

Business and Trade Sub-Committee

Oral evidence: UK economic security, HC 835

Tuesday 8 July 2025

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

[Watch the meeting](#)

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

Questions 235-258

Witnesses

[IV](#): James Babbage, Director General (Threats), National Crime Agency, Andrew Gould, Temporary Commander for Cyber and Economic Crime, National Cybercrime Programme Lead for the National Police Chiefs' Council, City of London Police and Richard Horne, CEO, National Cyber Security Centre.

Examination of witnesses

Witnesses: James Babbage, Richard Horne and Andrew Gould.

Chair: Welcome to the final panel of the Sub-Committee on economic security. I thank the witnesses who are joining us from the National Cyber Security Centre, the City of London police and the National Crime Agency. We are extremely grateful to you for what you do and for your time today.

Q235 **Matt Western:** This is a question for you, Richard. The Government talk about a whole-society approach to this challenge. How do you think our deployment of resources and investment in our capabilities, in both the private and public sector, are matching up against the investment of our adversaries?

Richard Horne: That is a challenging question to give a simple answer to, but I will try. We talked in our last annual review about a growing gap. On the one hand, we have a growing dependency on technology across all of our society, and therefore we have a growing exposure to the impact of cyber-attacks. The kind of cyber-attacks that you see today have a greater impact because we are more dependent on technology. If you take the technology away, it causes a greater impact. Also, the threat actors are developing at pace, the market is evolving for criminals, and it is an expanding threat landscape. On the other hand, we are seeing a steady increase in our defences across our society and our ability to defend and be resilient against cyber-attacks. I think there is a growing gap between the two, and we talked about that in our annual review back in November.

Q236 **Matt Western:** We heard just now that 1% of small businesses are aware of the NSCS. Is that a surprise to you, and what do you need to do to build awareness? If we are going to have a whole-society approach, small businesses may be vulnerable, as we know, but small businesses supply larger businesses, and that can affect the larger business operation.

Richard Horne: I am less concerned about their awareness of us, and I am more concerned about their awareness of what we are saying. That same research acknowledged that they are much more aware of our campaigns, such as our scheme Cyber Essentials. That is a scheme of over 400 accredited companies, many of which are also small businesses, that are there to help businesses get cyber essentials in place and deal with the fundamentals of cyber-security. There would be greater awareness of schemes like that, and what matters to me is that organisations are aware of the schemes and the advice. Having said that, there is still a long way to go to raise the awareness for us across the UK of what organisations need to do for their cyber-security.

Q237 **Matt Western:** Finally, we just heard from M&S—you may have been the room—about its situation with legacy systems, which is typical of all organisations. It was looking at the financial cost of doing that, and the cost to business that it has been hit with. What can Government do to incentivise more investment in this sphere by business?

Richard Horne: That is a great challenge, not just in business but in Government. You will have seen the Public Accounts Committee's report on Government's own IT. It is a huge challenge, and organisations that are racing to modernise and digitise will always have this challenge of either investing in replacing legacy systems, which might not give any advance on their mission, or adopting AI and new technologies.

It is a real challenge, and one thing I am really aware of in the NCSC is that, over the last year, we have shifted to a stronger message to boardrooms. A lot of the work that the NCSC has done over many years has been engaging with professionals and IT people across the country. There is a much greater need now for a strong message to boards on the urgency and the importance of acting and investing. We have been working with DSIT on a code of practice for governance of cyber-security, and there are other initiatives that we are taking to drive the message into boardrooms much more strongly.

Q238 **Chair:** That is very helpful. Can you help us now contextualise this, and talk us through some of the threats that we should foresee over the next five to 10 years? Richard, do you want to kick off? Give us a bit of horizon-scanning.

Richard Horne: The high-level message is: it is diverse, dynamic and changing. It is almost a bit too simple to say "nation state" and "criminal" now. We have nation state-directed activities, and some of the previous conversation focused on that. We have private enterprises creating the capability that nation states buy, so there is the proliferation of attack tools to enable often smaller nation states to undertake activity. As well, we have seen a lot of the bigger nation states using private enterprises to enable their attacks.

Q239 **Chair:** Almost like mercenaries.

