HOUSE OF COMMONS

Digital, Culture, Media and Sport Committee

Oral evidence: Connected tech: smart or sinister?, HC 157

Tuesday 11 October 2022

Ordered by the House of Commons to be published on 11 October 2022.

Watch the meeting

Members present: Julian Knight (Chair); Kevin Brennan; Steve Brine; Clive Efford; Damian Green; Dr Rupa Huq; John Nicolson; Giles Watling.

Questions 69-146

Witnesses

I: Matt Lewis, Research Director, NCC Group; Professor George Loukas, Professor of Cyber Security, University of Greenwich; and Simon Moore, Director of Strategic Engagement, Palo Alto Networks.

Examination of witnesses

Witnesses: Matt Lewis, Professor George Loukas and Simon Moore.

Chair: This is the latest Digital, Culture, Media and Sport Committee hearing on connected tech. We are joined today by Matt Lewis, Research Director at the NCC Group; Professor George Loukas, Professor of Cyber Security at the University of Greenwich; and Simon Moore, Director of Strategic Engagement at the Palo Alto Networks. Matt Lewis, Professor Loukas and Simon Moore, thank you very much for joining us.

Before we begin, it is beholden on me to ask Members whether they have any interests to declare. I declare that I am the chair of the all-party parliamentary group on new and advanced technologies. Does anyone else have any declarations to make? Fine. Our first question will come from John Nicolson.

Q69 **John Nicolson:** Good morning. I will start with you, Mr Moore. How do we know whether our connected tech has been hacked?

Simon Moore: That is an exceptional question. We were talking about that earlier. Clearly, there are a lot of different types of OT, but if we talk about it generically—I am stealing the professor's point actually—it is really hard to identify it because there is no telemetry, and there are not that many indicators on the box. It is not like your PC or even your phone, which will give you an alert.

Q70 **John Nicolson:** So it is pretty much impossible for us as private individuals to know. Recently, I went to a tech briefing in Finland, given by someone who briefs the Finnish military on this subject and who has written multiple books about it. He said that a very basic thing all of us can do is to allow the battery to run down on our equipment—that helps. If we have already been hacked, that might help to de-hack us—

Simon Moore: Effectively a hardware reset, putting it back to a known and trusted state.

Q71 **John Nicolson:** That is interesting. What about ransomware, Professor Loukas? That is increasingly a problem for lots of different institutions, isn't it? I understand that sometimes tech people might find themselves working on particular projects without realising that they have been recruited by ransomware companies that are in the process of demanding large ransoms from the target of their attack.

Professor Loukas: Ransomware are very common, and possibly the most common in conventional computing. They have significant downloads across the whole industry, but in connected devices, we have not yet seen outside the lab any ransomware—

John Nicolson: Outside where?

Professor Loukas: Outside laboratories. You can see that in research—there are recent papers on how it can be done—but for the time being we have not seen it in the wild. In my estimation, it is not yet economically meaningful, because ransomware is about compromising something that is very important to you—the victim, let us say—so there is a point in you paying for it. When it is about a single device—when it is about internet of things-connected devices—most of them are not that important individually or in isolation so that it is worth paying for them.

If we are talking about large deployments—for example in industrial internet of things systems, manufacturing or areas like that—then ransomware will make economic sense, so we will see them in the future. For a smart home or something in smaller deployment, they do not make sense at the moment.

John Nicolson: Mr Moore has his hand up.

Simon Moore: Something that I think we will come back to during our session is the threat. The threat to OT that would concern me most—because they are generally quite simple devices that do one thing, or a simple subset of things—is not necessarily a ransomware one directly, but if a device is compromised and that then allows it to be used to attack the rest of the equipment in your household. For example, if you have something like an Alexa device, it is not that it is listening to what you are saying, because most of the time there is no information in that, but that it is being compromised and that might allow it to hack inside your network, inside your firewall, to attack your PCs and your iPads, and to get your passwords. That becomes a much more successful threat factor.

Q72 **John Nicolson:** Who, at the moment, is the target of those trying to collect ransoms? Big institutions?

Simon Moore: The threat of what, sorry?

John Nicolson: Who, at the moment, is the target of those malicious actors who are trying to collect ransoms? We have heard that it is not individuals. Is it big institutions like the national health service, which we know has come under attack?

Simon Moore: My personal view is that it is more random than that. Basically, they go fishing—looking—for someone who has a known vulnerability. To take OT, for example, if you have bought a baby camera or nursery camera that has a breach on it, they will go looking for it. They will look across the entire market—the entire globe—and when they have found it, they will go, "Right, that is my pivoting point."

Q73 **John Nicolson:** Let me ask a very naive question. Why is it that I sometimes see popping up among the adverts on my iPad lots of things that are directly connected with me? For example, I am getting a lot of arthritis cures at the moment, even though I am obviously in the prime of middle youth, so I don't know why they would associate me with arthritis. To the best of my knowledge, I have never googled arthritis, so how is that happening? Is it just coincidence, or am I just not noticing all the

adverts that are not targeted at me and just happen to be noticing the things I don't know about arthritis, about politics, about house restoration—things I am interested in? Do I just happen to notice that or am I being watched and listened to, and my messages read?

Professor Loukas: To some extent, you are watched. You have a profile because of your general use of the internet, which might correlate from an artificial intelligence perspective with you possibly having arthritis, for example. It might be the age group, it might be the location, it might be other aspects, so even if you have never searched for a particular term, the data exchange between companies will be such that someone who will do the artificial intelligence analysis of that might think that this will be a possible advert for you. It is not that targeted, but it is targeted enough, let's say.

Q74 **John Nicolson:** Okay. Mr Lewis, who are the main hostile actors at the moment? Who is the biggest threat, and how is that threat manifested?

Matt Lewis: It is quite a mix, and it depends on the motives of the threat actors and what they are going after. The mix is that there are nation state intrusions—we are all quite familiar with those now—where they will typically be after intelligence about whatever businesses or countries are doing. They tend to be quite stealthy, multi-year campaigns where they have levels of intrusion to get that information for whatever purpose they want to use it for. You then have organised crime, which is typically behind ransomware attacks. That is where it monetises the vulnerabilities that it is exploiting in various networks and systems.

Having said that, we also know that, through groups like Lazarus and others, some nation states—North Korea—have been attributed with ransomware attacks where they use those as a legitimate means of financial gain. A lot of that is becoming easier to do with the prevalence of cryptocurrencies—anonymised currencies that allow for the transfer of funds—which are difficult to attribute or trace back.

We even have what we might call the bedroom hackers, or the script kiddies, who, for whatever reason—just out of fun or for curiosity—can cause sometimes quite significant damage going after certain organisations when they find a loophole, manage to identify a data breach, and maybe publicly dump that and expose the business in the process.

Q75 **John Nicolson:** Finally from me, how can we all protect ourselves—as individuals round the table, as viewers, as voters such as our constituents watching this, and as bigger bodies, which might find themselves subject to ransomware attacks?

Matt Lewis: For ransomware specifically, at the user level there is still a fair amount of space for user education, so I hope that businesses can provide training and awareness on what ransomware is and how to instil a security culture in an organisation, so people know how to report possible suspicious behaviour. There are things that organisations can do technically to mitigate the risk of ransomware, a classic one being back-ups. In our world, we have seen that, typically, businesses can't recover

from a ransomware attack because they have back-ups that are vulnerable, or they are architecturally vulnerable, and their back-up system has been on the same system that was compromised by the ransomware attack. There are a few things that businesses could do to educate and inform users.

Things are a bit more difficult in the domestic space. Not everyone is technical. There is a lot to understand and learn, so again, ideally—

Q76 **John Nicolson:** Give us one top tip.

Matt Lewis: Passwords. If I may offer a second: patching and updating. As and when there are security updates available, apply them immediately, but choosing strong passwords is key.

