HOUSE OF COMMONS

Business and Trade Sub-Committee

Oral evidence: UK economic security, HC 835

Wednesday 21 May 2025

Ordered by the House of Commons to be published on 21 May 2025.

Watch the meeting

Members present: Liam Byrne (Chair); Sarah Edwards; Charlie Maynard; Gregor Poynton; Matt Western.

Questions 145-164

Witnesses

Chris Parker, Director, Government Strategy at Fortinet; Zeki Turedi, Field Chief Technology Officer, Europe, CrowdStrike; Simon Thomas, Chief Executive Officer, Paragraf; and Brendan Casey, Chief Executive Officer, Kelvin Nanotechnology.

Examination of witnesses

Witnesses: Chris Parker, Zeki Turedi, Simon Thomas and Brendan Casey.

Q145 **Chair:** Welcome to this final panel of today's hearings on the economic security of our country. Thank you very much indeed for joining us for this third panel, which is looking at emerging technologies and cyber-security.

Mr Parker, I will just start with you. Do you think that defending our national security basically means that we have to retain a technology lead over our rivals in this world?

Chris Parker: We have a challenge in the United Kingdom, because the emergence of the IT sector has only had 25 years or so of really great accelerated growth, and, of course, a large amount of that, in terms of what is used in the western world, originates in the United States of America. That does not mean that that is a negative; it just means that that is a hub for design and engineering.

What the UK does extremely well is in knowing how to put those technologies together, as we have always traditionally done in other sectors. Due to other sectors—such as finance lead, insurance lead and some of the other great things we do in our country—we can leverage that technology, which may well originate elsewhere. For example, Fortinet, my company, has a British global CISO sat in California, and there are many other examples. I am sure that other panel members and people across the sector will say that the way that the technology people move around, and design, seems to be almost borderless.

Q146 **Chair:** Is it therefore impossible for us to maintain a technology lead over our rivals in today's world?

Chris Parker: I would say that to catch up at this stage would be exceptionally difficult. It is a bit like when we compare it to our normal daytime use of any computer; those are using systems that are well established. What tends to happen, which the wider community outside our sector is perhaps not aware of, is that there is an awful lot of trust and sharing going on inside the sector.

That is one big piece that I think would be a really valuable deduction today—that, behind the curtain, if you like, there is an awful lot of sharing, collaboration and trusted work going on in what is actually quite a small sector. A lot of people know each other. I also find it highly ethical as a sector; having worked in other sectors, it is one of the most ethical I have ever seen in my working life.

On the basis of trusted international collaboration, I personally do not see the need and requirement for us to emerge as a leading country.

Q147 **Chair:** Mr Turedi?

Zeki Turedi: I would say that when we look into the technology sector, it can be very rewarding for a country to be ahead of certain innovations.

But we also have to remember that, as you adapt new technology innovations, there are also risks. For example, we see artificial intelligence being a subject that is very much spoken of in organisations here in the UK. We want to take those technologies that can bring the UK forward, but the reality is that there could be risks in it—for example, not fully understanding the digital supply chain of those technologies. But again, there is a great advantage in that.

Simon Thomas: I come from quite a different perspective. As a hardware manufacturer, I see things a little bit differently. In terms of national security and technology, does the technology advantage deliver what we want? It always will because those that are in the lead have always got the edge, but what does that actually mean? We can talk about security and IT, but where does security come from? IT does not run without hardware.

When we think about the future of all these different wonderful technologies that are coming along, what is it that will drive them? Software is always going to be developed, but, as you can see now, particularly with the AI that has just been mentioned, the hardware is the bottleneck. You can see national security and technological security as being the control over the critical components. Here today, critical components mean things that go to the core of what you are trying to deliver. I am in the semiconductor world, so semiconductor chips are one of those examples.

Even if you look at quantum or AI, there are specific types of devices required that come from specific material sets or specific technologies that sit at the heart of them. If we were to start thinking about what national security for the UK means—I like to use this term quite a lot, but we are the innovation nation—we should be able to take hold of those critical components and use them to our advantage. I do not mean an advantage that is a threat. I mean an advantage that is a hand-holding, hand-shaking exercise: "We have got this. How would you like to work together? We have a critical component. How do we work together in a secure way?"

