# Joint Committee on the National Security Strategy

## Oral evidence: Cyber security: UK national security in a digital world, HC 895

Monday 27 March 2017

4.15 pm

Watch the meeting

Members present: Margaret Beckett (The Chair); Yvette Cooper; Baroness Falkner of Margravine; Mr Dominic Grieve; Lord Hamilton of Epsom; Lord Harris of Haringey; Sir Gerald Howarth; Dr Julian Lewis; Lord Mitchell; Dr Andrew Murrison; Robert Neill; Lord Powell of Bayswater; Lord Ramsbotham; Lord Trimble; Mrs Theresa Villiers; Lord West of Spithead; Mr Iain Wright.

Evidence Session No. 1 Heard in Public Questions 1 - 16

### Witnesses

I: Dr Richard Horne, Cyber Security Partner, PricewaterhouseCoopers; Mr Rowland Johnson, CEO, Nettitude; Dr Brandon Valeriano, Reader in Law and Politics, Cardiff University; Mr Ollie Whitehouse, Technical Director, NCC Group.

# Examination of witnesses

Dr Richard Horne, Mr Rowland Johnson, Dr Brandon Valeriano and Mr Ollie Whitehouse.

Q1 **The Chair:** Good afternoon, gentlemen. The Committee is grateful to you for being prepared to give oral evidence to us. We are fortunate to have quite a lot of written evidence as well, so we already have a lot to chew on. This is our first oral evidence session in this inquiry, so I would like at the beginning to put on record some simple context-suggesting questions. You will know that the National Security Risk Assessment categorises cyber as a Tier 1 threat. Do you think that is justified? What would you say is the nature of that threat to the United Kingdom, and how might it be made manifest? Are there any threats to which either the Government or the private sector are particularly vulnerable? If so, what are they?

***Mr Ollie Whitehouse:*** That is a fair assessment of the threat today. As to where it manifests itself, much is made of nation-state capability, and aggressors are targeting the UK and its private sector. Similarly, we should not underestimate the force with which organised crime is embracing cyber capability for various reasons, obviously and primarily to gain direct economic benefit, but, secondarily, by proxy to support certain nation states in their endeavours by creating some clear water, let us say.

***Dr Brandon Valeriano:*** I am bit dubious about the idea that it is a Tier 1 threat. I believe that the cyber threat has been vastly overhyped. We have an intense worry about cyber espionage in information warfare, but a critical infrastructure attack would only be likely in the context of a global war, which is a bit beyond the normal consideration. Most cyber aggressors are using it for information advantages. That is the nature of the cyber threat right now.

***Mr Rowland Johnson:*** I suggest that it should probably be classed as a Tier 1 threat, largely because it has so much impact on some of the other category 1 threats to the UK. Cyber can happen directly, but it can also have an impact on public health and in relation to terrorism, and it can be an enabler for military conflict. Because of that, it makes sense that it should be classed alongside all those things as Tier 1.

The other way of looking at it is that we often talk about what it means from a nation-to-nation perspective, but we should not lose track of the fact that there is a real threat to the population through ransomware. We are now seeing organised crime units trying to monetise attacks by targeting end users, encrypting their laptops and having an impact that is probably much more frequent on a day-to-day basis.

***Dr Richard Horne:*** I would come at it from the consideration of exposure. We are a digital society, whether we like it or not. Almost everything that we do that is physical has a set of digital processes behind it, so we are incredibly vulnerable to those digital processes and

data flows being interfered with. Much of what we do as a society depends on them. In hospitals, for example, not only very physical things such as operations but a whole load of scheduling, blood ordering and all the things that go on in the background are digital processes. Without those digital processes, a lot of our physical world would deteriorate. It is absolutely a Tier 1 threat, less because of the threat today but because of the vulnerability and the possibility that a threat could materialise very quickly.

**The Chair:** Having established that three of you think that it is a Tier 1 threat, although one of you has some doubts about it, and without wanting to scaremonger, what is the worst-case scenario for a cyber attack on this country, and how likely is it? As you will know, the whole point about the risk register is that it is a mixture of impact and likelihood.

***Dr Richard Horne:*** Without getting into the specifics of what could happen, a likely scenario is where the ability to function of our financial market, much of our health system, our electricity and our critical national infrastructure could be disabled or severely impacted. Interestingly, for many of the adversaries who might want to do that, there have until now been other geopolitical bounds that might cause them not to do so, but as capability becomes more accessible to criminals and terrorists, there is less of the normal diplomatic and political bounds around behaviour to constrain them.

***Mr Ollie Whitehouse:*** I agree with that. In the UK, by virtue of our maturity, we adopted technology early on, and because of that we have legacy systems that run some key elements of our country. That provides unique challenges. We have some ageing systems and there is an increasing capability that may not intend to take those systems down but which through exploration and success in compromising may have an inadvertent outcome for them. If the worst happens, it may not always be intentional. That is something to bear in mind.

***Mr Rowland Johnson:*** My comment would be to use your imagination on what it might entail. What do I mean by that? I mean anything that draws on data and information or anything that touches currency in trading. I read an article last week on the BBC website about the fact that farmers are now using data to make decisions about how much fertiliser to put on their crops. The suggestion was that, if a hacker could get access to some of those systems and manipulate information, in theory there could be a scenario where we had insufficient levels of crops being produced, which might result in some form of famine. Similarly, you might come up with another scenario involving the industrial control systems that power our manufacturing, many of which touch data networks. As a result, if somebody straddled a data network, they could get access to industrial control systems. That individual might be able to do all sorts of things. We have seen some of that out in Ukraine and in some other countries over the last two years.

***Dr Brandon Valeriano:*** The problem is that we cannot make policy based on worst-case scenarios. We need policy based on probabilities and actions that are likely to happen. Aggressors have had this technology for over 30 years and they have been generally restrained from using it for aggressive purposes. Terrorists are not so restrained, but they do not necessarily have the capabilities of nation-state actors. The real difference is in who the aggressor is, who their target is and what their goal is. The clear thing that we need to worry about is a general societal programme to promote resiliency within the state to recover from possible cyber attacks. A dramatic cyber attack is, as I said, only highly likely in the context of a major war with Russia or China, which is not necessarily on the table. So will this happen any time soon? That is something out of the imagination and it is not how we should govern. We need to govern based on what is likely to happen. We have not seen cyber technology used for great massive effect so far and we are unlikely to. We have seen sabotage, but that has generally been done by main nation states to attack left-of-launch capabilities to prevent other countries from acquiring certain technologies. We have not seen any great devastation so far and I do not think that we are likely to any time soon.

***Dr Richard Horne:*** If I may counter that slightly, from a policy perspective we cannot say that we will deal with it when it becomes an issue. We are building the future digital society today. If, in 10 years' time, we find ourselves in a conflict situation, we will not be able to rewind the clock 10 years and say, "Let's rebuild a secure digital society". There is a policy imperative to build a secure society, without necessarily trying to anticipate what the threat may be or may become in the next five or 10 years, because we have to build today for the future.

***Mr Ollie Whitehouse:*** I agree with that. Brandon used the important word "resiliency". The free market, if left to its own devices, will make money, which is a wonderful thing, and security is, to a greater or lesser extent, not seen by buyers as a key point at the moment in that purchasing decision. Our resilience is probably not where it should be, which is where the national cyber strategy outlined the levers and incentives model and where we need to take a long hard look at how we increase that resilience.

**The Chair:** Would I be exaggerating if I were to say, from what all of you have said, that if you had to say where the balance of investment should go you would put it into resilience rather than defence or just stopping attacks?

***Mr Ollie Whitehouse:*** Indeed yes, I think we recognise now that the concept that you are either secure or not secure—a binary state—has long gone. You need to be able to deal with successful attacks with varying degrees of impact and recover accordingly, with the minimum level of disruption. That is why resilience is now a key concept in cyber security.

***Dr Brandon Valeriano:*** We throw this term around without really defining it or saying what needs to be done. The key thing would be look at investing not so much in the public-private partnership but in education—investing from the ground up. The other thing that we need to start to invest in is the public, by promoting how they might react to a cyber threat or a cyber attack. We have not really done that. We did that back in the nuclear era but we are not really developing these new programmes to manage the emotional reaction that will happen, because of our digital dependency.

**The Chair:** That is a very good point.

Q2 **Yvette Cooper:** You talked a bit about the cyber threats to public infrastructure and to the private sector. In the light of the experience of the US elections, what is your assessment of whether there is any sort of cyber threat to British democracy—either to democratic institutions and electoral systems or to political parties, Parliament and so on?