Q77 **Giles Watling:** Everybody uses an exclamation mark, don't they, at the end of their passwords? It's a sort of universal truth—

Simon Moore: Or a hash.

Q78 **Giles Watling:** Yes, they do, apparently. I am so glad we have you chaps here because you can put to bed an urban myth—or not, as the case may be—following Mr Nicolson's questions. Are our devices listening to us—our Amazon Echoes, or whatever they are? Are they listening to us at all times?

Simon Moore: By definition, an Amazon Echo is listening to you because it is trying to get your wake word. So, by definition, it is.

Q79 **Giles Watling:** Outside the wake word, is it listening to us?

Simon Moore: Which hits the earlier question, are they listening and hearing? I said something about a new watch and suddenly I get new watch adverts. I can't comment on that authoritatively.

Q80 **Giles Watling:** So this urban myth could continue.

Professor Loukas: No, it is not an urban myth. They do watch; to what extent, we are not certain. They have admitted to that in public, so we know it happens. We know there have been cases where employees and companies actively listen to information. We do not know the extent, again.

Q81 **Giles Watling:** What inquiries are going on to find the extent of that, because this is intrusion into personal lives, isn't it?

Professor Loukas: I am not aware of the inquiries.

Q82 **Giles Watling:** Fair enough. Thank you very much. You might not have answered the question entirely, so the urban myth will continue—or not, as the case may be—but thank you very much for that.

I have a whole pile of statistics here that say that cyber-crime has been on the rise for many years. Is it getting easier to become a cyber-criminal in this day and age? I think that goes to Mr Moore.

Simon Moore: I would say yes, because the organised crime bodies are setting themselves up to sell services, and I think this will continue going forward. They will have help desks and things. You may want to become a hacker yourself, say, wherever you are at in life, and you can go and get help to enable you to do that and pay services. Because of this industrialisation, I think it is going to become easier to do, including the packaging of attack kits.

Q83 **Giles Watling:** So it is easier to, if you like, google "How do I hack?" and you will get an answer and get guided through it. You do not need specialist knowledge.

Simon Moore: You could google today "How to hack a BT home hub", for example. That is out there.

Q84 **Giles Watling:** What should we do about that? How can we legislate? How can we stop that from happening?

Simon Moore: The trouble with the legislative approach is that you are always going to be reactive and chasing the latest thing. It goes back to your question about whether we are we being listened to, in that even if we are not being listened to today, it is a threat, right? Whether a device is deliberately compromised to listen to you or it is built into a company's product, the capability is there, so what do you do about that?

My view from a networking perspective is that you can look for evidence of that in the flows of traffic that go in and out of your house or your business. We need to find a way of reacting to it, because it is a truth that is with us forever, isn't it? Pandora's box is opened, if you like, and there will be a continuing stream of new attacks coming at us. If we are constantly legislating for the last one, we are not really looking at what is coming next.

Q85 **Giles Watling:** Absolutely. That comes to my next point, which is that it appears to me that the Government are always behind the curve, but that will always be the case because the technological innovation will happen independently outside of Government, and then Government will always be playing catch-up. What I am trying to ask here is how Government or legislation can get ahead of the curve.

Simon Moore: Potentially through support services. For example, we all go through an internet service provider such as BT or others. If they can be supported to provide services to the people who connect to them, they are in the ideal place to be able to see traffic going in and out and therefore whether it has been compromised or not.

Q86 **Giles Watling:** Do you think that periods of anxiety like the current energy crisis make businesses specifically more vulnerable or more likely to be attacked? Do you think the fact that we have a crisis and that people are looking for ways out—for help—makes them more vulnerable?

Simon Moore: I don't think any more than anything else. If you are alluding to honeypot attacks where people go, "I need to find something", it could equally be, "Who's out on 'Strictly Come Dancing'?" You can get

carrots of all sorts of types, and that method has been used for some time.

Q87 **Giles Watling:** We have the Product Security and Telecommunications Infrastructure Bill coming up. Do you think that will make connected tech more cyber-secure, or are there ways that the framework could be improved?

Simon Moore: I am not aware of the contents, I'm afraid.

Professor Loukas: I have read the Bill. As a Bill, yes, it will make a big difference, but it has a specific characteristic, which is that its success will depend on the requirements that it refers to. The Bill talks about requirements—about the power to set requirements and enforce them. There are three requirements, as far as I know, that are now being considered, and they are perfectly meaningful. They talk about passwords, they talk about patch management—I don't remember the third one, but they are perfectly meaningful. The question is what we do beyond those three, how the Bill will actually be implemented and what requirements will be set that the Bill would relate to.

My main point is that, up to now, they lack the relevance of the human. The requirements are all about the device itself: they talk about how it will enforce this with that, but they do not talk at all about the relevance to the user—to the human. In practice, we know that this is a major weakness in cyber-security. I say that because in the vast majority of actual cyber-security breaches in the real world, there is an element of human deception—in almost all cases. If you receive a phishing email, for example, one out of three people, let's say, will click on that email, go to a website and be infected with malware, or they might be deceived into thinking, "This is the legitimate Cabinet Office website. Let me put in my credentials to log in." That is how most of the attacks happen in the real world. In the real world it is not about a super-hacker finding an amazing vulnerability and sneaking in, like we see in the movies. In reality, most people will make a mistake once in a while—even a professor of cyber-security will make mistakes, let alone a lay person. As a result, there will be an intrusion in their system, which will then escalate into something much worse.

This is the point at which connected devices are actually very different to conventional computing. As was mentioned earlier, in conventional computing, when you have an email you can check the address. You know the context—for example, "Was I expecting an email today?" Or you have been to this website before and it looks a bit different. That is not the case with connected devices. If you ask any person whose connected device has been hacked in the last few years, they will say they have googled for an answer—"What do I do now?", "How do I prevent this from happening again?" or "What do I do the moment it is hacked?"—and they will all say that they can find no information online that they can actually act upon. There is a lot of information, but no information you can actually act upon. That is the big difference.

The NCC, for example, is recommending cyber-hygiene measures. They are very meaningful, but they are mainly for protecting the network or for the manufacturer to design the product securely. The actual human user asks, "What do I do now? My thermostat is switched off and I am cold. How do I stop this?"

Q88 **Giles Watling:** Precisely. So you are saying it is about education?

Professor Loukas: It is about education, but education is limited at the moment, because you do not have the basic research to know what to teach people. The manufacturers do not say anything about their products. If you see how they sell their products, they say they are secure, but they do not say what they are secure against. They do not say what the cyber-risk is. The assumption is, "We have done what we are meant to do from our side as manufacturers. They are secure to an extent, and you have to believe us, because we do not even tell you what they are secure against. If something happens, I am sorry but you are responsible for your own protection." This is the main problem we see at the moment with connected devices.

Q89 **Giles Watling:** So it is caveat emptor. As far as you are concerned, the Product Security and Telecommunications Infrastructure Bill leaves out the human aspect?

Professor Loukas: Not the Bill itself, because the Bill is open to the requirements it will enforce. The requirements that are currently recommended do not have that, and they are outside the Bill.

Q90 **Giles Watling:** Thank you. I have one more point on the Bill. It mandates that manufacturers must monitor data, keep software updated and so on, but at some point manufacturers will need to discontinue their product and they will not continue to update it. How do we get around that?

Professor Loukas: There is a bigger problem, which is that they do not tell the users how to safely dispose of their systems. That would be the first thing they could do. If it is impossible somehow to legislate to keep supporting a product—which might be impossible—at the very least they can say how we can get rid of a product when it is no longer supported, and they do not do that.

Giles Watling: Thank you.

Q91 **Chair:** Mr Lewis, how can you be truly connected and yet retain your privacy?