Richard Horne: Absolutely. Then, there are nation state-aligned, often called hacktivists. We have seen that particularly in Russia but also elsewhere in the world, where you have groups of individual criminals who are independent of the state. They are not acting to make money; they are acting in the aligned interests of the state, as it were, attacking people who attack our state kind of thing. Then, you have what I call your nation state-sheltered—a lot of the ransomware groups, for example, operating in countries where they benefit from some kind of protection from the nation state, but not necessarily direction. Then you have individuals. It is really quite a broad spectrum. We start to see trading within it. It is a marketplace rather than clearly defined black and white.

Q240 **Chair:** And the threat is going up.

Richard Horne: Yes.

Q241 **Chair:** James, how does this show up in your world?

James Babbage: May I add to that from the perspective of serious organised crime? In the NCA we look across the range of serious organised crime threats and we formally publish on this every year. But one of the



HOUSE OF COMMONS

things we say is that the thing that is most affecting how serious organised crime is growing is not so much what the criminals are doing but us, the public: our own dependence on online services, our use of them and our use of other services that depend on them. If you look across the whole range of online crime, not just cyber-crime, but fraud and child sexual abuse online and other crimes of that sort, you can see that they are, in general, rising. The limiting factors that there have been in the past are falling away, particularly on fraud. I will come back to cyber in a second. Previously, the number of criminals in a boiler room would be the limiting factor. Now, perhaps the number of people trafficked across international boundaries, unwillingly, to do fraud is the limiting factor. AI is taking some of those limiting factors out of the equation. Specifically on cyber-crime—

Chair: Wait, can I just check? Are you saying that fraudsters are being imported into particular countries?

James Babbage: Yes. In south-east Asia and in west Africa. That is right. People are conned into going and working in scam compounds. But increasingly, AI allows you to automate some of the earlier stages of that.

As far as cyber-crime is concerned, we believe that the threat was level between 2023 and 2024. It has been rising for many years. That is probably a short-lived plateau, but it is a significant success and it is worth dwelling on it. As your earlier witnesses said, the bulk of cyber-crime affecting the UK is foreign in origin, particularly Russian-speaking. It is that where the threat largely has levelled off. There is, however, a growing but smaller level of threat from what we are calling English-speaking cyber actors. I should touch on both parts briefly. First, on the English-speaking cyber actors, we have these Com networks. Scattered Spider is an example of a cyber-focused Com network. These are loose networks of individuals, usually aged—

Q242 **Chair:** Sorry, for the record, are they common networks?

James Babbage: Com networks. That is what they call themselves. Scattered Spider is what industry calls them. They are aged 15 to 25 or so, with loose affiliations, doing it partly for profit but as much for kudos. It has sort of come out of gaming, I think, as people have said. The point is that it is very closely aligned with coercive and abusive behaviour of often vulnerable children. To some degree, the same social engineering techniques that are used on those children to abuse them are then used by a smaller subset on companies to get into help desks in the way you have heard.

To touch on the Russian-speaking cyber-crime phenomenon, what has gone on there? The original cyber-crime groups were very focused. They were individual groups of people. Conti was mentioned earlier—that is an example of that. That moved on to a ransomware as a service offering, where you would have a set of people who would make it possible for any affiliate to do ransomware. LockBit is a good example of that, with 2,350 victims listed on its leak site over about four or five years—the biggest



HOUSE OF COMMONS

number of victims listed by any group. The NCA, working with a number of other law enforcement organisations around the world, disrupted it very substantially in early 2023¹, about the same time as the FBI, working with us and others, disrupted another group called BlackCat. We have seen a sort of fragmentation of the Russian ransomware ecosystem, hence the levelling off.

Finally, DragonForce, which plays a bit part in the Marks & Spencer incident, as you have heard, is almost taking this level of abstraction a step further. It is making tools available for individual cyber-criminals to build into ransomware. It lowers the barrier to entry, but it is even less of a sort of congregating factor than LockBit was. When we first knew that there had been a DragonForce message to Marks & Spencer, it was put in touch with the relevant regional organised crime unit in Yorkshire and Humber, which we had tasked to lead on DragonForce. They were able to say that the message was quite different from other messages they had seen from DragonForce. That was useful, but also to be expected, in that the sorts of criminals using DragonForce can be expected to be much more varied.

Q243 Chair: That is very useful. Mr Gould, would you like to round out the picture of threats?

Andrew Gould: I completely agree with what both Richard and James have said. In terms of policing, particularly in relation to the Com, it is interesting for us how it plays out locally. You might have these national and international threats, but the impact is played out on local victims. If you think of traditional cyber-crime, if there is such a thing, ransomware was purely focused on the cyber-crime offending, but now there is a more hybrid approach, where they are offending across threat types.