***Mr Ollie Whitehouse:*** If we look at what happened in the United States and the primary means taken to manipulate the message and to try to influence public understanding of the situation, we are obviously susceptible to that by virtue of having free and open media in a highly connected society. To say that they would be able to influence how someone casts their ballot through the pencil and paper that we still employ would obviously be going too far. But in terms of leaking or manipulation and propaganda, we have to accept that that is a practical means which they can employ.

***Dr Richard Horne:*** There is a really important general principle to do with how attackers think in cyber space, which is illustrated by the question about elections. Whether it is in online banking or all sorts of attack scenarios, we see that the attackers will often not target the core system itself, which you are trying to defend, but manipulate the inputs that go into it in order to get a different result. In the discussion on elections—we know that the head of the NCSC has reached out to political parties to talk about their security in this context—there is a really important principle. You may not be able to influence the casting of votes themselves, but if you can influence the data on which those decisions are made you might be able to influence them. That is a really important principle for how attackers attack in this space. If political parties' emails could be breached and then selectively leaked, maybe to present a coloured view of what that party or its individuals stand for, that is the kind of concept often used in cyber attacks.

***Dr Brandon Valeriano:*** We have to be clear about the US attack, though. It was mainly done through third-party applications and third-party emails, by people changing email passwords based on spear-fishing. It was the least of the least in terms of cyber tactics. The real problem with the American electoral system right now is the lack of trust in the media. That is the question you have to ask yourselves internally: "Do we trust the BBC and our media?" In America they certainly did not, and they trusted Russia Today—RT—quite a bit, to the tune of 9 million

views for a video about Hillary Clinton taking money directly from her foundation, which of course was not true. It is really a question of trust, and where people get their information from and how they are educated to take in information. We tell ourselves these stories about this dramatic Russian hack of the election, but the story was really much simpler than that.

**Lord West of Spithead:** I am interested in Dr Valeriano's take. I put a huge amount of work in with the Americans on Y2K. There was an immense amount of work on Y2K and it never quite came to what we thought. Although some of the things that we did were good, thousands and thousands of man-hours were spent on it. We had some useful data, such as on the Quebec ice storm and the impact on a populace when they suddenly lost cashpoints and could not buy food, et cetera. That could be used in this context of what would happen in a cyber attack.

I suppose my question—this never came up on Y2K—is about resilience and recovery. Do you believe that sufficient money is being spent, primarily by commercial companies, on their recovery procedures for when things go slightly wrong? Is there any role for legislation in forcing certain types of companies to have proper recovery mechanisms in place?

***Dr Brandon Valeriano:*** There is a role, which is why we need to start to look at the cyber insurance industry that has popped up. It is not necessarily regulated at this point and we really need to think about whether these people are going to pay out if there is an attack. Are they encouraging good practices? We do not really talk about what the good practices are or about how the majority of companies use IT departments to handle their security when they really need cyber security groups now. That is the real imperative: we need to understand the nature of the threat and how to respond to it. But I worry that we focus too much on the offence, and are not doing the things that you are talking about, by interrogating what we are doing on a defensive perspective first.

**Baroness Falkner of Margravine:** Going back to the earlier point, the impression one got from most of you on the interference in democracy and electoral systems was by implication that there is manipulation rather than a direct impact. Angela Merkel has now come out I think three times to warn of interference in the forthcoming German elections. Why is she so concerned?

***Dr Brandon Valeriano:*** There is a realistic threat. The Russians have been engaged in this activity for a long time in Europe. Just by putting that warning out, she is triggering the population not to respond to these information attacks. As I said, the issue with the Americans is a lack of trust in government. The hope is that Germans have more trust in government to respond and fight back the attacks that will inevitably come.

***Mr Ollie Whitehouse:*** The BSI, Germany's intelligence agency, came out today to say that it had caught a known threat actor group, aligned

with Russia, in trying to compromise various systems. That is where her concern would have emanated from, based on that hard evidence.

***Dr Richard Horne:*** Three of us are in companies that deal with threats and respond to incidents when they happen. We help companies in the public sector to deal with it and the threat is real. You cannot deny that there are people all over the world whose day-job—they work 9 to 5 in their local time, take lunch breaks and go on holiday—is to get into networks and compromise digital processes for whatever means. If they are criminals, it is often for financial gain. If they are nation states, it is often to lay backdoors that they can exploit in the future or to get information out. There are armies of people out there, and that is their job.

Q3 **Lord Harris of Haringey:** We are obviously focusing on the Government's national cyber security strategy. What would you see as the key lessons learned from the 2011 strategy and was it effective? Do you think those lessons have been sufficiently addressed in the 2016 strategy?

***Mr Ollie Whitehouse:*** There are two key things coming out of the most recent strategy. One is the tacit acknowledgement that there may need to be regulation—I guess you might call it incentives. The other is capacity-building in skills, and as we have already seen in enacting that policy it is about getting to the younger generation now. We are talking about ages 11 to 15, so that there will be a material benefit for us in six years or a little later—whenever they enter the workforce. That is key, and it addressed a lot of the shortcomings in the previous strategy.

***Dr Richard Horne:*** I was in the Cabinet Office in 2011 and took part in the first one, so clearly it was brilliant for its time. The thought process back then in 2011 was very much that the Government could encourage the private sector, on which much of the dependency for action sits, to understand the risk and take action appropriately. What has become clearer is that the Government may need to be a bit more active and make more interventions. The establishment of the National Cyber Security Centre is a very welcome initiative in driving innovation and working with some of the infrastructure providers in the UK to tackle what I would describe as a lot of the noise at source. If we remove a lot of the low-level activity that is going on, people can then focus their efforts on the more sophisticated activity that is happening.

***Mr Rowland Johnson:*** I agree. One of the challenges with cyber is that leaving things to market forces sometimes does not lead to quite the results that you might imagine. Often, cyber security is regarded as being a bit of a lemon market in which there is an asymmetry of information between the people who buy services and those who sell services. What does that mean? If you are a seller you might understand a lot of three-letter acronyms and the complex details about threat and risk, whereas if you are a buyer a lot of those things are confusing and difficult to understand. Cyber is a realm where market forces alone probably do not come up with an appropriate level of response, and we are now seeing a

greater need for some form of regulation to try to define the bars for people to strive for.

***Mr Ollie Whitehouse:*** When we talk about regulation, it is important that we do not necessarily see it from our perspective as universal. Regulation has to be proportionate to the criticality of the firm and the services that it provides to our nation. As long as we take that into account—we have already seen certain regulators take a lead on this with that proportional approach—we absolutely see good responses from the firms in question, and an improvement.

Q4 **Lord Harris of Haringey:** It sounds as though you are all saying that the market has not really delivered in this area, perhaps because the vendors are selling people products that they do not really need and certainly do not understand. Is that how we should interpret the emphasis on active cyber defence? Is it essentially an admission that the existing strategy is not working or is not going to work?

***Mr Ollie Whitehouse:*** Active cyber defence addresses two problems. One is partly that, but it is also that active cyber defence helps those who cannot help themselves. Cyber is a complex subject and there is an assumption that there are skilled people on the purchaser's side, but the majority of the firms in the United Kingdom are SMEs, which cannot retain the requisite skillset to have that informed discussion. Active cyber defence provides those types of firms with some meaningful defence against actual threat actors in the real world. That is where we have to look for its benefit.

**Lord Harris of Haringey:** More generally, is the 2016 strategy really robust enough for the protection of the UK's critical national infrastructure? We have seen the recent attacks on Ukraine and in France. Has the latest strategy learned the right lessons from those major attacks? You will probably have seen the recent US Defense Science Board report, which essentially said that actors on behalf of the Russians and Chinese had effectively penetrated the US's key critical national infrastructure to the extent that it presented the opportunity to switch off that infrastructure, which would obviously have existential consequences for American society. Are we facing the same level of potential threat, and has our infrastructure been penetrated to that extent? If so, what can we do to deal with that, given that I think the US Defense Science Board said that it would take at least 10 years for the US to rectify that position?

***Dr Richard Horne:*** The honest answer to your question is that no one knows. To some degree, you can take confidence in some of the things that happened, but at the end of the day, in the US story that you referred to, they did not know what had happened until it became clear that it had. Part of the challenge for the national strategy is that this area moves very fast. One thing that may need to be thought about in the context of the national strategy is that a five-year cycle may not be agile and rapid enough to deal with the world as it develops and with our dependencies in the digital world, since they develop much faster than

that five-year rhythm. A more agile approach to refreshing and revisiting the strategy might need to be thought about.