Matt Lewis: It can be difficult. It is a symptom of the connected world that there is so much connectivity of privacy-impacting technology as we go about our daily lives. We have everything from wearable fitness trackers capturing and transmitting data through to CCTV and lots of connected doorbells. There are lots of devices capturing video imagery and audio, maybe in conjunction with facial recognition. It is a symptom of where we are at in society and in the connected world. The best we can hope for is that we have regulations and legislation to ensure that products and systems are secure, that people are only capturing data in

line with data-protection guidelines, and ideally that users have the option to opt out, in terms of privacy controls. I guess that is where we have to go. We have to use legislative and regulatory tools to try to minimise the impact of the privacy-impacting world that we currently live in.

Q92 **Chair:** If you do engage in these opt-out options, are you therefore not, by definition, less connected?

Matt Lewis: Conceivably, yes. That is how it should work. The less a company is capturing about you, the less it will know about you and be able to profile you. So, in theory, yes.

Q93 **Chair:** But it also means that you do not benefit from that connection as a result.

Matt Lewis: That is correct. Equally, if we think about privacy in the context of audio and visuals, how does one consent to, or withdraw consent, in a smart city? You are walking around and are going to be captured on video. Even if there is no identifier of you, that is happening. Those are interesting things that we need to unpick and understand as a society.

Q94 **Chair:** The picture that I have is not of any deliberate push in order to effect something that is quite sinister. It is almost something we are falling into as a society. Years ago, the film "Minority Report" showed how an advert would be directly related to you, as you walked in the street. In the same way, now in your car, you can say a name and it will come up and go, "What do you want?" There's that sort of thing and you go, "What are you up to?"

In that same way, we are effectively sleepwalking a bit in society, and there seems to be no restraint. Is there any risk that, not just a hacker, but someone or some group wishing to control society, by controlling that information and accessing and learning how to use it, can effectively bring about major societal change?

Matt Lewis: The sinister aspect here is the emerging cyber-physical world. For example, in smart cities a lot of actuators cause movement or physical things to happen, which, if they went wrong, could cause harm. We have seen examples with the Colonial gas and oil pipeline in the US last year, where a ransomware attack physically inhibited the actions of the pipeline.

You could conceivably think of things such as automated traffic lights. If they suddenly fail, you could have accidents. If autonomous vehicles are compromised, they might be controlled and used as some sort of asymmetric warfare, whatever. The cyber-physical world is quite a concern.

If I may jump back to the provisions in the PSTI Bill, while it is good at the product level, what we are seeing in the connected world is maybe a lack of insight and governance around the connected world itself, the thing in its entirety.

A good example would be CCTV cameras and IOT cameras. You could make a really secure product that does that really well, and enforces all its security functions, but it might be transmitting the video feeds up to a cloud server, which is completely open. You don't necessarily have to compromise the device to get access to the information. You might be able to compromise another connected aspect of that technical ecosystem.

That's what we really need to be thinking about in the connected society. Yes, product security is important, but we also need to think about those products in the context of the deeper, wider systems, in which they interoperate.

Q95 **Chair:** How does it interact with what is commonly termed the metaverse?

Matt Lewis: The metaverse is a term that industry is still trying work out what it is, other than a lot of virtual and augmented reality. It is still early days to understand a lot of the security implications of the metaverse. We are unfortunately seeing a lot of stuff in a world of cyber-bullying, in various online forums that people go into. I am certain that there is a lot to unpick there.

From a cyber-security perspective, again, these are devices that will be privacy impacting. They will have audio-capture devices. I guess they fall into the same domain of how we need to consider securing these as products.

Q96 **Dr Huq:** I want to ask about tech abuse, which we looked at in our previous sessions on this subject. That is when domestic and/or sexual abuse can be perpetrated using some of the capabilities of connected devices.

Is there an argument that it is often aided and abetted by things such as security flaws that are there to be exploited, or the ability of perpetrators to bypass security altogether? Are there technical or design solutions that could be built in to stop this problem?

Professor Loukas: Tech-assisted abuse at home is common nowadays, which is a problem because support workers do not know how to deal with it. There is very little cyber-security breach actually happening, unless we consider the insider as a security threat. In practice, the technology used is surveillance apps, for example. In terms of connected devices, it is the device itself and the fact that the abuser has access to the same device, if they live in the same household. For example, looking at the history of audio commands on an Amazon Echo is enough to see what was discussed and requested. It is quite difficult to see from a cyber-security perspective, because even if you have the strongest kind of cyber-security in place, it is not that meaningful if the person who will be the abuser already has access to it.

Of course, there are some cases where cyber-security can be useful. One is multi-factor authentication if we assume that the person who is abused can have different access from the abuser in this case. The second would

be something like software that detects if there is a surveillance app installed. I would not see it as a traditional cyber-security problem. I think it is to do more with the digital literacy of the people involved. If there is a significant disparity between the digital literacy of the persons involved, you might have someone who is exploiting access to the app while the other person does not know that the app is collecting the data. In that sense, it is matter of transparency as to what data is collected by an app at the point of deploying it. How do you enforce that in a household?

Simon Moore: I think it is worth differentiating. There are several technologies that we are moving across here. Matt covered that when we talk about the cloud for example. From an operational technology—OT—perspective, they tend to be fairly simple and straightforward, as you mentioned, which is why they are hard to monitor. For them to be subverted in this way is a bit more complicated. Take my Hive home cameras for example—they have stopped doing them now, but people have known they existed. That control is down to password. It is on some private wi-fi network. It becomes hard for an external person to mess with that.

If we then talk about multi-purpose devices such as phones, which is where a lot this would sit, it is about the app domain and it becomes a lot more difficult. If an abusive partner makes you share a password and they put an app on that, they can track you. That's not a cyber problem as such, but technology being misused. Then you have the data in the cloud in terms of whether that is misused.

One of the things that previous questions were looking at is relying on trust, almost on an escrow basis, in the person who is providing that service or looking after that data on your behalf. Take ANPR, for example, looked after by the Government—data on where I am travelling to and from in my car in very granular detail. If that were to be compromised in the most sinister method by a hostile country, they would be able to build a digital twin that has no controls over it. That digital twinning idea is something we use in a lot of domains, but it could be used not just for transformation and improvement but for abuse.

Matt Lewis: I agree with my industry colleagues, and I don't really have too much to add, other than that there is a lot of technology in the internet of things space. Unfortunately, the old adage is that anything that can be used can be misused. That is not really a cyber-security issue per se but how people can understand how they can abuse certain technologies. A fairly recent example was the Apple AirTag, which allowed you to tag on to luggage or whatever to track, but people cottoned on that they could use that to do physical real-world stalking. It becomes less of a cyber-security issue, or not something that we can solve in cyber-security, but how we understand the use of technology and what the pitfalls could be.

Q97 **Dr Huq:** The evidence we have heard points to the fact that it is about exploiting victims' or survivors' lack of understanding of the technology. Professor Loukas, you alluded to digital literacy and the fact that people

might put on child controls and those kinds of things, which are well intentioned, but then they end up, in a stalker type of fashion, as the victim. Is the security of connected devices dependent on the digital literacy of the person targeted? How would you get over that? How do we build that into the curriculum so that people are aware? Do we need a Government awareness campaign? What could we do?

Professor Loukas: There are two directions that you can follow. One is on the education front—purely on the curriculum and what kids are taught at school. At the moment, cyber-security is kind of covered in schools, but not really at the level of IOT security—internet of things security. What is covered is, for example, social media passwords. At six or seven years old, kids already know about passwords and have some idea of how they should behave in relation with them, but they have been interacting with internet of things devices and connected devices since they were babies.

Most kids who are born in a household with an Amazon Echo interact with it. They are monitored by a baby camera or a normal smart camera, they watch smart TV, and they are in the same room as smart sensors of any kind, so they are already interacting with smart devices. From that perspective, education is far behind when it comes to IOT security and what they should expect. At the very least, they should expect that when they do not need to use the Amazon Echo smart speaker or Google Home, it should be switched off. There is a nice little red button on top of it, which means that it is no longer listening to you. That is something that they can learn, but it is not mentioned at all in schools. From the perspective of education, simply making users—kids—aware of the basic threats and cyber-risks would make a big difference.

