industrial control systems tend to be the big elements.

With the increase in connectivity, there are now more sensors and more very lightweight bits of technology that sit at the end in the IT system. It is a bigger element. Therefore, when we talk about OT we probably refer to the entire system, and then you have industrial control systems. Professor Rashid can probably describe that better than I can.

Professor Rashid: You have covered most of it. The term "operational technology" covers a whole suite of things, but the best way to consider

them would be that these are often very simple computer systems that run a pump that drives water or oil through pipelines, or it controls various elements of the power grid.

As Siân John said, they were initially not designed with connectivity in mind, but increasingly, because of business reasons and all sorts of purposes, they are connected.

They were also not designed with security in mind. While security is improving, there are very clear requirements that they have to be simple because you can improve safety properties about them. As a result, often you cannot put state-of-the-art security mechanisms into these kinds of systems.

Not going against my earlier point about fear, uncertainty and doubt, the challenge remains. Professor Martin and Professor Creese said earlier that we have not seen these kinds of catastrophic events come to pass, but it is because of defence in depth. Once an attacker is inside a network that is connected to these systems it is very easy to cause large-scale disruption. It is not a simple case of changing an iPad or phone. A large power grid or water company has a massive number of devices to upgrade and change, but they also have to remain in place for the next 30 years, and today's state of the art is tomorrow's legacy system.

Q47 **Dawn Butler:** When we talk about using old versions of Windows, I cannot help thinking that a Nokia 3310 would probably be more secure than today's phones because it is less hackable. Is that right?

Siân John: Yes, but the irony is that you are trying to connect that Nokia 3310 to the latest Windows or online infrastructure. That is effectively what we are doing in the OT world. A Nokia 3310 was designed to be mobile; it was designed to be connected and have certain approaches around it, whereas a lot of these devices were designed with the thought that they would be sitting in a secure physical location. Therefore, they do not necessarily have the same level of digital security. That is so even for the Nokia 3310. They probably do not even have the ability to put a PIN on many of these; you can just walk up and connect to something.

I am stretching this analogy too far, but the reality is that with a lot of this operational technology and connectivity, for good reasons, if we are to achieve some of our net zero renewable goals, we need to connect up because we need the management information, but effectively we are connecting equipment that is as old as a Nokia 3310 to a modern infrastructure. Therefore, we have to think about having in place the resilience and compensating controls to manage the fact that suddenly you have increased that attack surface. Effectively, if you are then putting in PC systems connected to those control systems and they are out of date, that is an issue.

Q48 **Dawn Butler:** For somebody in a secure environment, what are the

basics you would expect from a mobile phone? What are the basic things you would expect to be on there for security reasons?

Siân John: Take a mobile phone or mobile device. If somebody is walking into a system, there are two sides to this. If you have a mobile phone, it should always be up to date; you should be using multi-factor authentication to log into it. You should have stronger control over that. If it is used for connection to an industrial control system, it should not be used for checking your email or browsing the web because a threat can come in from looking at a consumer site. If you are running, say, a laptop that you are going to connect to an OT environment to do management, that environment should be dedicated to that function. If it has any connectivity, it should be to documentation, call centres or a back-end secure environment. It does not have to be on the premises; it can be the cloud, but it should be secure access only for that use case.

You see a lot of threats coming in where people take effectively what should be privileged workstation secure devices and start checking their email or browsing the internet. That is where a lot of the threats get in. If you use that in any other case you can effectively walk the threat in on your mobile device. It is more likely to be a laptop because quite often that is how they maintain these things. They walk in with a rugged laptop and connect it. It is about making sure it is locked down and it is not a device for checking your email. You have a different device for that. It is designed specifically to manage that infrastructure and should almost be treated as an extension of that infrastructure.

Q49 **Dawn Butler:** Professor Rashid, do you want to add anything?

Professor Rashid: I do not have any more to add.

Q50 **Dawn Butler:** Professor Rashid, you talked about education. I am wondering about pathways into the cyber-threat workforce. Is there a pathway from school where you have bright kids and you think, "Right, they will be good in the cyber-protection space"?

Professor Rashid: I would go back to the earlier comment Siân John made. For cyber-security, we need a diverse range of people from a diverse range of backgrounds. It is definitely a very technical subject and particularly for critical infrastructure we need engineering-based students as well, but there are all sorts of human factors—psychology, how you design systems and so on.