***Mr Ollie Whitehouse:*** I have a slightly different perspective. A lot of the things that we are calling for, be they new regulation or active cyber defence, take a while to build and thus for their benefits to be seen if they are to produce them. There will always be an anxiety that if you shorten the life cycle—if you shrunk it down to three years or something—you would not have fair and true data on whether it could work and deliver.

On your point about whether critical national infrastructure is compromised to the same extent, I do not think that any of our commercial companies would be willing to comment on client relationships, but it is fair to say that when presented with a determined and capable threat actor, most organisations will likely suffer a degree of incursion.

***Dr Brandon Valeriano:*** The reality is that these major actors each have 6,000 to 10,000 cyber operatives. They will target anything and everything they can, and we need to be prepared for that. I do not know whether we are doing the routines or the stress tests that we really need to do to make sure that our critical infrastructure is prepared. We cannot even survive major rainstorms sometimes, so there is a question of whether we can really survive these possible attacks. I do not think they are likely, but they are possible.

***Mr Rowland Johnson:*** Another way to look at all this is that instead of the focus being purely on defence we almost have to come to a mindset whereby we accept that at some point we will be compromised. The mindset needs to move to being more about how we detect and respond to those types of attacks. If you think about it, the aggressor needs to find only one way into an organisation; the defender needs to defend against every attack. Again, there is an asymmetry there. When the threat landscape covers not just technology but people and process, that is an awfully large landscape to try to protect. We are targeted at home, as employees of the organisations that we work for but also as people in the community. Our wives and children are potentially targeted. In theory, a determined threat actor might be able to pivot through all those connections. If you take that as the starting point and assume that if somebody was really determined they would get in, the focus should be on that ability to detect and respond.

**Lord Harris of Haringey:** Can I ask one more question before we move on? For those of you who work closely with private sector companies, some of which are infrastructure providers but many of which will be suppliers to the infrastructure, to what extent do you find that they already harbour compromises on their systems? I would not want you to breach client confidentiality, but you might give us a general impression. They may not know about those compromises, and there may not be much they can do about them.

***Mr Ollie Whitehouse:*** You raise a really valid point, because the supply chains are where it gets very murky. A firm that has to report to a regulator can report only what has happened and what it knows is true. We see organisations increasingly starting to look at their supply chains as a source of systemic risk to them because of the reasons that you outline. How can they have confidence that the much smaller firm that they engaged, and which may have connectivity into their environment, can itself detect an attack on their organisations that could be successful? That is where it is found wanting today, in an awful lot of suppliers, because typically they supply a magic widget or provide something niche but do not have the fully fledged systems because they are not necessarily a multidisciplinary firm. We see increasing sources of risk there.

***Dr Brandon Valeriano:*** The majority of successful attacks in America come through third-party contractors, so the supply chain really is the worry. A lot of the things that we do are done for a cost-benefit analysis. You sometimes need to spend a lot more to ensure your security, and quite often we fail at that.

**Lord Mitchell:** To what extent are these larger companies putting in criteria for small suppliers to meet obligations?

***Mr Ollie Whitehouse:*** The Cyber Essentials scheme is definitely being used by some, and there are contractual obligations, but the beauty is that it is the written word. If the supplier has no material capability to know whether something has happened, there could be any obligation to inform that you might wish, but if it does not know it cannot tell. The reality—this goes back to Brandon's point—is the cost-benefit analysis. If you outsource to them because they are cheaper at something or very specialised, you will not put such onerous requirements on them that erode the saving that you get. There is a fine line to walk there.

***Dr Richard Horne:*** It is causing some organisations to rethink some of their organisational decisions. My belief is that cyber security is not so much a technical issue as how you construct your organisation and its processes. The number of dependencies that you have on others is a key part of your risk. Some of the outsourcing and supply-chain decisions made in the past, which were driven purely by cost, may need to be rethought. Organisations may need to reconfigure themselves so that they have more end-to-end control over those processes, but they will still never be able to eliminate the supplier risk.

Going back to my earlier comments, the common feature of almost all cyber attacks is that they go not for the core but for the inputs. The suppliers, and suppliers to suppliers, can often be part of that thinking.

***Mr Rowland Johnson:*** Over the last three years, we have seen a lot more intelligence-led assurance frameworks. Instead of trying to deliver assurance exercises that look at organisations straight on, these try to look at other interconnecting elements around the organisation. That may not be quite as far-reaching as the supply chain, but they certainly look

outside conventional tech in the UK. We also see a growing number of attacks with relevance to the UK that target subsidiaries and other operating functions for multinational organisations that are outside the UK.

Q5 **Dr Andrew Murrison:** To what extent will the General Data Protection Regulation, and the big fines that it will potentially introduce from April next year, affect the supply chain that is being discussed? Are they going to alter behaviour significantly or not?

***Mr Ollie Whitehouse:*** Yes, there are certain firms today that are anxious about GDPR becoming active. That will definitely drive more of an invasive look at certain suppliers that process personally identifiable information.

***Dr Richard Horne:*** One of the things to watch is that the General Data Protection Regulation provides a strong regulatory environment for the protection of personal consumer information. But from a national security perspective, many of the cyber attacks that might concern this Committee are less about consumer information and more about attacking infrastructure and disrupting processes, including military processes. There is a strong regulatory regime coming in for protecting consumer information. We need to watch that it does not skew companies' defences to focus overly on it and not think about the disruption to their processes.

**Dr Andrew Murrison:** But there would be public health implications, for example, in accessing healthcare data.

***Dr Richard Horne:*** Absolutely. That is right.

Q6 **Lord West of Spithead:** I should have declared an interest in that I am chairman of a company that works in the cyber area. I also speak a lot on cyber—for which I get a bit of loot, which is quite nice. Lord Harris asked about the American report, which I have also read. It actually said that there are lines of code already in masses of the software in whole areas of the US and it is not known how they can be sparked. I would like to run on from there.

How dangerous do you think it is that switchgear and other bits and pieces from Huawei, for example, are incorporated into masses of systems? We do not know how the upgrades go unless we specifically put CESG on to this to look at it closely. A Chinese firm has now taken on the largest data centre in the UK, and the Chinese have just taken over the largest CCTV company in Europe—and we all know what you can do remotely with CCTV and the internet of things. How much threat and danger do the panel see in that, particularly when one takes these lines of code into account, which we already find at times? Let us face it, CESG might go in and say, "My God, we didn't know that was there". How much of a threat is this?

***Mr Ollie Whitehouse:*** For anything done deliberately, the pure software quality will outstrip that by an order of magnitude. So with any backdoors

introduced into these lines of code, the number of unintentional weaknesses present in software and hardware systems today far outweighs them. Again, that is because of the economics driving it. In a lot of cases today, none of the things like quality assurance and good architectural principles make sound commercial sense, so what we can attribute to malice we sometimes have to attribute to pure neglect.

**Lord West of Spithead:** Sorry, you did not really answer my question. You do not think that these companies doing this is not an issue, then?

***Mr Ollie Whitehouse:*** It is obviously an issue, but for those that are capable of bringing that force those same systems will be vulnerable to many other things which those actors did not introduce. I would be more worried about that when we talk about the internet of things in particular, because we expect those products to have a half-life of between three and 10 years at the outside. They have a very cheap price point. Where do we think firms can produce to that point? They do not have sound security engineering in them, which is why we see a regression of what we have learned in hardware and software security design over the last 30 years. That is being undone with the advent of the IoT, because we are moving away from three or four massive multinationals, which can invest heavily in cyber security product design and implementation, to many smaller manufacturers churning products out as quickly as they can. There is no company to hold to account, but you would not necessarily cut off an entire country from supplying to you today.

***Mr Rowland Johnson:*** I would add that you could assume that there is definitely a threat from lines of code, as you describe, but equally there is a threat from people and process. The Mirai worm that went out at the end of last year targeted a whole load of IoT equipment, and a lot of what it did to propagate initially was just to use weak credentials. We should probably focus on the problems that we still face of people choosing bad passwords and usernames and putting no kind of security configuration on to devices. That is the low-hanging fruit. We need to think about the code that powers a lot of these systems, but it is much more than just the technology alone.

**Lord West of Spithead:** So why did America and Australia say, "No, we're not going to use Huawei kit"? If it is as you say, are they not buffoons who are obviously not doing things correctly?

***Mr Ollie Whitehouse:*** The UK had a compensating control by creating a security cell. As a country, we cut a specific commercial agreement with Huawei to have UK people in an area to provide a level of due diligence over that code. They report independently every year, so instead of cutting it off entirely we realised the commercial benefits. But we also put in compensating risk controls by having those individuals be British nationals who could review the products that it produces.