The other side is the manufacturer, as it is impossible to figure out whether the devices that they produce are under attack. It is impossible almost by design, because seamless design is now preferred in connected devices for reasons of practicality—they look nice if there is no display but maybe a little light and a little sound, so they are more attractive to buy. In that way, there is almost a clue as to whether they are behaving correctly or not.

In our research, every time we have worked with connected devices, we have seen that users, even if you tell them to look out for cyber-attacks and the types of cyber-attacks that they might observe, misattribute them simply to the device playing up again. So manufacturers do their best to hide the cyber-risks and do not even explain in their manuals what fault one can expect. When you buy a washing machine, there is a page at the back that says, "If you see this error code, do that. If you see that, call this person." For IOT devices, if there is a manual, there is not a single reference to cyber-risks, so a human is not able to protect themselves.

Q98 **Dr Huq:** Simon Moore and Matt Lewis, how can we mitigate the lack of digital literacy, given that some vulnerable people are outside the school curriculum?

Simon Moore: I would come at it from a slightly different angle, given my personal experience. I am the IT expert for my parents and mother-in-law. Their literacy is very low, and it is worrying. As they get older and frailer, they don't want to know how these things work, and yet they are—I wouldn't necessarily use the word "sleepwalked"—encouraged to use more online devices. There are fewer banks, so they use online banking.

Online banking shows a path of how it might be done, in that it is a trusted environment. We could train our vulnerable users only to use trusted services—that might be reviewed and commented on, perhaps at a governmental level—so that they know what to trust and are given that advice to start with. When you log on to a bank, it makes this clear: "Are you sure you want to move this money? Have you done x, y and z before you move the money?" It gives you really simple steps and assumes that you are not educated when you are taking those steps and making those actions. There is a space for a service middle layer to help people, and if you decide to go outside that, it is on you.

Matt Lewis: Just to add from a cyber-security literacy perspective, the National Cyber Security Centre has some amazing initiatives, and we and industry are involved in those—schemes like CyberFirst, which gets young people interested in cyber. They run a number of summer schools. We pay a few bursaries for students as they progress through to higher education, and they do lots of work placements and so on. While the medium-term goal is to get these young people into cyber-security with that level of digital and cyber-literacy, I think we will start seeing the benefits within the next five years. That is a double win, because it is both digital and understanding of security and cyber-concepts.

Q99 **Steve Brine:** Good morning and thank you for coming in; it is appreciated. I want to explore a little bit with you how we are doing against the national cyber strategy and how the Department and the Ministers, who have obviously just changed, are doing. I would be interested to know your interactions with the previous ministerial team and any interactions you have had so far with the new ministerial team. How do you think we are doing in facilitating homegrown businesses? I will probably ask Professor Loukas in the first instance, because obviously you are a homegrown business, Mr Lewis. How do you think we are doing, Professor Loukas, in facilitating homegrown businesses to develop the technologies that help us meet the pillars in the national cyber strategy?

Professor Loukas: There is a lot of support—for example, for start-ups. There is a lot of support for innovation in general. If there is something that is very characteristic of the UK, it is that we are doing very well in terms of supporting early phases of development in cyber-security, and the innovation and new technologies that will be used for cyber-security in the future make a lot of sense. From an economic perspective, this is really excellent, but from the perspective of the average person—the average user or average human who might be the victim of a cyber-attack or who is vulnerable in general—I don't know to what extent they can see the initiatives. I don't know to what extent they can see the work by

NCSC. I don't know to what extent it reaches them. For Simon's mum, for example, I don't know if she would have ever come across the help that exists. That is my general view. In terms of developing new capabilities, we are excellent; in terms of these capabilities having an impact on the more vulnerable people, I am not so sure.

Q100 **Steve Brine:** Obviously I am interested in the front-end user as a constituency MP, but let's put that to one side for a minute. As a Select Committee, we are interested in scrutinising how Ministers are doing against the strategies that they have published and the policies that they have set. With particular reference to the national cyber strategy, are we focusing on businesses that develop the tech? Is that too narrow? Should we also be looking at the consultants, the research and the academics? How are we doing on meeting what we have set out as a Government—the pillars of the national cyber strategy?

Professor Loukas: I have not seen any weakness there in terms of what was promised.

Steve Brine: Mr Lewis?

Matt Lewis: We work a lot with the National Cyber Security Centre, and we see a lot of that policy being enacted through them. There are a number of things, including their provision of routine threat intelligence about emerging threats in different domains and affecting different technologies and, as I just mentioned, their initiatives for schooling and getting people into cyber. At a national level, they were very successful in blocking certain types of fraud and email fraud through changes they made systemically across UK Government systems or around the work and pension scams that we used to see a few years ago. They have pretty much quashed those types of issues or made it very difficult for attackers to mount attacks. That is probably mostly what I would say. We see a lot of good stuff coming from them, in addition to a lot of free advice and guidance to businesses and consumers. The NCSC website is very rich, with a lot of information. I think they go above and beyond by working not just with critical national infrastructure, which is obviously a key element of their remit, but with UK plc more broadly.

Simon Moore: I would absolutely agree with that. They have really stepped up to helping the country as a whole—UK plc. Matt is right to say it is really good. Having tried to run a small business, I would point to the professor's point earlier about SMEs—not just my mother, who would hate being brought up in this environment. You can take a horse to water, but sometimes you cannot make them drink, and the trouble with the security things that a business needs to do is that they are a cost to the business. We perhaps need to make that slightly easier, but it is an educational thing again. We are back to people.

Q101 **Steve Brine:** Yes. One of the key pillars of the cyber strategy—pillar 3—talks about securing the next generation of connected tech and mitigating the risks of foreign suppliers coming into that. We will come on to talk about Huawei later, but do you have any words about the next gen?

Simon Moore: There are so many threats coming up now. If we look back 20 or 30 years, the first firewall was a fantastic step forward in the fight against cyber-crime. Every time there is a new threat, there is a new silver bullet, but each time the impact of that silver bullet is becoming less and less. There are now so many products and services globally that a user can go and buy. For me, it is becoming an operational problem. It again comes back to the human element. How do you tie all those technologies together usefully? How do you keep them patched? How do you keep the passwords controlled? How do you make sure that people use them properly?

On the next generation of threats, you could deal with all the things you have got today. Exactly as Professor Loukas said, quite often they don't come in through the front door—they don't hack your firewall any more. They just talk to you socially and work out your passwords and other data. Look at some of the security questions that you get asked when people ring you up. They go: "What is your date of birth? What is your address and your postcode?" They are standard questions. Those are openly available. That has to get better. That is an operational problem, not a technology problem.

Matt Lewis: Broadly, I always like to relay the point about security being a process and not a solution. We will always see the need to monitor and react to the emerging tech landscape and the threat landscape. It is always going to be evolving. I get a sense that because of the connected world as it is now, and the level of vulnerability that we see, we feel a bit overwhelmed and like we are possibly missing some things—maybe we are, but these conversations are probably going to be ever more common in terms of managing the security process, which will be constantly evolving.

In terms of emerging tech, there is something I would like to add. It is not necessarily just about new equipment developed with new techniques. A lot of the connected world that is being enabled by new technology is actually bridging and connecting older legacy systems. They become part of the process. Therein lies, typically, vulnerability. We need to be careful as a nation about how we do that securely. There should be some advice and guidance where necessary for that and maybe even some provisions within legislation for how businesses can and should safely connect possible vulnerable legacy systems and/or at least an agreed timeline for secure decommission of those vulnerable legacy systems.

Q102 **Steve Brine:** Do you want to expand on that? We are interested in writing a report, obviously, that could be used by Ministers for the production of legislation. That is ultimately what we do, as a legislature. Can you expand on that? What would you suggest?