The challenge remains that there is not really a clear pathway as it stands from schools all the way into the profession. That pathway at the moment is largely through GCSE and A-levels in computing. However, there is not a very substantial focus on cyber-security within GCSE and A-level computing. A lot of this work is covered as extracurricular activity where, for example, teachers may have the resources or the time to do this, or through programmes that do incredibly well. I would emphasise something like CyberFirst, which has made a lot of difference in improving awareness, but, unless from very early on in schools young

people see cyber-security as something that is quite integral to society, we will not fix the pipeline. Certainly from my own experience, already we see that at GCSE level the numbers coming generally into computing are in decline compared with other STEM subjects, for example. I speak with confidence only about STEM subjects. Already we are seeing a much narrower pool coming in and, out of that, a much, much narrower pool going towards cyber-security. We are seeing absolutely diminishing numbers coming into the sector.

Q51 **Dawn Butler:** There might be an appeal in being a hoodie and eating pizza. Why is there that decline?

Professor Rashid: I think it is exactly because of the trope that cyber-security people sit in hoodies and eat pizza. The issue is that you are just doing this because this is a kind of geek, nerdy thing to do. I am a self-classified nerd. I do not have any objection to that. However, the key issue is that we need to make sure people understand where cyber-security sits within our everyday lives. In particular, when we talk about critical infrastructure these are not invisible systems; they are systems that bring water and power into our homes. For example, when schoolchildren come into our lab, they are most surprised but also excited by the fact we are working on systems they are familiar with that bring services into their homes. It is the first time they come across the fact that this is something that drives infrastructure every day in society.

We need to change that very early on. If we change that, we will see more people engaging with it. Young people increasingly today—hopefully, always—have a desire to make the world better, but we should start with that rather than saying this is just about somebody in a hoodie.

Siân John: I think the image of a hoodie and eating pizza is seen as having no interest in the wider world, whereas in reality as we go through digital transformation we connect everything. Cyber-security is about making the world a safer place and connecting with that. We need to make people realise that you can wear a hoodie and eat pizza—I have been known to do both those things—but you are doing that while trying to make the world a safer place, not sitting behind your computer never talking to anybody and trying to break the world, which comes with that image.

Q52 **Dawn Butler:** That is where ethical hacking comes in.

Siân John: Yes, but even with ethical hacking, if you are breaking it, you are helping to find the vulnerabilities that you then report to the manufacturer so they can fix them.

Dawn Butler: That is really fascinating. It is a bit like politics. It is about making sure everyone knows that it is injected into everything that you do.

Q53 **Tracey Crouch:** You mentioned earlier youngsters growing up in the digital age. Rather than skills and training, do you think that the

curriculum, particularly at primary level, is geared very much towards literacy? My son is in year 3 and has just started coding. It feels like a very good place to start. Do you think there is enough there already for that, or could it be improved?

Siân John: There is some there, but there is more we can do. In the past 10 years we have had a lot more coding in primary schools, but there are things like online literacy and digital literacy. The fact is that those now in primary school will be spending their entire lives surrounded by technology, so it needs to be as core to what you do as history. Coding is one element of it, but it is about securely using the internet and connecting your device, literacy and the whole element. There is more we could be doing in that area.

Q54 **Tracey Crouch:** Do you think that would help in connecting switches and PlayStations into the online community, the chat and all that sort of stuff?

Siân John: Yes, and it is about being aware when something risky might be happening so you can make that decision.

Going beyond school, when you work in the industry or you are on a board, you think about the risks and threats that come with these things. If you are digitally literate you become more aware of what the threat might be, as well as the opportunity.

Q55 **Tracey Crouch:** In response to that, you can have a situation where children are more literate in these things than their parents. How do we forge that gap?

Siân John: We need to do some awareness for adults as well as children. Letting the children fix the technology is not where you should be.

Q56 **Chair:** Who should do that—the schools?

Siân John: It is obviously about education. For adults, it is probably a combination of Government initiatives and private sector initiatives, but it will probably be mostly Government educating people.

In the workplace, a lot of education is happening around IT and cyber-literacy to make sure people are more secure online. That should be as much about talking about how you secure your home environment as your work environment, particularly in the era of hybrid working where your home environment quite often is your work environment. That will make us better in that the people sitting on boards will better understand the risk.

Chair: The Committee has to be in the Chamber to ask questions of the Secretary of State about these issues and others. Siân John and Professor Rashid, thank you very much indeed for your evidence today. You and our earlier panel of witnesses have got our inquiry off to a flying start.