**Lord Powell of Bayswater:** As a quick addendum to that, is it just possible that American concerns about some Chinese companies such as Huawei are caused by competition factors, because they do not want

Huawei in their market?

I take silence as consent.

***Dr Brandon Valeriano:*** There is a certain amount of prudence, though, in avoiding our past mistakes in intelligence and making sure that we do not diversify that much. That has been the path forward: to be careful about what we let in. I am not as worried about lines of code as about the actual physical hardware. That is something that we are reluctant to change through time.

***Dr Richard Horne:*** We need to recognise that from a national security strategy perspective we are in a position of weakness in this area because we do not have our own technology supply base in the UK to manufacture the core infrastructure that we need. Other countries have the luxury of that supply base.

Q7 **Mrs Theresa Villiers:** The 2016 strategy contains a list of categories of cyber threats: cyber criminals, states and state-sponsored threats, terrorists, hacktivists and what I gather are known as script kiddies. I would be interested to hear the views of you all as to whether it is useful to categorise the threats in that way.

***Mr Ollie Whitehouse:*** Yes, in so much as it makes it real to businesses and users. They need to understand who they are defending themselves against and their motives, so we need some form of categorisation. At the moment, that relatively core set is probably a good measured balance—from the archetypal teenager in their bedroom, who is a bit bored but massively inquisitive, through to the nation-state threat that you see in the Hollywood movies.

***Dr Brandon Valeriano:*** Method and target are critical, because each threat group will have different methods and targets. The nation state will focus on cyber espionage or a critical infrastructure attack; information and critical infrastructure would be its targets. That division tends to be useful for parsing out what we need to protect and what is more critical or important. The nation state is a more capable actor. Then comes the terrorist, then the criminal and then the script kiddie—the basic chaos type of person.

***Mr Ollie Whitehouse:*** My only caveat would be nation states. When we communicate with clients, we differentiate between established nation states that understand the international norms for using this capability and emerging nation states. Those developing cyber capability rapidly may not be used to sanctions or anything else placed on them when they go too far, or having other sticks wielded at them. It is important because the disincentive, as we have seen in certain public instances such as with Sony Pictures, is that they are happy to use that capability to quite aggressive effect.

***Dr Richard Horne:*** One thing I would caution against is seeing them as too distinct. This area is essentially a marketplace of adversaries. If you were a nation state with a hugely sophisticated armoury and wanted to

get access to a company, you might try first to buy access through a criminal forum because you could make it look like a criminal attack and would not have illuminated any of your more advanced techniques. We see quite a lot of that potential activity happening. It should be recognised that this is a marketplace. A nation state can deploy a tool that can be available for criminals to buy and use within days. We saw that with one called Poison Ivy many years ago.

**Mrs Theresa Villiers:** That partly anticipates my next question. It will be interesting to hear from the rest of the panel where you think the key overlaps are between these different categories.

***Mr Rowland Johnson:*** To pick up on an earlier point, the overlap is definitely significant and is becoming more and more so. The modi operandi might remain distinct, but the level of sophistication and capability is continually growing. The cyber security strategy refers to different levels of capability. You might say that organised crime units have a different level of capability compared with that of nation states, but the gulf between those is beginning to blur, so you might assume that that will also continue to blur down the stack.

Script kiddies and other people who might be regarded today as having unsophisticated tooling can still have a significant impact on infrastructure. One of the large breaches against a telecoms provider a couple of years ago was disproportionately devastating for it and was committed by somebody who would have been regarded as a script kiddie but who had a large financial impact on that provider.

We should not assume that nation states are the only type of entity that can inflict significant damage. The reality is that all of them can.

***Mr Ollie Whitehouse:*** I agree. On a technical level, organised crime groups and others are getting very close, if not the same, in what they can unleash. The difference is generally planning, co-ordination and capacity to launch, which is the difference when we talk about nation states and upper-end organised crime. But on a purely technical level, going one for one on one engagement, they can be approximate now.

***Dr Brandon Valeriano:*** They are not getting that close. The real issue is that Russia and China will identify and utilise the people who have the capabilities. They will identify them early and pull them out and tell them basically, "If you don't work for us in addition to your day job, you will have trouble". That is the real thing. There is no mythical cyber criminal who has these dramatic capabilities. Generally what they do falls in line with what we call shrinkage: assume losses by revenue or volume. In the American cases of dramatic attack in the last 10 years, the only one that was beyond a shrinkage calculation was the Target attack.

**The Chair:** May I stop you there? I am afraid we have a Division in the Commons. I will adjourn the Committee for 15 minutes.

*The Committee was suspended for Divisions in the Commons.*

**Mrs Theresa Villiers:** I have two more questions. A lot of the material that I have seen so far tends to indicate that terrorists, although they have malevolent intent, have limited capacity in relation to cyber attacks. Yet we have these relatively low-tech script kiddie-type categories. How come that kind of individual teenager in their bedroom can inflict harm that seems to elude terrorist groups? Is there more scope for them? Should we be worried about a particular overlap between those two categories in our cyber security response?

***Mr Ollie Whitehouse:*** One reason historically attributed to that is stability: terrorists generally have various instabilities, either in their life or their physical environment, which preclude them from getting access to the computing facilities, the technologies or the education required to do some of these things. But you are right to highlight the risk. As we have seen with organised crime, young capable individuals who are persuaded, cajoled or otherwise influenced to undertake the activities at someone else's behest are a risk. That is why we have to look at what the National Crime Agency has been doing on intervention. The agency identifies younger people who might be on the wrong path, sits down with the parents or sends them a letter saying, "Do you know what your son or daughter is actually up to? Maybe you need to be a better parent".

***Dr Brandon Valeriano:*** If these individuals are successful, that quite often says more about our lack of defences than their abilities. That is a huge problem. These sorts of malevolent enterprises by youths have always been going on. It is like a status competition. Their enduring nature for attack is not really there compared with that of the terrorists, but as Mr Whitehouse said the terrorists have a problem with infrastructure, setting and education.

***Mr Rowland Johnson:*** Those different threat groups have different modi operandi. Quite often, script kiddies are looking to go out and attack systems, but they do not necessarily care what the system is or who the entity is; they are looking to try to gain peer notoriety. That is slightly different from a terrorist group, which might have a very specific focus on a very specific set of end goals. It is reasonable to assume that, again, as technology and the skills of the people who are practising these types of attacks develop we will see more terrorism-driven attacks in the future.

**Mrs Theresa Villiers:** One last question, which in a way takes us back to the very first questions that you were asked at the start of this session: which of the categories in the 2016 review poses the biggest threat? Is it the criminals, the state actors or the upper categories?

***Mr Ollie Whitehouse:*** I guess the corresponding point back to you would be about availability, the long-term financial health of the United Kingdom, et cetera. Again, you have to take each of those on their merits. You can talk about nation states, long-term economic competitiveness and the viability of the nation, but it will be someone completely left field who will cause the unforeseeable event to happen just because they are willing to go there.

***Dr Brandon Valeriano:*** Certainly nation states are the most capable, but the probability of those actors targeting us, besides through information warfare, is very low. I guess the main threat now is cyber crime and crime enabled by cyber activities. The real thing that people are not really talking about is what we are going to do once Brexit happens and how we divest from the European Union. That is the real question that we need to dive into, and I have not seen a lot of positions on the actual impact on regulation, on crime industry, on the use of Interpol and things like that.

**Dr Andrew Murrison:** Why do you think Interpol might be affected, given that there are so many signatories to Interpol that are not members of the European Union?

***Dr Brandon Valeriano:*** I do not really know what the impact of Brexit will be on British cyber security capabilities. That needs to be interrogated. I have been encouraging students to do so, and they have not gone that far with that.

Q8 **Dr Andrew Murrison:** To what extent do you believe it is possible to distinguish the source of cyber attacks? I think you have touched upon it already in some of your remarks, but it is obviously important when one tries to attribute these sorts of interventions, and it has a bearing upon what we might then do, collectively or otherwise.

***Mr Ollie Whitehouse:*** If you are ever thinking of launching a kinetic response, I would say that it is very dangerous to rely on attribution in cyber to do that. It is a very, very hard problem to solve. Today, we have levels of confidence, but I do not think that we as the private sector can say categorically, without further government advice, that we know for sure. We know that they exhibit the traits and the modus operandi, but those are all copyable. Something might originate from a computer network that happens to exist in a country, but these are all capabilities that can be amassed by someone who wishes to misrepresent themselves if they so wish. I would always caution against attribution categorically.