I agree the software side is important, but we have also got to look at those layers that go underneath that deliver that critical capability. For me, yes, definitely: the way in which national security is handled in the UK with regards to technology is critical, but I would really like to take the conversation towards what that means in terms of what we have to deliver and what we have to control.

Q148 **Chair:** Dr Casey?

Brendan Casey: I think critical technologies have the potential to significantly impact the UK's prosperity, security and global leadership. We come from the cutting-edge technology perspective. Things such as quantum technologies underpinned by semiconductors and photonics will be key for national security and critical national infrastructure. Quantum technologies coming through will transform communications, computing, imaging and sensing to help us ensure that our infrastructure and services

such as healthcare, transportation, environmental sustainability and security are fit for the challenges of the future. I think we are leading in areas such as quantum, and we should embrace that and support that fully.

Chair: We are going to move through the questions quickly now, because there is going to be a vote in the House shortly as the Opposition day debate concludes. Let me come to Matt Western.

Q149 **Matt Western:** How do you think the Government should balance the need for national security protections while also fostering the emerging technology sector?

Chris Parker: It is always a dynamic. I would also say that there is a healthy dynamic of positive stress, as opposed to negative stress that can be uncomfortable. The positive stress means there is always a healthy balance between regulation and an enormous amount of industry collaborative work that goes on already globally. Returning to my point, cyber-security does not respect borders at all. It is very much a global problem, a global issue. We can look at data. There is some very good data out in the public domain. Most companies produce those. Fortinet's FortiGuard Labs produced a report recently that has some superb data out in the public space of exactly what needs to be done.

On the point about balance, the biggest need is for collaboration and for people just to talk and communicate. I see a lot of that. I have to do a lot of that as well. That is part of our duty in our sector, but also, our ability to secure our customers and people everywhere is only through collaboration with the national agencies on quite a regular basis. You would probably not be surprised to hear that we cannot talk about the ways that that happens, but the regularity of it is impressive.

Q150 **Matt Western:** Dr Brendan Casey, and then Dr Simon Thomas?

Brendan Casey: I think collaboration and transparency of the process, and good communication, would be key.

Simon Thomas: From my perspective, coming from a specific type of company that has been VC-backed in order to get our technology to the level it is, I completely agree with what has been said. On top of that, if we want to ensure that we get these technologies to a state where we can use them properly in this country, we have to make sure that those technologies succeed. If they do not succeed here, they will succeed somewhere else. The way in which investment screening, for example, is looked at today is not quite correct, because quite often, that screening happens at the point of investment. That is the most critical point for a company that is trying to push its runway out, and that is when the investigation starts.

I completely agree with having a more open and beneficial approach, where the Government and the company can work together over time, maybe even starting at the inception of the company, so that the technology is understood by the Government as we move through the

different phases. I also think that would add a level of knowledge to the civil service about what type of technology people are developing and how it can be used. I do not think people, particularly in investor companies, would be averse to being questioned at early stage if they knew it was going to be useful and collaborative going forward.

Q151 **Matt Western:** And it would aid investment or funding coming through.

Simon Thomas: Yes.

Q152 **Charlie Maynard:** Does the UK currently have the right approach to controlling the export of sensitive technologies? I am interested to hear your experiences in your two lines of work.

Simon Thomas: Today, we have not really had any—other than obviously having to comply with dual use, which is a big thing for us, particularly at the cutting edge, where we are. I think we could have better trade deals, but everyone is fully aware of that.

Q153 **Chair:** Can you say that again, Dr Thomas?

Simon Thomas: We could have better trade deals, which the Government are working on right now. In terms of technology borders, it is very clear that there are certain technologies you cannot sell to certain states. As long as you are aware of that, it is quite straightforward, from my perspective.

Brendan Casey: I would agree that it is not something that we have had an issue with. It is something you need to be aware of and comply with and ensure that you do it correctly, but we have not found it as a particular issue, so I would agree with Simon on that.

Q154 **Charlie Maynard:** Does anyone on the panel have a particular view on our approach compared to the US CFIUS approach? What are the pros and cons, and what might we have an advantage over or disadvantage over compared to their approach?