Matt Lewis: Take an example in operation technology, particularly in the energy sector; there is lots of older technology that runs water stations or energy-based systems. The connected world and the need to get access to data telemetry from those systems is appealing enough to open it up, to aggregate it, and to maybe use that data in AI models to learn new

insights about the data that those old systems capture. But in doing that, you are opening up the vulnerability. You are exposing it. What we would hope is that there can be some provisions whereby where that is happening, particularly in a critical national infrastructure scenario, there are agreed timelines for how the older legacy systems will be decommissioned, or at least the assurances that can be put in place for opening them up to a wider internet-type connectivity.

Q103 **Steve Brine:** Okay. Finally, what do you think the biggest misconception within the Government is when it comes to the resilience of cyber?

Simon Moore: Resilience is a big word—it can mean a lot. Well, the biggest misconception—

Steve Brine: I mean, does it matter that the Ministers have changed and we have another Culture Secretary, because ultimately the system carries on?

Simon Moore: I will start my answer by going back to the point we made either. It is too rear-view mirror-focused, as opposed to forward focused. The reason resilience is a big word is because it is almost a paradigm shift in how you behave. You go, let's say: "I am prepared to accept a breach, because I am going to fix it very quickly or I will limit the impact of that breach—I will have smaller datasets." There are lots of comments that we have picked up. I think you asked about privacy and connected data. One of the things that we can do to address that—in a resilient manner as an individual—is to start compartmentalising what your data is and what you are going to share with whom.

It is not just making it open. At the moment, we have it very flat. Take a password keeper, for example; if I am going to something like a coffee shop, I have a standard password that I use all the time because I know I am going to go straight to VPN—it will be encrypted—and I therefore don't care too much if that password gets compromised. I am limiting what data that coffee shop will have about me. If it is my bank account details, it is in a completely different league of risk. That is part of the resilience problem. It is about compartmentalising and dealing appropriately with each risk type.

Matt Lewis: In terms of what might be missing or misunderstood, there might still be a broad assumption that where legislation regulation dictates certain requirements, those will actually get enacted. What might be missing is some sort of mandated independent third-party validation of security products systems, because that is when you get the evidential piece about where maybe the developer or manufacturer did make assumptions about the security—

Simon Moore: Like the old kitemark, perhaps.

Matt Lewis: Yes. There are various certification schemes available for various types of IOT device, and having some sort of guidance to push manufacturers through that so that they get that independent validation of the systems that they are developing would be good.

Q104 **Steve Brine:** I know that we care and I know that you care, but do you think most people care? There is a chance when you get on an aeroplane that something might go horribly wrong, although it is unlikely. There is a chance, but people still fly. Ultimately, tech makes our lives easier and better, so is it just a risk that people take? Yes, they probably do have silly passwords with exclamation marks at the end, but life is a risk, isn't it?

Professor Loukas: Absolutely, it is a risk. That is very important. Cyber-security, if you boil it down to what it actually is, is a risk-management process. There is no doubt that people take risks in many cases. What there is a doubt about is whether they know the level of risk. With social media, for example, we have some idea about the level of risk. We have heard so many things, and we interact. Most people—most parents, even—will know, for example, how to advise their kids on social media. With emails and websites, we have some experience by now. It has been decades, and we know what might look okay and what might not look okay.

When it comes to connecting to devices, in all our research and in research that we have seen from other universities, people do not know the risks. They simply do not know the risks. They either choose to ignore them because it is often convenient to ignore risks, or they exaggerate risks. They might consider a completely different risk. Something that has never happened, for example, is a serious risk, and they might not consider something that is happening every day. The big change happens the moment you are hacked or when someone you know is hacked.

A researcher in my team a few months ago told me that she needed help with her response to her internet provider, because the internet provider emailed her to say that they needed her to turn off her network connection because she was using too much internet, and that must be the result of a new device that she has purchased and which has now been compromised and used in an attack against someone else—against a third party—and as a result she is consuming a lot of internet, a lot of bandwidth. She is not a computer scientist, so for her it was a shocking realisation that although none of her data has likely been hacked and none of her devices misused from her perspective, it has been misused by a third party, so now she is left, according to the attitude of the internet provider, to somehow figure out what has happened, identify the right device that is doing this, disconnect it, report it accordingly and so on—things that she has no idea how to do.

Chair: Thank you. Damian Green next.

Q105 **Damian Green:** Can I break the rules for 30 seconds and help to answer one of the very good questions that Mr Brine asked, which was what is the biggest misconception inside Government? I don't think it is a misconception problem; it is a lack of interest at the political level. I used to be responsible for cyber-resilience in Whitehall in one of my ministerial jobs, and I did a presentation to Cabinet. You know when you have lost the audience. I could sense that nobody round the table thought this was

their problem. I deliberately did a presentation designed to frighten them by saying, "All the stuff we are talking about could happen to you, and that could mean the NHS stops working"—things like that. I know that officials inside Whitehall are much more seized of the immediate potential for complete disaster if that sort of thing goes wrong than the politicians are. Sorry—I think that is breaking the rules of the Committee.

As a Committee we visited Korea a few months ago, and we were told by our counterpart committee that the North Koreans were now using household devices as the principal target for hacking. Is that common? Are they the most vulnerable part of our lives at the moment, more than the infrastructure of big institutions?

Professor Loukas: I cannot comment on whether Korea or other countries do that because it is very difficult to tell where our network traffic is coming from. There is no doubt that those devices are the most vulnerable—no doubt at all. That is for many reasons. One reason is that they are very complex in terms of software; for example, they are built on top of other software that was made by someone else, which was made by someone else—which was made by someone else. That means that there might be a flaw in the original software, in the next software, or in the one after that—a flaw in the supply chain of software. In fact, it is considered so easy to find vulnerabilities and flaws in the software of connected devices that some of my undergrad students look for flaws and report them to manufacturers for monetary reward on a weekly basis; that is their part-time job. That is the case because there are all these flaws on the underlying software that are common across all devices, to such a degree that it is financially meaningful to look for vulnerabilities as a steady source of income.

The second reason that household devices are vulnerable is that designing them is extremely difficult. You need, at the same time, engineering and computer science, as well as electronic engineering knowledge and cyber-security knowledge. As far as I know, no university is teaching cyber-security to electronic engineering students. The two are in different departments; they are not taught to the same people. You will never have someone who is an expert at developing software for connected devices but who also understands cyber-security. That is very rare.

The third reason is that those devices are always on because otherwise they are meaningless. A connected device makes sense only if it is always on. It makes more sense to compromise an always-on device, rather than a laptop that could be switched off in half an hour, for example—so they are very vulnerable.

Q106 **Damian Green:** The second point is very interesting—that we are training people in silos, so we do not have the electronic engineering capability and the cyber-security capacity. Is that true in the commercial world as well?

Matt Lewis: I can speak only to my world. In security there are a lot of skill sets available for the understanding of embedded system security—what it means to be able to unpick a hardware device, understand how it

is operating, what the security controls are and how they might have been bypassed, and so on. Jumping back to the technical aspect of using an IOT device as a place to hide in and infiltrate—that is a great thing to do, if that is your modus operandi. We looked at some enterprise printers about two years ago. We took six commercial, off-the-shelf enterprise printers, and in pretty much all of them we found a number of vulnerabilities that allowed us to compromise them and install a back door where we could remain silent.

What I am getting at here is that most embedded systems lack the security controls that we become accustomed to on our laptops. They do not have anti-virus or anti-malware. They do not have any visual feedback that says, "I've been compromised." Unfortunately, they are a great place for people with the right motive to stay silent for a long time in a connected device, which could be connected to a very sensitive network.

Q107 **Damian Green:** Do they characteristically need to get physical access? I forget which of you mentioned that you can google how to hack a BT home hub, which I found mildly terrifying. I have just googled it and reading about it—with my slightly ignorant eye—it seems that you need physically to get hold of it to hack it effectively. That is mildly reassuring, because they would need to burgle the house first. Is that generally true, or can you do it remotely?