**Dr Andrew Murrison:** So it is the ideal proxy weapon.

***Mr Ollie Whitehouse:*** Indeed.

***Dr Brandon Valeriano:*** That is a bit of an overstatement in some ways. Attribution is easy. What is difficult is responsibility: finding that chain of command, finding the leadership from the top saying, "Do this". That will never be there, but was it ever there in any form of armed conflict? It is not clear that it was. We have gotten better at attribution through the years. We are seeing more cyber activities being used as signalling and that the states actually want us to know what they are doing so that they can push us in a certain way. I do not worry too much about attribution. Being able to pin it on a figure so that you can say, "This person did it", is really difficult, especially with states like Russia and China.

***Mr Rowland Johnson:*** I agree with Mr Whitehouse. It is very difficult to attribute attacks. It is quite easy to subvert an instant responder or

somebody who is looking at malware and point them in the wrong direction. With some of the attacks that occurred last year—I have already mentioned Mirai—initially there was the narrative, "This looks like it might be a Russian-based attack", the rationale being that there were some Russian words inserted into some of the code. But in reality it is not difficult necessarily to insert some Russian code to make it look as though it is somebody from another nation state.

Similarly, things like Tor are used to try to disguise where people come from. You talked about proxies. Again, these are very common. Quite often, where it is possible to attribute an attack back it is more because the attacker made a mistake; they did something to provide that attribution. But if they are working effectively, it is very difficult.

***Dr Richard Horne:*** I would echo those comments. Attribution is fundamentally an intelligence activity, and it comes with degrees of confidence.

Q9 **Dr Andrew Murrison:** I suppose none of you would particularly recommend that we extend Article 5 to this particular sphere.

***Dr Richard Horne:*** Numerous issues would have to be worked through. That would be a hard area to work through.

**Dr Andrew Murrison:** One possibility, of course, might be that you respond like for like. One could make it more explicit that anything one might deploy is as a result of our intelligence, which we believe is reliable, that a particular state actor is responsible for something that we have picked up.

***Dr Richard Horne:*** That could be one possibility. You would then have the danger of a sort of spiral effect.

***Dr Brandon Valeriano:*** When the Americans respond, you generally see them do so at a lower level with things like sanctions or attacking Russia Today's base of money. They do not necessarily respond with cyber attacks, because that might unleash the metaphorical Pandora's box. We do not want to enable the actor and let them continue their operations by doing that ourselves.

**Lord Powell of Bayswater:** Surely one should not be too pessimistic about Article 5 and its application. It is about collective defence, and if a small country in NATO, let us say Estonia, were subjected to continuous assault in the cyber sphere, surely it is quite right for countries to get together to take action. It does not have to be a nuclear war; they could put on sanctions or various other things. Including cyber in Article 5 was actually a very sensible decision, and I am not quite sure why such objection is being raised to it.

***Dr Richard Horne:***, If you viewed it from the British perspective, one counterview to consider is that if a criminal organisation in the UK launched an attack against a foreign entity and the UK was held

responsible for it rather than it being seen as criminal activity, we might feel slightly different.

**Lord Powell of Bayswater:** I would hope that we would feel very guilty and get to the bottom of who had been doing it. That would be the right reaction.

***Dr Brandon Valeriano:*** The real thing about Article 5 is that there should be actual physical violence attached to the cyber attack. That has been rare up to this point, but if it were to happen, theoretically the answer would be yes. However, the probability of physical violence through cyber attacks is conjecture.

Q10 **Baroness Falkner of Margravine:** One problem is that the whole NATO regime, and the general UN Security Council regime, was built around more conventional warfare, although it has adapted to be more hybrid—some might not like the expression "hybrid". To what extent, alongside attribution, do you believe that the state-to-state environment has become safer through the inclusion of something like collective defence under an enlarging NATO, since the inclusion of cyber came in? It seemed to come out of the blue last year at the Warsaw summit.

***Dr Brandon Valeriano:*** From my perspective, collective defence leads to collective offence, and that leads to escalation, so that is a bit of a problem. It is each country's decision whether it wants to move forward—and push NATO to go forward—with a collective offence. That is a major threshold, which I hope we will not get far enough to talk about.

***Mr Ollie Whitehouse:*** On collective defence there is a case to be made that as power generation does not necessarily occur purely on our island, and we consume from other partners in the European Union, having a collective defence strategy ensures that our country functions for certain things. We are not self-sustainable in food production and all these things, so as those can be impacted by cyber events it would make sense to look to take a more combined approach.

**Dr Julian Lewis:** Would it be possible to break down the different cyber threats into certain categories? I have come up with three, but they may be inadequate, and I wonder whether you feel I am missing anything here.

The first category is using cyber for gathering intelligence, whether commercial, political or military. That clearly requires defending against; hardening your systems and making sure that they are as well protected as they can be.

The second was talked about in relation to the US election: the use of cyber in quite a traditional method with regard to any communication system for the dissemination of propaganda, disinformation and misinformation. For that, your best weapon is to get your own messages out and expose the fact that your opponents have been doing dirty tricks.

The third, which I should think concerns us most in relation to NATO,

because the other two are bound to go on as long as there is a cyber sphere, is of attacks that could paralyse societies. Although you may try to prevent those, that is surely where the concept of deterrence and the threat of retaliation would come in. There, I am inclined to think that Dr Valeriano is right: if it got to that stage, conventional military action would probably be going on at the same time anyway. Have I missed anything in the spectrum of threats that would not fall into one or other of those categories?

***Dr Brandon Valeriano:*** I think you are right. I have been writing a book on this very topic that is almost done. We divided cyber into three activities. You include information warfare and mentioned operations, which traditionally are not included in cyber but are an adjunct part of cyber. That is what cyber really is: the adjunct methods. We divide actual cyber tactics into disruption or harassment; espionage or the manipulation of information; and the degrade options, which are to deny, sabotage or destroy the targets so that they behave in a certain way. Those are our three main categories, and they seem pretty comprehensive for most nation state-based cyber attacks.

***Dr Richard Horne:*** That is probably true for nation states, but when you get into the criminal sphere you can have different impacts that are equally large.

**Dr Julian Lewis:** I want to concentrate briefly on the defence side, because the issue then arises of how you deter something like this. The only real way to deter something is to have a threat of retaliation that is both unacceptable and unavoidable. That was not unknown in the past. Between the wars it was thought that the great threat was gas warfare, so a lot of resilience was put in and every household had a gas mask. It is generally accepted that it did not happen in the end because the threat of massive retaliation by this country was an effective deterrent. Can you envisage a threat of massive cyber retaliation that would be effective in deterring that third category that I talked about: attacks that are seriously intended to paralyse societies?

***Dr Brandon Valeriano:*** In short, no. There is intense disagreement in academia. The majority of academics do not believe that deterrence has ever worked even in a social construct. That is why we do not have the death penalty. The problem with deterrence is that you need to have credibility and some assurance that if someone does such a thing there will be this sort of response. The main problem with cyber is that there is a lack of utility in displaying weapons, because those weapons can then be used right back against you. There is no real assured retaliation, which limits the idea of cyber deterrence. We can have cyber resiliency—an assurance that there will be a response to any attack—but it is almost impossible ever to prevent a cyber attack, given those conditions and the way the domain operates, and given what deterrence as an academic term really is.

**Dr Julian Lewis:** Two last brief points, if I may. When you say that there is a belief that deterrence has never worked, I hope you are not

suggesting that that is so in any field, because there is a very strong belief that deterrence in the form of NATO has been effective for half a century. If you throw at us academics who do not believe in deterrence in any sphere, you are frankly wasting your time with this audience. I hope that was not what you were doing.

In dealing with this construct, if a massive attack was taking place to try to bring down a country and it went hand in hand with conventional warfare, as you seem to think it would, surely that notion solves for this category the problem of identifying where the massive attack comes from. If it is part and parcel of a conventional attack, the secrecy surrounding where the cyber attack is coming from will presumably have disappeared, because we will know whose tanks are simultaneously attacking.

***Dr Brandon Valeriano:*** There is a low probability of the military using cyber tools in any war game right now because of the risk of using them. There is no assurance that those cyber tools will work, so there has been less of a utility to want to use cyber as a response to cyber attacks. Conventional deterrents and conventional responses are surely something that should be made very clear: that if you do this, there will be this sort of response. No Government, as far as I am aware, have clearly said, "This is what will happen if there is a massive cyber attack". That is what needs to be done if you want to establish a system of workable deterrents.