Simon Thomas: We have a US subsidiary in San Diego, and the CFIUS rules are obviously a lot more strict. If we are looking at proliferation and progress of technology, then I believe the UK has a better set-up. Whether that offers the level of protection that the US has is the balance we have to look into. Right now, at companies like Paragraf, we are very aware of IP. We are very aware of technology control because it is our value, so we want to keep it ourselves. We are very well aligned with UK strategy and wanting to make sure that that IP or technology remains within our control. We have run across some CFIUS instances that require a lot more paperwork—we definitely know that—but we have not really had any specific troubles yet.

Q155 **Chair:** We know that the American national security strategy quite explicitly entails a plan to try to slow down China, when it comes to China developing advanced technologies. In the conversations that are no doubt going on in trying to get a trade deal with the United States agreed, there will therefore be questions about whether the UK should be doing more to

join in with that American-led strategy. Is that a good idea, and is it possible?

Chris Parker: You can probably expect me not to comment on geopolitical balance. My view is that, again, going back to technology, if it is set up correctly and used efficiently, it should protect against all threats. It is the goal of certainly quite a few people in the sector every day of the week to try to make sure that happens.

When it comes to state actors, the CEO of the NCSC recently, at CYBERUK—on stage, on record and still available online—cited China as the big threat that we have to cope and tangle with. So everyone knows that is the challenge. The particular challenge I think we have to deal with internally in the sector and in the UK is to make sure we are set up to be able to secure against any threat that might disturb our national prosperity.

To be honest, in the sector and certainly at the technology end of things, people are pretty apolitical. They focus very much, very clearly, on the threat, because it is not just state actors. There are also now a lot of criminal actors and gangs, as we have seen in this country very recently, and they can cause an awful lot of damage. So the sector tends to be focused on the technological threat and defeating it, and that is being done day in, day out. Where it comes from is certainly part of our threat analysis and what we analyse, but it does not feed so much into a political level; it feeds much more into a technological level.

Chair: Are there any other views from others on that?

Zeki Turedi: I completely agree. We have to remember that China, Iran and Russia are definitely targeting the UK. We saw a 150% increase in the targeting by China of a number of sectors globally last year. But going back to what we have said here, a number of other threat actors are still interested in the UK. E-crime has become more sophisticated and more targeted, but there are also new tactics, such as fake IT workers from North Korea targeting UK entities at the moment. The cyber landscape we have at the moment can be quite complex. It is ever evolving and shifting.

Q156 **Chair:** Very interesting. Is the implication that we have to be on guard against protecting ourselves against the wrong peril?

Zeki Turedi: Yes, exactly. Again, that landscape, literally day by day, continuously evolves.

Q157 **Chair:** Interesting. Do you think we are therefore giving enough attention to the threat from cyber-criminals?

Zeki Turedi: It depends on where you look into it. The NCSC, for example, is doing a great amount of work to make sure that individuals are very aware of the threat. We have suddenly heard a lot in the media over the last few weeks, but the reality is that it is continuous. It is not just what we see in the media; it is continuous in the background, so maybe that has not gone down to every single public entity or every single

organisation realising that it needs to start resourcing for security protections as well.

Simon Thomas: I just go back to my field—the hardware side of stuff. I completely agree with what has been said here. In terms of aligning with specific export and import or investment regulations, I would urge a bit more pragmatism to try to understand what it is we want or what we define as sensitive technologies and, in the future, where we think those partners need to be, because if we do not at least try to forward-plan where we want to put our critical technologies or those critical components I talked about, we may find, if we align with other people's rules, that we cannot access those markets or, even more critically, get those things that we want and need for national security.

Q158 **Chair:** The implication is that we should not be purely demand led when it comes to investment. Actually, let's be a bit smarter about where we want to secure forward investment from.

Simon Thomas: Absolutely.

Chair: Interesting. Dr Casey, do you have anything to add to that?

Brendan Casey: I don't think I have anything further to add.

Q159 **Sarah Edwards:** Chris and Zeki, could you describe a bit more the types of threat that we face and how over the last few years those threats from a cyber-security perspective have transformed or morphed? Are we able to chart the change? Where have we been? Where are we now? And where might we be going?

Chris Parker: The first good bit of news is that we do know the threat, because the threat is continuously scanned, monitored and passed around—certainly in our case, in Fortinet, to all devices globally. There is an awful lot of automation, which we hear about as a negative thing in terms of the threat from AI and everything else. We have been using AI in Fortinet for a decade. We just haven't necessarily been telling everyone about it, quite rightly; nor do we share, quite rightly, a lot of the detail of what we do.