Matt Lewis: Not always. The vulnerability could manifest itself in a way that you could compromise it remotely. For example, a lot of connected devices will talk out to the internet, to remote servers. There are a number of scenarios that could occur whereby an attacker may compromise the server that all of those devices communicate with, and then use that as a vector back into compromising a device. With typical phishing in the home network, if you get phished while connected to your home wi-fi network, suddenly the attacker has more privileged access to all the other devices on that network and can try an intrusion via that phishing attempt. There are a number of ways that that could be done remotely.

Simon Moore: You mentioned North Korea, for example, as a different level of attack. They will try to get into the manufacturing process and build in these breaches. I think the ones Matt is referring to are probably open vulnerabilities, but they might put in a so-called "zero-day", for example. That would be at the most sinister level. If we are talking about a nation state that is that aggressive, that becomes the risk and it is inside your home firewall.

Q108 **Damian Green:** Are the most capable malicious actors states rather than criminals?

Simon Moore: I think there is a blurring now. They will be supporting organised crime agencies, or the people who are in those will flow to and fro between them. I am not sure if this is a fact or not—I am sure you are going to tell me, Professor Loukas—but North Korea makes money out of

this. Is it true that as a nation state North Korea makes money out of aggressive hacking?

Professor Loukas: I do not know.

Matt Lewis: There are other aspects to it. It is not just always about financial gain or intelligence gathering. There are also things like denial of service. We saw this through the Mirai botnet, which was a botnet that infiltrated thousands of millions of IOT devices around the world that were incorrectly connected to the internet. Typically, they infiltrated through simple user name and password guessing, but they were able to then use that infrastructure as a mechanism to target key internet infrastructure in a denial of service attack, which brought down significant parts of the internet for several hours. There is a lot to unpick here. It is not just about nation state information gathering. It could be more disruptive in terms of what the end goals are.

Simon Moore: Going back to your opening point, when you cross-referenced people not looking at cyber properly at a political level. If we talk about growing the country and the economy, that is about productivity and that we need to get better at doing things. One of the industry's ways of doing that is digital transformation; they make things smarter and cleverer. As the professor said earlier, every time you do that or you build a big database, for example, you are building up a risk at the same time.

In the same way that we all know how to use email, we all need to know, at a project level and an individual level, that security is the other side of the coin at all times. It is not something to do as an afterthought. There is a misconception in industry, and a lot of the customers I talk to say they've got their project and ask, "Now, how do I make it secure?" They use the term "secure by design", but I think that should be more of a verb than a noun. Let's be designing securely on a continual basis. As we are doing our transformation, let us make sure that the transformation is secure and suitable for my mother or others. It is complicated.

Q109 **Damian Green:** Looking at our, as it were, defence capacity against this kind of activity, in the last Parliament one of our fellow Committees raised concern about the NCSC's capacity. It does immensely good work, but does it have enough capacity to meet demand for its services, which I imagine are rising every year?

Simon Moore: They work with industry, so they are trying to build that not just themselves, but organically across the piece.

Q110 **Damian Green:** Does it feel like we have enough capacity to do that through this private-public co-operation? Or are we being overwhelmed by a wave of cyber-criminality?

Matt Lewis: There is a known cyber-skills shortage in general—not just in the UK, but globally. That response addresses your question from a different angle, but I imagine that shortage may get more difficult as the connected world gets ever more connected, and we get more devices

online and different types of technology and technology profiles. Ensuring we have the right skillsets, and people who can understand that and work to those will be key. It comes back to initiatives such as CyberFirst. The more we can do now to prepare for then is advisable.

Q111 **Damian Green:** Do your students have a choice about whether they take the dark side or the light side?

Professor Loukas: They always do. In my case, I have never had an experience where I would recognise that someone has gone to the dark side, but in the past colleagues in other universities have told me about finding out later that one or two in their cohort have gone to the dark side, so it can happen, yes.

Q112 **Damian Green:** One last thought. We mentioned Huawei briefly. We set up a Huawei cyber-security evaluation centre and oversight board. Do you think that will have any effect? Is it having an effect?

Simon Moore: In what terms?

Damian Green: Is it changing Huawei's behaviour? Is it changing the way we treat Huawei? We have set up this system to check it. Do we think that it will work?

Simon Moore: I think there's a reluctance of people to buy, because of rumour and myth—not necessarily fact. From that point of view, it has had an effect.

Matt Lewis: My understanding from the general consensus is that the outcome from Huawei was an issue around software quality. It was not able to demonstrate sufficiently secure approaches to the code in the systems that it was developing, so it was considered too much of a risk for the UK to be using that. That is not to say that the threat was necessarily coming from China or the Chinese state per se, but if you put vulnerable infrastructure out there, it is open season for anyone who might try to target it. That is the last thing that we wanted.

On whether it will make a difference, it is on Huawei to understand whether or how it can demonstrate or appease people about its secure development practices. Things such as the PSTI Bill might go some way to doing that, but how much companies in foreign countries might want to adhere to or look to that guidance is up for debate.

Q113 **Damian Green:** So if we have a code that people have to adhere to, it could be applied to other companies.

Simon Moore: NCC is encouraging that: it asks for details on how you make your product. So it can take a view on how well you have published, and therefore how likely it is that it might be subverted. So there is a view. But that is more of the enterprise-type level than necessarily on domestic. It comes back to the point that Matt made about a kitemark-type model.

Matt Lewis: It does happen with domestic space, in the sense that it is CNI as well, with smart meters. Smart meters have had to go through a level of third-party independent testing to demonstrate a level of rigour before they can be released into the market.

Simon Moore: We're going to set out a process which is more forward looking than just a particular state in time.

Q114 **Kevin Brennan:** Professor Loukas, someone mentioned North Korea a few moments ago, and you said that you were not aware whether it successfully stole money. Is that correct?

Professor Loukas: I'm not aware.

Q115 **Kevin Brennan:** There was a United Nations report in, I think, 2021 that said that North Korea had stolen $316 million, in the cryptocurrency Ethereum, for use in developing its nuclear programme.

Professor Loukas: I have heard of the story, yes.

Q116 **Kevin Brennan:** It was a United Nations report. It seems to me a quite direct and sinister example, validated in a UN report and freely available in the media, that indicates how serious these sorts of breaches can be. Broadly, do scammers, hackers and so on have a better understanding of human nature than the manufacturers of connected tech devices?

Professor Loukas: By necessity, I imagine, because that is how they make their money. Deception is the dominant means of compromising a technological system at the moment, so of course they would. But it is also a matter of numbers. We look only at the successful ones. There are many attacks happening all the time; the number is astronomical. The fact that we see only the successful ones creates an impression that the cyber-criminals are all so intelligent and capable, and that that is why this is happening. That is not quite the case.

What is happening is that, through digital transformation across all sectors, we have opened ourselves to vulnerabilities across every domain and in every little system: from the mobile device to the connected device, the computer, every little app we use, social media, cloud and so on. Because there is such a large attack surface, let's say, it makes sense that there will be many people who will successfully—by chance, perhaps—find that this is the way that it works. For example, if you saw the first phishing emails, you would laugh at them now: there is no way they would work. Now, they are much more sophisticated. They will mention you by name, for a start. When a company, for example, hires a new recruit, you will see a cyber-attack against that person the next day, because they put it on LinkedIn and now a cyber-criminal will figure out that this person joined and is probably the easiest target at the moment—"Let's go for them". So you see an evolving situation where cyber-crime is gradually finding out the human weaknesses but by sheer chance, I would say.

Q117 **Kevin Brennan:** I understand what you are saying. I suppose I am asking: is there enough incentive for the manufacturers of connected tech devices to actually invest more in understanding human nature

themselves, and in the people who understand human nature, in order to devise security methods that are more effective against the attacks of the very clever and devious scammers?