***Mr Ollie Whitehouse:*** We have seen evidence of certain nation states launching attacks against particular sectors. One country launched denial-of-service attacks against financial sectors in various countries, or it tried to.

**Baroness Falkner of Margravine:** You are referring to Israel against Saudi Arabia.

***Mr Ollie Whitehouse:*** And Iran targeting stock exchanges. Our greater concern comes when we start to think about our response. We have heard the word "asymmetry" a lot. Our susceptibility versus the potential source of susceptibility to a corresponding cyber attack may be far less, because their own dependence on technology may simply be far less. That has to be a key consideration. Unfortunately, that is why we would likely have to consider other responses such as sanctions, because it simply will not work against the target.

***Dr Richard Horne:*** One final point on attribution and deterrence. If you placed yourself as someone who wanted to do harm to the UK, you might well imagine a scenario where you chip away and gradually increase the level of attacks without conventional attacks being part of it, and you confuse the attribution so that you undermine and weaken before you use other attack mechanisms.

**The Chair:** Lord West and Sir Gerald have questions, but may I say to everybody that we are getting short of time and there is likely to be a

Division in the Lords? Who knows, there may also be another Division in the Commons. I therefore urge colleagues and witnesses to make questions and replies as brief as they can.

**Lord West of Spithead:** My question continues Dr Lewis's point. It seems to me that one problem is that countries do not even know what their own vulnerabilities are and are scared to get into a tit-for-tat with other countries because they have not actually calculated those vulnerabilities. The other factor seems to me to be the intelligence balance. There are lots of countries whose entire computer world we march at will throughout, allegedly of course, and of course there is that massive intelligence balance. The constant argument is therefore that if we reveal that capability we will not know exactly what the president is saying to his oppo, or whatever, so there is quite a difficult calculation to make. Do you agree that those are calculations that make this very tricky?

***Mr Ollie Whitehouse:*** Yes, and your first point about understanding our true vulnerability today is probably one of the biggest concerns.

**Sir Gerald Howarth:** We have had a very interesting presentation from Dr Tara McCormack on how cyber has become a potential military weapon. Leaving aside your various points about the unlikelihood of cyber being a principal weapon, by virtue of the fact that in 2013 the then Secretary of State for Defence, Philip Hammond, announced that we were going to engage in offensive cyber, to what extent do you think this should, as Dr McCormack suggests, be a matter of public debate, bearing in mind that when the Secretary of State made his remarks to the Commons he said that much of this action will not be in the public domain? Indeed, it has been suggested that the necessary secrecy surrounding cyber weapons undermines its credibility. If it is to be a deterrent, if potential enemies out there are to understand that we will retaliate with a cyber attack, it needs to be credible. To be credible, it has to be known about. How do policymakers manage to juggle this, in the opinion of the panel?

***Mr Ollie Whitehouse:*** I find the question of whether it needs to be known about interesting. Can you infer a country's national cyber capability from the health of its industry? If you look at Israel and the private sector cyber capability it is amassing, and on the back of that make the logical leap to the probable nation-state capability, the question is: can you do something similar with the United Kingdom? Without having to disclose your hand entirely, by seeing the buoyant industry that can produce these things in the private sector you can probably jump to seeing the actual adversary that you are up against.

***Dr Brandon Valeriano:*** Credibility is just as much about the willingness to use a weapon, and that has been one of our major problems. The American experience at least is that they are considering using lawyers with every unit because of the immense implications for civilian space. If we start to use cyber tools in the military, the question then is how much we need to train these people on the legal ramifications and the

difficulties in training if the entire operation is secret. They do not know how to train, because there are no qualified teachers to train the units at the unit level, so that becomes a huge problem. Credibility is more about the willingness to use a weapon. Are we really willing to use it at the unit level? I am not so sure that the West is.

***Mr Ollie Whitehouse:*** We also have to worry about proliferation, let us be honest. Typically with the weapon that we are talking about here you could fit many hundreds of thousands, if not millions, on a USB stick, and we have seen the devastating impact that some of the government leaks have had on the North American programmes. That will always be a consideration. As you lower the bar of entry in terms of those in a country's defence force who can use it, what safeguards are there around it that they will not leave when they leave?

***Dr Richard Horne:*** This is an area where, as soon as you publish details of your technique, you have rescinded the value of that technique. So there has to be a degree of secrecy around our offensive cyber capability. Some of the leaks that have been talked about earlier, while potentially very damaging to our security agencies, have reinforced the credibility of what their capability has been and by extension continues to be. So I do not think that the credibility of our capability is an issue.

***Mr Rowland Johnson:*** If you have a kinetic weapon, it can be here or it can be there, but in theory it cannot be in both places at the same time. When it comes to a cyber weapon, in theory it can exist in multiple places. We saw at the beginning of March the Vault 7 disclosure by Wikileaks that a whole load of cyber tools had been collected allegedly by the US. As much as they may have been able to use that arsenal against their adversaries, arguably now that that has been disclosed it could theoretically also be used against them. That is one of the challenges of cyber warfare.

**Sir Gerald Howarth:** Your verdict is that we should be having a debate about the management of this potentially quite significant weapons system.

***Mr Ollie Whitehouse:*** If there is the consideration to make it more widely available, then yes.

***Dr Brandon Valeriano:*** There is no division between military and civilian space, so the use of this weapon is entirely difficult and problematic because of the involvement of civilians and the possibility of war crimes. That is the real issue here, I would say.

Q11 **Lord Mitchell:** We hear a lot about the internet of things. We had a briefing from Melissa Hathaway, who has worked with President Obama, and with President Trump I believe. One thing she said that was quite amazing to me is that by 2020 it is expected that there will be 50 billion devices globally that are attached to the internet. In fact, the people I have spoken to think that is a massive understatement. I just want to get your reaction. Is the prospect of our televisions being a Trojan horse and

being able to spy on us all hype, or do you take this very seriously?

***Mr Ollie Whitehouse:*** It is going to be a thing. We are seeing in our own country smart meters and other benefits. Now that your boiler can report when it starts to degrade in performance so that when an engineer comes out they replace the part proactively, companies will see that kind of upside from the internet of things. We are also seeing the proliferation of connected vehicles before autonomous vehicles, with software updates and all those types of functionality. So we have to accept that our lives and our infrastructure, in our cities and buildings, will be connected to the internet for telemetry purposes at the very least.

***Dr Richard Horne:*** One thing that probably needs to be considered as part of the national security strategy is a consumer protection angle for the internet of things. There is various consumer protection legislation and policy around much of what we bring into our homes. How could that be extended to protect us, as individuals, from all the connected things that will be in our houses? How can we also protect society from the mass effect?

***Dr Brandon Valeriano:*** While there will be a proliferation of internet-connected devices, there is something to be said for complexity breeding a problem and being able to attack. Complexity can make us safer in some ways. The more things that are connected, the less worrisome it is in some ways that some things are disconnected. That is something to consider: that this is inevitable, but that does not mean it is doom.

***Mr Rowland Johnson:*** I would say that the risk is very different. If you look at conventional PCs, laptops and smartphones, if one of those devices gets compromised there is a fair chance that because people are interacting with it daily they might notice when it goes a bit slower or does things that are a little strange. But broadly speaking, people interact with a connected device such as a video recorder or web camera only for a specific function. If those devices run a bit slow, that does not necessarily make them think that they have been compromised.

We see consumers going out to buy these types of device based upon their functionality, not the security that should in theory be built into them. We have a bit of a disconnect in that manufacturers are trying to produce something as quickly and cost-effectively as they can, but users care about functionality, with security as an afterthought. We therefore see the risk being passed from the manufacturer to the consumer. One thing that we as an industry, and potentially government, need to do is to work out how we can manage that risk more effectively. Whether that is through kitemarks or standards, manufacturers of IoT devices need to strive towards that.

***Mr Ollie Whitehouse:*** The challenge is always what we have managed to build in the intervening period before regulation catches up. Today, things are being connected every day, so there will be a legacy that we have to contend with.

**Lord Powell of Bayswater:** I come back to something that we discussed quite a bit earlier: the relationship between government and the private sector. There is a tendency to think that government should be responsible for virtually everything. I am sure that you gentlemen do not believe that. Since you all make your living from advising the private sector, you do not necessarily believe that government should be trampling about too much.

Obviously there are areas where the Government are essential. Critical national infrastructure is one, defence intelligence and so on is another. But surely across the private sector generally, government should encourage companies to take steps to protect themselves and make information available. Is there really a need for much more intervention than that? Do we need legislation and regulation? I suggest that it is probably not necessary. I always remember President Reagan saying that the nine most dangerous words in the English language are: "I'm from the Government. I'm here to help you". I wonder whether we are not getting a bit too hung up on government intervention in this area. What do you think about that?