I will be careful about what I say here, but there is a particular investigation by a north-western cyber-crime team in a local force, which has identified a number of individuals who are hacking into people's devices to access intimate images. That is a Computer Misuse Act offence—a hacking offence—but they are then extorting the young women whose images they are, making direct contact. In that one investigation, there are 4,000 victims. There will be local force cyber-crime units doing those sorts of investigations across the country, as well as ransomware denial of service attacks and all the traditional offending.

Suddenly, we are having to operate at a scale, in terms of managing victims, as a small force team, where you might have 10,000 victims in every force in the country. How do you manage that at that scale? They are offending across crime type. There is domestic abuse, violence against women and girls, and an incel element. The threat is diversifying and playing out into real-world harms in a way that it has not in the past. We are doing a lot of work with the NCA and the Government to think about how we can be more flexible in operating along those threats, and not

¹ The witness subsequently wished to clarify that the disruption was in 2024, not in 2023.

working in threat and geographical silos as policing sometimes traditionally has.

Q244 Charlie Maynard: Following up on that, if those barriers to entry keep dropping, which seems very probable, can you sketch out how this will look in five years, in terms of how you try to stay ahead? It sounds almost as if it is traditional policing: you are trying to identify who these people are and going after them, or is there much more than that?

James Babbage: I think it is different from that. Richard, do you want to start?

Richard Horne: I will start from the defenders side, and James can touch on the policing side. From a defenders perspective, one interesting thing is that at the end of the day, the core techniques these attackers are using are not evolving that fast. Many of the attacks we see today are exploiting vulnerabilities in configurations and issues with how your most privileged users administer systems and things like that, which were there 20 years ago. Yes, the threat is rising overall, but actually, what we as defenders need to do is not changing that fast. The biggest step change we can make is to get those fundamentals consistently rolled out in more organisations. That is where schemes such as Cyber Essentials and having those basics in place across as many organisations as possible raise the barrier of entry from the defence perspective, even though the barrier of entry to gain access to the tools, as it were, is dropping.

James Babbage: Building on that, the minority of our work is going after individual reports of cyber-attacks, following them up and trying to find out what happened, because the work factor needed to do that is very large, and you may get to a couple of individuals, or you may not. Of course, in a significant incident we will either investigate ourselves or task it out to the broader system that Andrew has described. We would describe the majority of our work as proactive: it is going after the cyber-crime ecosystem that allows these barriers to lower, and these attacks to go ahead. That is looking at the infrastructure, hardware, systems, tools and services that enable the cyber-criminals; the financial services that they use, particularly cryptocurrency; how they achieve their initial access and compromise; and the marketplaces and forums in which they congregate, and share tactics, techniques, procedures and victim information.

Over the last few years, there have been several disruptions and takedowns, as well as arrests and sanctions of individuals involved in those key ecosystem elements. LockBit is just one example, as I mentioned earlier. On the day of the LockBit operation, we took down 11,000 domains, closed 14,000 nefarious accounts, identified and froze 200 cryptocurrency accounts and took down 40 key servers across nine countries. That sort of impact translates into the change that we saw in what had been a doubling of ransomware, year on year, over the previous 12 months.

Q245 Charlie Maynard: You talked about English language and Russian



language as two big blocks. Sticking with the Russian language side, that is obviously across several countries, not just Russia. Is it impossible to access, or can you access a lot of that to take things down in other states? Are there effective means of doing that, so that it is not necessarily beyond reach, with the right tools?

James Babbage: Cyber transcends geography, so any of these actors, whatever language they are speaking, will just naturally, without even really trying, use infrastructure throughout the world. Then, of course, they do also try to do that, to make it complicated for us.

Q246 **John Cooper:** I wonder, Mr Babbage, if you are related to Charles Babbage, the inventor of the computer? That would be interesting. On funding, what impact, if any, is the recent spending review likely to have on your ability to deal with cyber-threats? The single intelligence account, which funds British intelligence services, got quite a substantial raise in that review. Will that have an impact?