Professor Loukas: Well, they do it for anything other than security, without a doubt. They do it for user-friendliness and for being attractive at the point of purchase.

Q118 **Kevin Brennan:** It's just not worth their while from their point of view, is it?

Professor Loukas: No, it is not.

Q119 **Kevin Brennan:** We were talking about the Product Security and Telecommunications Infrastructure Bill earlier. Is there a role for Governments to try to insist, incentivise or require—whatever it is—the manufacturers of connected tech devices to invest as much in understanding human nature in the way they develop and design their products as they do in making them look good?

Professor Loukas: I do not think it is a matter of a lack of understanding. I think the understanding probably already exists through the rest of the understanding of human nature that they do anyway, but they should be required to disclose their findings—to disclose that there is a cyber-risk at that level, and if you are, for example, vulnerable in this way, then you should know that there is a risk for you. If you are extremely stressed that someone might break into your house, then maybe when you are buying a smart lock, you should be alarmed about the likelihood of a smart lock failing; that can only happen through legislation.

Q120 **Kevin Brennan:** You'd be better off having a stupid lock sometimes, wouldn't you?

Professor Loukas: Absolutely.

Kevin Brennan: Your house might be safer.

Professor Loukas: But it's not a choice for most people. When you buy a new property now, it comes with a smart lock. You do not install it yourself.

Simon Moore: I think we are conflating some things here as well, in that the psychology element pertains more to things like emails and phishing, for example, whereas with hardware, it becomes a really hard one to always make it secure. Hardware is something you buy—say, a baby monitoring camera—so there is a hardware and software element to it. As we have already discussed, that software is layers of software that they are borrowing from something else before, and you are relying on all of that having been written securely. That is a trust thing you have to build, but when you are building your product—if I am designing a new one, and testing all of that and against all my devices—how much time will you take? The answer is that you are in a rush to market and a rush to make to profit, and that will tend to dominate. Making that secure is really

difficult, but I do not think it is a psychology problem; psychology is more in a different domain.

Q121 **Kevin Brennan:** Understood. When we are doing things like passwords and so on, we are right to try to get people to improve their password security—to change their passwords frequently, and to make them more complicated and difficult to detect and less obvious, and all those sorts of things—but it strikes me that that is entirely pushing against human nature, isn't it?

Simon Moore: Top tip: use a password keeper.

Kevin Brennan: In our lives, we all encounter a plethora of devices and accounts for which passwords are required these days, and the idea that most people—your average Joe or Joanne—are actually going to do all that is just not realistic. That is why the scammers can always win in the end, isn't it? Do you agree with that, professor?

Professor Loukas: Absolutely, but that is why there is a need for more research into alternative types of authentication.

Q122 **Kevin Brennan:** I remember being told a couple of years ago by my bank that in just a couple of years' time, quite soon, every time I spoke to anyone from the bank, my voice as my password would become the great method. Of course now, every time I access my internet banking, I have to put my glasses on, but I can't see the screen and can't read it with my glasses on, so I take them off, and then of course it doesn't recognise my face without my glasses, so I can't get into my bank account. Is facial recognition technology and that kind of voice recognition technology any more secure than password technology?

Professor Loukas: Maybe five years ago I would have said yes, but since then there has been so much progress on deepfakes that I do not say yes anymore. It is now so easy to create a face like yours or mine and then transmit it to the system that is detecting it that I don't know whether I would recommend it anymore.

Q123 **Kevin Brennan:** That is an interesting thought, isn't it? I say this having been to see "ABBA Voyage" and watched some of these deepfakes. The implications of all this are quite disturbing, aren't they?

My colleague Giles Watling was asking earlier about smart speakers in the home and so on, and I felt I ought to ask you the question that I have asked other people before: do you have a smart speaker in your home?

Professor Loukas: I do have a smart speaker, and I always switch it off when I am not issuing a command to it.

Q124 **Kevin Brennan:** Okay, and do you have a smart speaker, Mr Moore?

Simon Moore: Several, unfortunately!

Q125 **Kevin Brennan:** Do they talk to each other or just to you?

Simon Moore: Well, it depends. Sometimes the children play with them. And there are the different networks. I don't want to name them, but yes, I have them.

Q126 **Clive Efford:** Do you switch them off?

Kevin Brennan: Yes, do you do what Professor Loukas does, or do you leave them on all the time?

Simon Moore: No, I do tend to leave them on.

Q127 **Kevin Brennan:** Mr Lewis?

Matt Lewis: I have had one for research purposes, but it then became surplus to requirements—not for any particular security concerns. On a personal level, I don't want to become lazy in life; I like to be able to find other means for doing things. I don't need that level of automation personally, but I would add that there are sincere benefits from that technology to people with disabilities, for example—it is absolutely life changing.

Kevin Brennan: Indeed.

Simon Moore: I have a monitored firewall on the outside, though, which I suspect is not normal.

Kevin Brennan: Sorry, you have what?

Simon Moore: A monitored firewall, so I am looking at what goes in and out.

Q128 **Kevin Brennan:** Oh I see—okay. One of the reasons why I asked that is that I have previously asked the question of a former Information Commissioner and of a cyber-security academic—whose name I can't remember without checking the record, but who appeared before us in previous hearings—and both of them answered the question by saying no, they didn't have smart speakers in their homes. I asked them why and they both said it was because they didn't trust them. Are they being overly dramatic in their responses to this Committee by saying that, Professor Loukas?

Professor Loukas: No, they are not overly dramatic. It is a matter of risk management, as I mentioned before—or, to be more specific, of risk and benefit. If the benefit is so significant that it overrides any concerns, that is fine. I do not think that the risk is massive. However, if the benefit is just that this is a new gimmick—"Let's try it"—it was a toy for Christmas, then I think the privacy and cyber risks should be considered. So I would see them against each other, not in isolation.

Q129 **Kevin Brennan:** Mr Moore, earlier you mentioned the phrase "digital twin" and I wasn't quite sure I understood what you were talking about at that point. Can you for the record, for the Committee—so that it is on our record—just explain what you were talking about?

Simon Moore: It's taking the data that you might get from an environment, from telemetry, and then putting it into an environment where you can run applications on it and run what-if scenarios—

Q130 **Kevin Brennan:** So this is the data, perhaps, of a person—

Simon Moore: Simulation—

Kevin Brennan—from their movements, from what is picked up on their smartphone or from their car. Is that what you're talking about when you say "telemetry"? I am aware, from the context of the Apollo missions and so on, what telemetry is, but just explain in everyday language what you are talking about.

Simon Moore: Yes, any data point that might be useful; and you build a database that you can then run simulations or applications against.

Q131 **Kevin Brennan:** What is the purpose of that?

Simon Moore: It enables you to work out what to do next—to gain insight about how I might improve things. Let's say, for example, the transport hub was looking at the data on rail signalling. They would run a hackathon; they would say, "Here's our data. What can we do with it to determine a better way of running our trains?" You see these types of models used quite often in a beneficial context. But if I can then take that data, I might be able to do something non-beneficial with it.

Q132 **Kevin Brennan:** This could be data about people moving around—how they move, where they go and all those sorts of things?

Simon Moore: It could be exactly that, or it could be how a business works or how critical infrastructure works.

Q133 **Kevin Brennan:** Right, okay; thank you.

Finally, on the Product Security and Telecommunications Infrastructure Bill, which I am supposed to be asking you about, is there anything that any of you would suggest that would improve that Bill? Could it be amended in any way that might improve it in order to strengthen cyber-security?

Simon Moore: I think, going forward, it comes back to your point when you were asking about how we can make these devices secure. I do not think we will ever get to the point where we can mandate or create an environment where every single IOT device is secure because, at worst case, someone will buy something from North Korea and plug it into an environment. This comes back to, "How do we enable people to be resilient?"—I use that word again.