***Dr Richard Horne:*** I would agree from this perspective. Almost the worst outcome would be if the Government set a whole load of requirements and it became a compliance exercise. That would drive the wrong behaviour in the private sector. It would drive lawyers and compliance activity rather than managing the risk. The Government can be demanding in what they expect of the private sector. I talked in my written evidence about the sort of principles that you could expect the private sector to adopt, which could also go across the public sector. You would expect a degree of responsibility in stepping up to those principles. In some areas that might be embedded in regulation and in some it might be in a code of conduct. There are many policy tools available that I guess are unlikely to require legislation but by which the Government can be clear and demanding about what they expect.

***Mr Ollie Whitehouse:*** I support that. Look at what the Bank of England, and through it the FCA and the PRA, have managed to achieve with the critical economic functions of our country. They do not tell others what to do. They simply say, "We want independent evidence that you can be resilient against a proper attack". Granted, that attack is simulated once in every three or five years, but it gives them the assurance that the institutions are maintaining the appropriate capability. They do not tell them how they should solve it or by what level of investment, but they want independent assurance that they are doing the right thing.

***Dr Brandon Valeriano:*** If you were to insert government into private transactions, government would then become responsible for those transactions. That is where the problem is. We simply need clear lines of oversight and control to say that if this happens, this is who you should consult and go to, especially for critical infrastructure.

***Mr Rowland Johnson:*** We are looking at three different frameworks, some of which are just frameworks and some are regulation. I guess a lot

of organisations are looking at the GDPR because it will come into effect. That is definitely driving behaviour, and I think that all the organisations we work for are seeing that. I suspect that if the GDPR did not exist, some of that focus on disclosure would probably not be happening today.

A scheme like Cyber Essentials is not built into regulation, but we have a great idea there that is aimed at a large part of the population who definitely have significant levels of vulnerability. However, its adoption levels are probably not where anybody in this room would want them to be, so the question is: how do you try to bridge that gap? Many of the organisations that have gone through Cyber Essentials look at it as a tick-box exercise: "I need to do this so that I can report to the supply chain that I've done it, but I don't necessarily care about risk". The ones that have not done it do not really understand the threat. They look at it and say, "Why do I need to do it? I'm never going to be targeted". We need to have more of a debate about whether regulation drives that or whether there is a way of building things into supply chains whereby the Government tell some of the larger corporates through their procurement frameworks, "You need to do this". The insurers might say, "You need to start doing this". We cannot just have a framework that people look at and say, "We will not bother".

**Lord Powell of Bayswater:** But at the end of the day it is surely in a company's self-interest to do this. I sit on a number of boards in the US, and all the companies I am involved with take the cyber threat very seriously. They invest hugely in managing it and so on, but they are not told to do it by the Government or are accountable to the Government for it. They do it in their own self-interest. Is that not the right way?

***Mr Ollie Whitehouse:*** But they work in a very punitive business environment, and we do not necessarily have a cultural mirror there. If we did, I think that organisations would take a long, hard look at themselves today.

**Lord Powell of Bayswater:** If by punitive you mean that people will not do business with them if they show themselves to be incompetent, then fine.

***Mr Ollie Whitehouse:*** Or they would be sued.

**Lord Powell of Bayswater:** That is what business is about.

***Mr Rowland Johnson:*** There is some disconnect. Many large boards around the country still do not fully understand the risk. They think that it is still technology-centric, and often a function of IT departments is to try to mitigate against it when the reality is that it is much wider. If boards do not understand the risk, it is not surprising if mitigation and adherence to these kind of frameworks do not work quite as well as we might have planned.

**Lord Powell of Bayswater:** My experience is that most large company boards insist on a report on cyber matters at each board meeting.

***Dr Richard Horne:*** One challenge is that as our digital world evolves, investing money in building controls for the existing way that we do business will no longer be adequate in many companies. That will drive some really hard decisions and take the level of discussion in those companies to a different level. That is where existing mindsets such as "We can just tell our CIO to build a set of controls and report back to us once a quarter" will not be sufficient.

**Lord Powell of Bayswater:** There is just one other aspect of government and the private sector which I think the Member who has just left was going to ask about. Are the Government right to be bullying the big IT companies into revealing their encryption?

***Dr Richard Horne:*** The rule of law in the digital world drives three criteria that exist in balance. One is that we need those who protect us and enforce the rule of law to have at times some quite terrifying capability available to them. However, the rule of law demands that that is constrained in its use and that the law determines how it is used. It also demands that its potential misuse is constrained.

One challenge in the digital world is that you cannot necessarily constrain the misuse of some of the capabilities that law enforcement might require. Our policemen have guns around here, for which we are very grateful, and the potential for misuse is quite limited because those are physical things. However, if a backdoor were built into every television so that law enforcement could log on to it and look into people's bedrooms, or whatever, the potential for misuse by criminals if that one vulnerability was discovered would be much greater. Those three criteria are in tension; you cannot look at one in isolation.

***Mr Rowland Johnson:*** This is a really interesting question that goes much further than cyber. It is an ethical and moral question, and I have been at conferences where it was posed to the audience: "Which is more important, privacy or protection?" There is not necessarily an either/or answer. I guess the response is, "We want both of them". Sometimes they want more of one than the other, but they both have their place.

**Lord Powell of Bayswater:** That is called having your cake and eating it.

***Mr Rowland Johnson:*** Indeed.

***Dr Brandon Valeriano:*** But that relationship is driven by the last security threat, and in Israel they are much more willing to sacrifice privacy for security. Are we willing to do that? The other issue is that the digital marketplace is very fluid. If you make sure that WhatsApp or Signal cannot use end-to-end encryption, consumers will move to another platform just as they did with the digital music platforms; they moved to other forms of communication.

**Lord Harris of Haringey:** But presumably you would say that if end-to-end encryption was generally weakened, the options available to cyber

criminals and so on would be enormously increased.

***Mr Ollie Whitehouse:*** That is correct.

Q12 **Mrs Theresa Villiers:** We have one obvious example of where a regulator has taken a very assertive, even aggressive, approach to the systems of the sector it regulates: that is, in financial services. There are all sorts of reasons why, given the systemic impact that failures in that sphere might have, the regulator has understandably taken that approach. But there is obviously a broad spectrum across other regulators in the extent to which they feel they need to get involved with this issue. Are there particular gaps? Can you think of a regulator that should perhaps look at this more seriously than they do at the moment?

***Mr Ollie Whitehouse:*** No. We see today that all major regulators understand the challenge but are forming their own views. They are speaking to the Bank of England and gaining its experience. From the conversations that we are having at least, they are not doing it in isolation. I think everyone recognises the threat. The challenge is with certain sectors such as power and energy. National Grid's funding comes through a tariff, so there will be hard decisions to make. If there is more cyber security, it will have to pass that cost on somewhere. It will not be able to come out of general competitive practices, so if I am honest we will run into that kind of friction as opposed to regulators being asleep at the wheel.

***Dr Richard Horne:*** The other challenge is that regulators focus on the companies they regulate and those companies have dependencies on a load of other companies, along with infrastructure and providers. The attackers do not attack just the regulated company; they attack the whole system around that company. So focusing on just the regulated companies will not drive the right result. All businesses really need to understand their role in society, as well as in relation to themselves.

Q13 **Lord Ramsbotham:** Could I move on to the National Cyber Security Centre, since we have covered the earlier question? The National Cyber Security Centre has been announced as the linchpin of the Government's engagement with the private sector. Are the Government being realistic about what can be achieved by what is at present such a small organisation? Does it need to be expanded to take account of all the dialogue that you have mentioned that ought to be taking place?

***Dr Richard Horne:*** I would say that it is a great start. I think it would say the same thing itself. The Government have taken quite an innovative step; they look to allow innovation to drive policy at times and to work in partnership with the private sector and industry and with other public sector organisations in a different way. That step is absolutely the right one. Will it need to evolve over time? Absolutely.

***Mr Ollie Whitehouse:*** I concur. "Too much too early" could always have been a distinct risk where it was given far too much, and we would not see a return on investment. With its initiatives, it has built the

foundations of a critical function in our country, although obviously its budget will need to increase over time.

***Mr Rowland Johnson:*** From my side, it is a big aspiration but a very welcome one. From a personal perspective, we have relationships with the Foreign and Commonwealth Office, the DIT and the Cabinet Office. To have the opportunity to engage with one part of government that will consolidate a lot of ideas will make for much more joined-up thinking. It is definitely warmly received.