To go back to the threat piece, the biggest development, the things that are leaping forward now because of automation, are really on the underworld sites, the dark sites that people hear about but actually do exist and fortunately are monitored as well. There are things that are now becoming almost too easy for people to buy. They can buy exploit kits. You can go and just do that and you can go and work out how to do it.

You also have ransomware as a service. Bizarrely, people can go and actually outsource their criminal acts. You also have cyber-crime as a service—people doing those things. So people who are malicious actors are doing those things. In terms of the broad view, there is now an uptick in that automation—almost commercialisation—of crime, but I know that our agencies in the UK, with a hell of a lot of contribution from the Three

Eyes, Five Eyes and the wider community, make sure that that is kept at bay.

Zeki Turedi: The reality is that it is still as simple as this: you are dealing with hacktivists, e-crime and nation states. But the reality is that, especially when we talk about nation states and criminal actor groups, there are going to be a lot more of them. They have seen the success over the last few years, especially during the pandemic, when we started to see a lot of organisations being targeted. They have seen that success, have taken that opportunity and are increasing the targeting.

For me, the biggest concern is the increasing sophistication. Year on year, they are becoming more sophisticated and a lot quicker. To give you an idea, we continuously track how long it takes a threat actor to get into an organisation. If we had had this conversation five years ago, it would have been roughly 10 hours on average. Today, it is less than one hour, and the best time is 51 seconds.

They are getting more equipped. They are using technologies like artificial intelligence to speed their processes up. They are very aware of automation, new technologies and techniques. There is also an ever-growing marketplace. As Chris mentioned, they are sharing tools and techniques as well. That would be my biggest concern. The biggest change is that sheer number of new actor groups, including nation states, as well as how successful they are in terms of speed and automation.

Q160 **Sarah Edwards:** We have seen quite a lot in the news recently about the vulnerability of companies, particularly in the food sector. People are obviously falling foul of this; they may have been trying very hard not to, but it has happened. What do you think about the National Cyber Security Centre's guidance? Is it good enough? Is it helpful enough? Can companies access, understand and apply it? Do you have thoughts on ways it could be improved? We are talking about large companies, but if we start to look at the smaller ones, where the vulnerabilities might be, there are back doors into larger companies. What do you think about the support available?

Chris Parker: I am very lucky to sit as the vice chair of the cyber resilience committee for techUK, which works with the Department for Science, Innovation and Technology to make sure we as a group of industry people can support. I sat on it for two years before my current position, and I never heard negative views about our UK NCSC. Only last week I heard from a very senior American, who was talking about the differences among the Three Eyes community. They are all very strong, as you would expect to hear, but he was very laudatory about the UK NCSC's ability to keep ahead on some of those aspects. There is some good news there.

If there is some bad news, it is this. While there is a lot of awareness and understanding about what to do inside the sector and the NCSC, there is a problem at the wider levels of leadership in the UK and other countries—it is not just a UK problem—in understanding what the challenges and risks

are. As always, time is the biggest problem for everyone—finding time to study and bring themselves up to speed. We always urge everybody in leadership and financial positions to understand more about the impact on their business. I do not think there is a person in the UK who has been hit by a cyber-attack who is not very focused afterwards. What we are after is the prevention being better than the cure.

Zeki Turedi: I think the guidance is very good. There needs to be a lot more clarity and probably explanation. A lot of organisations struggle with taking that guidance and making use of it. The National Audit Office's Government cyber resilience report was great. One area that it highlighted was not being able to get cyber-security expertise into Departments. That is true not just in the public sector, but in the private sector.

One thing that has been beneficial in the private sector is the realisation that they can start utilising shared service providers or managed service providers, which can provide a hybrid approach, rather than thinking they have to build everything themselves. They also need a bit more clarity on how to get started on their maturity journey when it comes to cyber-security.

Q161 **Sarah Edwards:** Do you think that there needs to be a much greater focus at board level as well? Ideally, you would have somebody with that expertise, but we know that this is an evolving, highly digitalised economy, and there are fewer and fewer people to go around as it becomes more important. What could be done to strengthen oversight at board level?