In an enterprise environment, the way we would do it, if I wanted to make my company secure, is that I would offer services to all my employees and check what is going on. It is whether we can do something like that with the ISPs. They already do it, for example, with telephones. When a rogue telephone number comes in, it goes "Suspected scam". We are starting to get data back from telephone providers about numbers that are coming at

us on how far we can trust them. It is whether we can take that further, and I do not think there are any recommendations on that in the Bill.

Q134 **Kevin Brennan:** Do you think it might be possible to draft a clause that would actually encompass that?

Simon Moore: Or to encourage services in that regard, because I think it is a service to people from the ISPs.

Q135 **Kevin Brennan:** Mr Lewis?

Matt Lewis: I know I mentioned it in a previous question, but to reiterate, I think that having some provisions in there for third-party independent validation of security controls would be really good to get that independent view. Then, we will not get into a position where, maybe, organisations are just doing a self-assessment, tick-box type exercise, where we have to just implicitly trust whether they have or have not implemented the security controls.

It would also be interesting for Government to explore—I think you mentioned this in your initial question—incentives, and what that could look like for organisations. What is the incentive for them to go through the various controls and recommendations in the legislation, if for example we will still have lots of cheap, vulnerable kit from China—or whatever—available on online stores? There needs to be a level playing field there, and maybe some incentives, or, I guess, disincentives for those who are not playing properly, whatever those might look like.

Q136 **Clive Efford:** I apologise for my voice. I am recovering from a cold that I have had for three weeks, which has gone to my larynx, but I'm not contagious, I assure you, and I haven't got covid.

The questions I was going to ask were covered earlier, so I will be very brief. We talked about the responsibility in Cabinet for cyber-resilience and cyber-power in economic policy. Where do you think that responsibility should sit, primarily? Who should have oversight within Cabinet?

Matt Lewis: In terms of the overall strategy, I have mentioned a few times that the National Cyber Security Centre has a lot of advice and guidance and initiatives for the general improvement and betterment of the security posture of the UK in critical national infrastructure. I do not think that I have too much more to add on that. A lot of what they do there is great, and they will continue to do good stuff, with the right level of support, in line and commensurate with the cyber strategy.

Q137 **Clive Efford:** The responsibility sits across five different Departments. You would say that they are coming up with a coherent policy and doing a good job?

Matt Lewis: That is a good question. They have good advice, which probably can and should be enacted by the other Departments. Certainly, there is a need for more rather than fewer people in those respective Departments who understand the guidance, the best practice and how to

implement that effectively within different Departments, rather than it being solely the responsibility of NCSC—just to clarify.

Q138 **Clive Efford:** Does anyone have anything to add?

Simon Moore: I will just build on my earlier point that it is the flip side of the coin, in that, whatever any Department does, they should all be cyber-aware and take responsibility for it. I would liken that to the 1980s revolution in quality—if you remember it—in manufacturing. At that point, at British Leyland, we had inspectors; you would build your thing and you would inspect it at the end and go, "It's wrong," and put it back through. We do not do that any more. We have quality at the outset. Everybody is responsible for quality.

Q139 **Clive Efford:** We have discussed China's interest in this area, but the Chinese Government appear to have identified connected tech as a key industry going forward. What do you think the implications are of China's focus on connected tech manufacturing?

Matt Lewis: Just from what we have seen in a lot of our own vulnerability research into a lot of the cheaper domestic tech from China, there are genuine concerns about the software quality and the fact that it might be vulnerable out of the box, as it were, because it has not been built or constructed to secure standards. That would be a main concern from my side.

Q140 **Clive Efford:** Do you think that China has a unique advantage in developing such tech because it can deal in its huge captive domestic market, which allows it to get ahead of other markets? Is that likely to have any influence on what is available and what is out there?

Matt Lewis: Likely yes, in that—you are right—they fabricate a lot of the microcontrollers and semiconductors that a lot of the world's devices use. I am aware that, not just in the UK but in the US as well, there are considerations about how much or how little of that is allowed to come into the western world, because there may be concerns about the level of proliferation. They definitely have the scale to mass produce and get those devices out there into various marketplaces.

Q141 **Clive Efford:** Smart cities rely on picking up data from people moving about in their everyday lives. Does the way that they collect and handle data open people up to any security risks?

Matt Lewis: It could be a number of things depending on the nature of a smart city application. There could be privacy risks if there is a level of data collection from individuals. I would hope that whatever that application was, there were the usual provisions for opting in and out in full awareness of any privacy-impacting aspects.

On the more sinister level, there could be cyber-physical aspects. Where there are actuators controlling things, and a cyber-attack has compromised that, the safety of an individual as they move about a city could be compromised. There is a lot to unpick in the different threats in a world of smart cities and how we mitigate them.

Q142 **Clive Efford:** When moving about from place to place, or driving from one city to another, if I go to a controlled-parking zone, there is a sign that tells me I am entering a controlled-parking zone. What tells me I am entering a smart city that will pick up all sorts of information from my phone, my car and everything else?

Simon Moore: It could be doing that anyway, of course, whether or not it is a smart city. A smart city offers us an opportunity—

Clive Efford: I have to tell you that in this session, I have gone from sitting here in absolute despair about this technology to being absolutely terrified.

Simon Moore: At one end we have the wild west, but I think a smart city actually offers us an opportunity. You have a single point of control for consumers and everybody in that environment to be treated as a company would be, in that a responsible organisational structure would bring it all together, would do the husbandry of that data, and would provide security services to it.

Q143 **Clive Efford:** My point was that if I do not have that information—if I do not know who is collecting what at any particular point—how do I make the choice?

Simon Moore: You are more likely to have it in a smart city.

Matt Lewis: I suspect the answer is that you cannot. I mentioned earlier that that is the nature of the connected world. How you would get a notification or indication about what level of data is being collected from you, by whom, at what point and for what purpose—that will probably not exist in one singular place. That is a risk that we might have to bear as citizens.

Q144 **Clive Efford:** We have talked about passwords. We make our passwords complicated, and when we go online, we have suggested passwords that we have no hope in hell of ever remembering—we would never remember a whole multiplicity of them. Do such passwords become a vulnerability in the sense that we have to store them somewhere?

Simon Moore: Yes. Browsers help with that now, and their method of doing that is fairly locked down. I would recommend using your own personal password protector. Another top tip is to use multi-factor authentication wherever it is available, so you are not relying just on passwords. You can either get a text back—not ideal—or use an authenticator. That can simply things.

Q145 **Clive Efford:** My last question is about autonomous vehicles, which are a bit of a hobby-horse of mine—the trolleybus theory and all the rest of it. If we went over to entirely autonomous vehicles, would fewer people die in road accidents?

Professor Loukas: That is an extremely difficult question. Are you asking from the perspective of failures in general or just of cyber-security?

Q146 **Clive Efford:** We are told that human error causes most accidents. If we eliminated human error, we would still have accidents, but would we have fewer of them?

Professor Loukas: Zero human error—well, there is human error in the design of an autonomous vehicle. You cannot have zero human error. Even then, you will have entities that would like to hack them—let's put it very simply—and cause even more damage perhaps than otherwise. The only difference, I would say, would be in the nature and the type of events, because it would be on purpose by someone in a specific case or for a specific target, while at the moment it is human error, which of course is very different.

Matt Lewis: It is a very valid point. My concern would be the fact that, different from now, when everything is connected and autonomous, certain threat actors, with the right level of access and vulnerability exploitation, might be able to control entire fleets of vehicles in ways that could cause harm. The change of technology is inadvertently increasing the number of attack vectors, or the possibility for attack, which could be safety or health-related impacting.

Clive Efford: Okay, I'll leave it there.

Chair: Thank you, Clive. As you say, that is absolutely terrifying. I thought you were going to talk about the automated hobby-horse for a minute. Thank you, Matt Lewis, Professor George Loukas and Simon Moore, for you evidence. It has been really interesting. That concludes the session.