**Lord Ramsbotham:** That is encouraging.

Q14 **Lord West of Spithead:** I am quite keen on asking Question 14. When I produced the first national cyber security strategy, one way in which I hoped to make firms do better was by tying in the insurance industry somehow, and possibly using kitemarking, so that there was a cost aspect to it. That does not seem to have happened as much as I hoped. My first question is: is that an important and useful thing to do, and should we do better? Secondly, when I worked on the banks and stock exchanges—this goes back to after the big hit on the New York Stock Exchange—we went for double biometric cards for log-ons. Do you think that when the citizens of this country log on to access all the new services that are about to come up—almost everything you can get, from the Department for Work and Pensions and everything else, will be online—such cards will be a useful thing or not?

***Dr Richard Horne:*** On cyber insurance, the market still needs to mature. We have done a lot of work with insurance companies and the providers to them. I have worked a lot with actuaries in PwC to combine our two views of the world. But the market is still quite immature. The insurance companies are still working out how to set premiums and so on, and what the loss would look like. In the US, you can bound a certain area of risk that you can insure with HIPA and other more regimented responses to cyber breaches. That is an easier loss curve to insure. The challenge is that insurance does not cover the whole loss curve, as the tail events are uninsurable, so it needs to mature.

I have completely forgotten your second point.

**Lord West of Spithead:** The double biometric cards so that the average citizen can log in and go to the DWP—

***Dr Richard Horne:*** There is a huge reliance on passwords in all sorts of services today, and we see so many attacks exploiting weak people and process there. The world needs to move beyond the use of passwords. Whether that is through biometrics, one-time passwords being pinged through the ether to you or however it works out, stronger methods of authentication are absolutely required.

***Mr Rowland Johnson:*** There are huge amounts of synergy with the cyber insurance sector. However, it is disappointing that we have not seen some of the take-up that we might have imagined. You would have assumed that an insurer would care a lot about cyber risk and want to

mitigate against it. They would want to understand organisations' vulnerabilities and have a robust process for measuring all of them before issuing some form of policy. That is not really where the focus appears to be. A lot of the insurers are more interested in what happens after a breach and making sure that if an organisation has been compromised from a cyber security perspective they have the forensic ability to go in and determine what happened—and, indeed, whether they are liable. If there was one take-away, it is that if the insurance sector could work more closely with the cyber industry and encourage more organisations to look at their vulnerabilities as part of their policy renewal or creation process, it would have huge value.

***Mr Ollie Whitehouse:*** On cyber insurance, we are seeing interest not only in the area that Rowland just mentioned but events such as that at the blast furnace in Germany, and whether those could be sourced from cyber events in the future. For those very large policies, a serious look is being taken, but I agree that it is not a mass market at this time. On your point about double biometrics, the thing to remember always is that they are not secret and can be copied. We have done some work on copying fingerprints, voices and faces. Whatever solutions we employ, they should always be agile and changeable in the future.

**Lord West of Spithead:** But it is difficult. That is why the stock exchanges and the banks started doing it.

***Mr Ollie Whitehouse:*** To give you an example of what is possible today, by taking three high-resolution photos of someone's face we managed to get a 3D face mask that would satisfy the current capability in facial biometrics. If it takes only three photos—think of a popstar or someone who has a lot of social media activity—we have to consider this.

***Dr Brandon Valeriano:*** It solves the responsibility problem quite well, because you know where the vulnerability point is, whether that be an insider or an outsider. But, yes, in some ways it causes more problems than it is worth. I know this from working with the US Government and their biometric system. The worst thing that could happen is losing your card. If you have to replace it, it takes a long time.

**Lord West of Spithead:** I was hoping for an unequivocal bid for an identity card.

**The Chair:** I am reminded forcefully of being told many years ago that whatever human ingenuity can devise, human ingenuity can find a way around. Unless someone has something that they passionately want to pick up, I am going to ask Mrs Villiers to ask our final question.

Q15 **Mrs Theresa Villiers:** Is it a realistic goal to get international agreement, a sort of Geneva convention for cyberspace, to set norms for activities by states in cyberspace? What do you think should be in it?

***Dr Brandon Valeriano:*** It is a realistic goal. "Does it matter?" is a whole other question. A lot of countries agree to certain things that they do not necessarily mean to go along with. Having some sort of shared standard

of behaviour, some sort of normative baseline, is something that we need to strive for, but that is very tough, given the difficulties and differences that we have with Russia and China and how they operate in cyberspace and indeed how they view it, which is diametrically opposed to how the West uses cyberspace. So it will be a very tough process, as we have seen from the UN GGE, which has been fraught with complications and a lack of engagement with and involvement of key critical countries.

***Mr Ollie Whitehouse:*** There are certain countries today that have a private sector that in the name of defence has some quite aggressive tactics and earns a lot of money for those countries. It is not intellectual property theft but intelligence collection happening in the private sector, and not at the behest of the Government. Again, what is the commercial incentive for them to sign up to these norms in what is an immature field? What have we learned about warfare over the last 500 or 600 years? At the moment we are dealing with a sector that is barely 30 years old.

***Dr Richard Horne:*** At the risk of sounding like a global politician, I would say that there is no harm in striving to do something, because often the bilateral agreements that you form along the way are valuable in themselves. Although you might not achieve the end goal, you will certainly make a lot of progress through dialogue. We have seen examples, especially the US and China, of where dialogue has made a difference.

***Mr Ollie Whitehouse:*** I have one word of caution. Where we sign up to agreements like Wassenaar, we have to think of the economic implications that that has for the economic growth prospects of the UK. We as a private sector firm trying to do what we are trying to do, which is not offensive by any stretch of the imagination, have somehow been caught up in Wassenaar and are having to seek export licences for certain bits of technology because of their potential dual-use application, for example.

**Mrs Theresa Villiers:** That covers my question.

Q16 **Baroness Falkner of Margravine:** One or two of you have touched on China. Why do you think China is so keen to sign up to some sort of international norms? Is it because it would help China to control its own domestic agenda, or because it is concerned that its capabilities will not be able to keep up with the developments once the US and others start putting real money into this? What is China's motivation to go for it, which is decidedly different from the Russian approach?

***Mr Ollie Whitehouse:*** If I were a betting person I would say they are sensing a change in the international attitude towards their behaviour—people are growing tired of it—and they realise that there may be a ratcheting up, so getting that taken out at the source by agreeing to something is probably a prudent step to take before their behaviour comes back to bite them.

***Dr Brandon Valeriano:*** China is just as vulnerable as we are in cyberspace, as is Russia, so there is an intense idea of an agreement as to how we should behave. The other real issue is that cyber conflict is not, I believe, the most important aspect, despite that being the basis of my academic work. I think cyber repression is more important. What I am really worried about is what states are going to do to individuals. China would be perfectly willing to sacrifice international conflict for the ability to repress its population, and that is what we should really be worried about.

**Baroness Falkner of Margravine:** And you think that is the motivation for China?

***Dr Brandon Valeriano:*** I think it would be a trade-off. China would get some sort of agreement that would allow it to behave how it wanted to internally and restrict external behaviour, which it has been quite happy to do till now.

***Dr Richard Horne:*** I would add that the ability to verify adherence to international agreements is very different in this space and very difficult. In the nuclear world, you can see nuclear tests.

***Dr Brandon Valeriano:*** That is why we need legal standards. We need more than the Tallinn Manual, because we do not have a buy-in from the East on that manual, and we need that if we are going to have some sort of legal expectations. Such legal expectations have been shown internationally to work in constraining behaviour, but that would work only if the other countries agreed to them.

***Mr Ollie Whitehouse:*** Just in closing, we also have to think about spaces like space and international sea, which have connected devices in them today, and what applies there.

**The Chair:** I must admit that the way we think about verification had crossed my mind. Thank you for your patience. I am sorry about the interruption. At least we were not disrupted by a Lords Division as well. Divisions are always a problem when we have hearings. As I say, thank you very much. I think we have all found this very helpful and illuminating.

**Lord Harris of Haringey:** Chair, I neglected to declare my interests earlier, and I may not have been the only one. I am a non-executive director of the Cyber Security Challenge; I chair National Trading Standards, which supports the National Trading Standards eCrime Team; and I am the UK co-ordinator for the Electric Infrastructure Security Council.

**Lord Powell of Bayswater:** I am sorry. I should have done the same. I have connections with three companies that are active in the cyber field in one way or another and with two institutions that are engaged in research on it, as declared in my Lords declaration of interests.