Richard Horne: There is no question but that we have the funding to continue our mission and drive, as hard as we can, cyber-security across the UK. To be perfectly honest, the big funding leap that we need is in organisations across the UK and how they defend themselves, be that Government Departments or private sector organisations. Earlier you heard the reflections of organisations that have been breached, realising that they kind of knew what they needed to do but did not realise the urgency. We see that again and again: organisations need to understand the urgency of investing in cyber-security, removing their legacy systems and getting the fundamentals in place to give them a secure foundation for their growth and prosperity.

James Babbage: On the Home Office and policing side, it is too early to say. The Home Office has a settlement, and we are in quite early stages of disaggregating that settlement and working with it on the implications across what is obviously an enormous family of departments.

Q247 **John Cooper:** That brings me to a follow-up point. Although that national spending review did lift spending in some areas, longer term you are looking at potential reductions of 15% in departmental administration spending. That will obviously be a concern—you say it is too soon to say, but you must be concerned about that.

James Babbage: There are two related funding issues, specifically from an NCA perspective. First, can we pay our people enough to attract them, and to keep them in this line of work? The work is very compelling, so that gives us a bit of a lift, but we have said publicly that we feel that we need a different model from the one we have now. We are working with broader Government on that. Our salaries are not particularly competitive compared with policing or the UK intelligence community, and still less competitive against industry, so we need to deal with that.

Q248 **Chair:** Do you want to give us some specifics on that? Pick a rank and tell us what the salary range is.



HOUSE OF COMMONS

James Babbage: I could not do that off the top of my head, but it is very different. The key difference is also that, in policing, people move up a pay scale over time, and in the broader civil service, of which the NCA is part, they don't.

Q249 **Chair:** How much more could they earn doing cyber-security in the financial services sector? Is it a factor of two, three or four times?

James Babbage: Yes, at least that—and they could also earn £20,000 or £30,000 more in policing.

Q250 **Chair:** Sounds like a problem.

James Babbage: That is the first point. The second point is about the overall resourcing levels. Across the public sector, resourcing levels are rising more slowly than pay levels. That is just the way we are in society at the moment. Andrew and I, together, would have a plan to deal with that by leveraging this whole national set of cyber-crime units across forces and regions and at the national level.

They are already closely connected; they are more closely connected than the other serious organised crimes forces than I oversee, but we need to get them even closer together. We have a good pilot in the south-east that connects the regional and local level. The question is: how can we scale that elsewhere in the country and how can we work even more closely together nationally and regionally?

Q251 **Alison Griffiths:** Even under the upcoming Cyber Security and Resilience Bill, the day-to-day enforcement of cyber-resilience is expected to remain distributed to sector-specific regulators. Does that limit accountability and oversight? I am particularly thinking about national infrastructure and the way the EU and the US have tackled that. We seem to be taking a different approach. I am interested to hear your thoughts.

Richard Horne: Clearly, our role is to empower the regulators in that scenario. That is something we do already, and we work with them. One thing that is really interesting is that if you talk to, say, a water company about why they have not invested in cyber-security in the way I would have liked them to, they will tell you that their price is set for a window—though I cannot now remember the regulatory timeframe—and that price drives their capital investment and spend on things such as cyber-security, so you cannot divorce cyber-security from the overall regulated picture.

Cyber-security is about how you run your business and how you run as an organisation, so having the regulation baked into the regulators for that sector is a sensible approach because otherwise you get these two regulators essentially operating in conflict, with one demanding something and the other saying, "You can't". In financial services, we have seen a step change in cyber-security—especially from the big banks—over the last decade, driven by the regulator and the regulatory framework in financial services supported by the NCSE and others. We have a model that works in this country, but we need to make it work across many more sectors.

Q252 Alison Griffiths: Linklaters found that of 99 cyber-incidents reported up to 2024, not a single firm was sanctioned by regulators for breaching current cyber-regulations. Why do you think that is?

Richard Horne: Is that talking about the cyber-regulations being data protection regulations?

Q253 Alison Griffiths: The ICO ones were pretty much the only ones that were live at the time, which I think was part of the problem. That is my view; you are here to tell us your view.

Richard Horne: I think that would be my view. Ciaran talked earlier about the fact that regulation in cyber-security has been focused on data and it actually needs to be focused on the continuity of services much more. That is a shift that is beginning to happen.

Q254 Charlie Maynard: You touched earlier on the top of the tech stack. There is a lot of conversation about the small businesses, but can you talk about the largest big tech businesses in terms of how your relationship with those companies has evolved, how engaged they are in UK security and how interested they are in co-operating with you?