Chris Parker: The UK NCSC has very recently put out some excellent guidance for boards—be they small companies right up to plcs. I would recommend everybody to read that. However, it is also a culture change; it is not just about having a man or woman sat on the board who is a technical person, and everyone says, "That's fine." It is really about everyone having a culture change and realising that this is just as live a risk as financial crime, fire safety, health and safety—all the things we are quite used to in this country, because this great place has made sure everyone is aware of their responsibilities.

Legislation is coming, and there is more legislation tightening, with the cyber resilience Bill being processed at the moment—and that is with industry. I think we could all urge more interaction with industry where we can, because that allows it to hit the ground as a better Act. But I would just say that legislation is not always the answer. It is definitely about culture change and making sure we urge all those leaders to pass it down into organisations—to produce those human firewalls, as we call them—and get the people just as aware of what to do as the technology.

Q162 **Sarah Edwards:** Finally, on this level of risk—and the increased risk we are seeing, with many more companies becoming quite public victims—there are reports that some insurers are viewing cyber threats in the same way they view terrorism: that is, they will not insure if there is a breach and an obvious resulting detriment. What do you think could be done

around private-public collaboration to start mitigating some of that? Because this is the world we are going into, and if insurers have decided they are not going to insure it, we have a problem.

Zeki Turedi: I think it comes down to more preparedness—that is the reality. For example, making sure organisations have things like incident response retainers in place and defined processes. Again, there is good guidance from the NCSC on how to initiate this, but I am not sure how many organisations are taking that seriously.

I think it also goes back to what Chris mentioned—having that culture within organisations to recognise that they need to focus on areas like secure by design or secure by default, and to make sure they are prepared for those types of incidents.

Q163 **Matt Western:** Briefly, it is interesting what you say about cultures within organisations and bringing about change. In the light of recent events—the British Library is still basically shut down, and we have seen attacks across the public sector, not just in business—do you think the time has come, as Estonia did all those years ago post their attack, for a national conversation and a whole-of-society approach to addressing these threats?

Chris Parker: Yes, definitely. We have done a lot of great things in this country. We have changed the understanding about, "Don't drown when you go to the seaside," or, "Wear your seatbelt." There have been lots of great campaigns, and that culture change will come from Government guiding, assisting and resourcing the messaging that goes through, no doubt.

One of the biggest problems we have is that there is a gap between the fantastic training available—Fortinet offers a huge amount of training for free online, and other companies do as well; everyone has some really good training out there—and getting people to actually click on it, sit down for 20 or 30 minutes a week, and keep themselves up to date. That is the challenge.

Normally, that says to me that there needs to be leadership or compulsion to do that. It also needs to start a few years before, in schools, if we are to get the UK really safe and aware. We need to make sure—just as the others on the panel are quite rightly saying about their businesses here in the UK— that we need to get people up to speed.

So STEM Learning, which we are partnering with at the moment, I learned the other day has had a resource cut. There are lots of things where, as a sector, we are stepping into headwinds, where we would rather they were tailwinds, particularly when it comes to resourcing some of those younger people and the workforce, to get them the free training and tell them: "Click the button. Train."

Zeki Turedi: I think there is really good collaboration between private and public organisations. It allows us to do what we do best and protect our organisations.

What we would like to see is the Government using the tools available to them—things like law enforcement—to find those individuals and arrest them; to do more things such as the takedown of infrastructure utilised by nation states and criminal actors. That could make a big shift and change to this landscape.

Q164 **Chair:** Dr Thomas and Dr Casey, do you have anything to add to that?

Simon Thomas: I can only speak from experience. We have a very robust approach to security at Paragraf, partially due to the person we have hired, who is very experienced in it. But I do think there is one way that you could proliferate this very rapidly, and that is through spin-out, start-up invested companies. The people who go through those companies are generally the ones that move on to other businesses, so if you want to spread this throughout the industrial sector, making it part of an investment requirement would be a very effective approach. Again, if people see the benefits, they are not going to complain about it.

Brendan Casey: From a lower level, day-to-day basis, I find that in a company, the Cyber Essentials approach has been extremely helpful. It makes you think, appreciate and review what you do. From a ground-up perspective, that is an extremely beneficial thing.

Chair: Thank you. The Minister is on his feet in the Chamber and a vote is about to take place, so I will conclude the panel there. Thank you very much for such clear and concise evidence today; it has made our job of coming to conclusions a little easier.