Richard Horne: I will happily answer that. We work across the private sector and work very closely with organisations where we can make a scaled impact. Whether it is big tech, our internet service providers or others, we have a really good working relationship with them. A lot of our advice and campaigns are in conjunction with some of the big tech companies. For example, back in November, working with the City of London police, we had a campaign called "Stop! Think Fraud". A big part of that was about moving away from static passwords and using two-factor authentication. We worked with Amazon, which put out an email to all its users to encourage them to switch to two-factor authentication.

Likewise, we have been working with other big tech organisations on other campaigns. In the background, we work closely with them on some of the more advanced threats that we see. Most organisations would not need to know about those threats, but if you are a provider of big technology that the world depends on, they will be focused on you. We work on that in the background with many organisations.

Q255 Charlie Maynard: Does anyone else want to add anything?

James Babbage: First, UK cyber-security is immeasurably strengthened by the arrangements that Richard has described, and the close connection with those tech firms. There is a little bit of a "but". I described, particularly on the English-speaking side, the platforms and forums that these criminals use to socialise, and those are run by some of the same companies. They are active, to a degree, in trying to identify breaches of their terms of service and to close down particular groups, boards and the like, but, over time, that is still going on. So the broader set of questions on the Online Safety Act needs to be put alongside the strong contribution of these companies to our cyber-security.



Andrew Gould: Just to add to that, we do not suffer from a lack of private sector corporations or partners that want to come and help. What we suffer from is the fact that we cannot manage the capacity of people who want to help because we do not have the infrastructure. We might have a lot of strong organisation-to-organisation partnerships or a joint plan to deal with something—and, in terms of maturity, they have moved on to a firmer footing from the personal relationships they were built on in the past—but there is not the infrastructure or the automatic sharing of data at scale that would really enable them to turbocharge and go to the next level.

One of the interesting things we are doing to address that is bringing in a new replacement for the Action Fraud system, which will come online towards the end of the year. A whole load of financial service companies, tech companies and other partners want to share their data and be part of that as we build it. That will not come in in the first wave over the next year, but those partnerships will build in to allow us to do those takedowns and stop-and-blocks at scale in an automated way that we have never been able to do in the past. So there is progress, but it takes big investment.

Q256 Charlie Maynard: In terms of the Cyber Resilience Act and what the EU is up to there, what do you think the UK should do in response? Should we do something similar here, and where is that transfer of liability best located?

Richard Horne: One thing to note is that we had an Act last year—it has a very catchy title, so I have written it down. The Product Security and Telecommunications Infrastructure Act 2024 mandated minimum standards that manufacturers of consumer devices—smart devices—must meet, so the UK had already taken a step on that journey before the EU. It is a continual evolution, but it would be wrong to portray the UK as totally behind on that.

The cyber security and resilience Bill will be an important step for our critical national infrastructure and services. Then, as Ciaran mentioned, there is a longer-term question about the approach for general producers of software and where the liability should be. We have a software code of practice and a secure by design campaign. The software code of practice is also reflected in US thinking. There is work evolving, but it will be a longer journey to get there.

Q257 Chair: We are almost out of time, but let me ask a final question about the recommendations that we need to draw up. I am interested in your priorities for powers and resources. When you think about the work that you are pursuing, what are the powers that you do not have that you wish you had, and what are the resources that you do not have that you wish you had?

Richard Horne: Powers is a really interesting question. It gets to the heart of the way the NCSC operates and how we are able to create such a collaborative community, in that we do not have any powers. That is really



HOUSE OF COMMONS

important. I spoke to a telecoms company CEO who said, “Just to be clear, if I was talking to you as a regulator, I would have two lawyers with me and it would be a very different conversation; it wouldn’t be collaborative in this way.” A big strength of the way the NCSC was set up, and something I am keen to protect, is that we are not a regulator and therefore organisations want to work with us, want to collaborate, want to get our help and want to share information with us, because they know we are acting not as a regulator. That is really important.

In terms of resources, in my view the way we scale has to be through others, whether that is working with policy departments on legislation, as with the cyber security and resilience Bill, working with regulators to reach their regulated sector, working with private sector organisations that we assure that can provide consultancy, or working with certified incident response companies. We have about 40 certified incident response companies; if an organisation is breached, we can point it to them, it gets the support it needs and the information can flow freely back to us, and from us to them as well. There is a whole range. Then we have Cyber Essentials; we enable 400 organisations across the country to empower organisations to get Cyber Essentials. That scaling through others really has to be at the heart of what we do, and that is very much the ethos—voluntary collaboration and scaling through others.

James Babbage: On powers, the Computer Misuse Act is a reasonably aged piece of legislation. It has stood the test of time quite well—it has been amended a few times—but the maximum sentences for some offences are not high enough to engage some of the investigatory powers that we would wish to and need to use on this sort of complex crime. Also, data is not defined as property under the Theft Act, so an offence of handling stolen data or something along those lines is worth consideration. We might offer to come back to you subsequently, Chair, if we have other thoughts on the powers side.

On incident reporting, which some Members asked about earlier, I would underline the importance of there being a ready expectation of swift reporting to law enforcement as well as to NCSC and regulators. It may well be right that there are different judgments for companies about when they report to different people, so it may not be as straightforward as a one-stop shop, but in law enforcement, the sooner we can know that a company has a problem, the sooner we can go after the evidence that we need to follow up on that, the sooner we can issue protect notifications.

There are good stories generally in terms of the companies you have seen today and how they have worked with law enforcement—I mean no criticism of them—and there are some good stories in terms of the protection of the broader sector that both the NCA specifically and Richard and his colleagues generally were able to do off the back of what they told us, but it needs to be normalised that both the companies and the third-party companies that come in and support them expect that they will be routinely and really quickly sharing with law enforcement, because that can make the investigation so much more possible.



Andrew Gould: I completely agree with what James has just said. The only thing I would add is that we do have some quite good powers in this country, but what we really struggle with is getting the evidence to use those powers. If you think about the challenges we have around encryption and about digital evidence, much of that is hosted overseas. The time it takes to get evidence back from foreign jurisdictions—even friendly, co-operative ones—can be years. These offences are committed in seconds, but it can literally take years to get the evidence and take it to a prosecutor for a charging decision. Anything that can speed up that process would be really welcome.

The other challenge is around digital forensics and accessing people's devices once you have got hold of them, and the challenge of beating encryption. Currently, under section 49 of the Regulation of Investigatory Powers Act, we have the power to serve a notice to a suspect that says, "You need to give us your passwords and your recovery seeds to allow us to access this device." It is an ineffective, ineffectual power. First, you will only get two years for not complying with it, so you will be out in one. If you are being investigated for a murder or serious offence, whatever it is, that is not going to encourage you to comply. Even for terrorism it is only five years. Secondly, there is a further restriction, in that we can only serve that notice if we cannot physically get into the device. We are disclosing to criminals what our capability is by the serving or not serving of a notice, so we do not serve notices. It has become an unused power. That would be a great way of beating the encryption challenge. If they got the same sentence for the predicate offence they had been arrested for, for non-co-operation with police, then it would not matter what was on their devices because they would be put away anyway.

Richard Horne: Can I clarify one thing? I said I had no powers. One thing that we do have, being part of GCHQ, is powers under the various pieces of intelligence legislation to pursue intelligence and understand what our adversaries are doing. Those are really important.

Chair: Anything else, Mr Gould?

Andrew Gould: There is probably something around serious crime prevention-type orders—something more specific for cyber-crime offenders, perhaps to restrict their access to devices and that sort of thing—but that is probably a more minor area.

Q258 **Charlie Maynard:** In other very international lines of work, you would have conferences where you would all get together and talk shop. Do things like that exist? If it is taking years to get stuff, in some ways, that could be because you do not know each other that well.

Andrew Gould: I will be careful how I describe this, but effectively there is an element of jurisdiction shopping. When you come together on an investigation as officers, you will be comparing who is allowed to do what under your domestic legislation. The Dutch may contribute one tactic to an operation, we might contribute another one, and then you bring that together and it is pretty powerful. Again, that takes time. These are



HOUSE OF COMMONS

complex investigations and international work is expensive, but it is completely the direction we need to be taking this work in.

Richard Horne: International collaboration is incredibly strong in cyber-security. We run a conference each year called CYBERUK, and we have a day before it starts that we call day zero. This year we had nearly 40 countries represented at it, and it is Government officials talking to Government officials about how we work together to drive cyber-security.

James Babbage: Strategic cyber-crime co-operation is really strong well beyond the Five Eyes.

Chair: Excellent. That has been a brilliant session. Thank you very much indeed for what you are doing and for your evidence to the Committee.