HOUSE OF COMMONS

Defence Committee

Oral evidence: UK Response to Hybrid Threats, HC 1816

Tuesday 30 April 2019

Ordered by the House of Commons to be published on 30 April 2019.

Watch the meeting (Audio only)

Members present: Dr Julian Lewis (Chair); Leo Docherty; Martin Docherty-Hughes; Mr Mark Francois; Mrs Madeleine Moon; Gavin Robinson; Ruth Smeeth; John Spellar; Phil Wilson.

Questions 58-122

Witnesses

I: Dr Rob Dover, University of Leicester, Dr Anna Hillingdon, University of Bournemouth, and Elisabeth Braw, Royal United Services Institute.

Written evidence from witnesses:

Dr Rob Dover

Dr Anna Hillingdon

Examination of witnesses

Witnesses: Dr Rob Dover, Dr Anna Hillingdon and Elisabeth Braw.

Q58 **Chair:** Good morning and welcome to this second oral evidence session of the Defence Committee looking into the United Kingdom's response to hybrid threats. We have three expert witnesses today, and I would like to invite each of you briefly to introduce yourselves.

Dr Dover: Good morning. Thank you for inviting me. My name is Dr Rob Dover. I am an associate professor of intelligence and international security at the University of Leicester.

Dr Hillingdon: Good morning. Anna Hillingdon. I am from Bournemouth University's department of accounting, finance and economics.

Chair: Thank you very much. Could you just speak up a little more?

Elisabeth Braw: Good morning. My name is Elisabeth Braw. I lead the modern deterrence project at RUSI.

Chair: Thanks very much indeed. Ruth Smeeth will begin.

Q59 **Ruth Smeeth:** An easy question to start with: what hybrid threats should the UK be worried about?

Elisabeth Braw: I think it should be concerned about the combination. Hybrid is obviously the combination of several threats, and that is what the UK should be concerned about. We are good at talking about, for example, cyber-attacks, and we have a fantastic cyber agency that is pioneering in Europe and beyond, but the combination of threats is what we should be concerned about, and also how they target not just the Government and the private sector but the wider population. Our response to that should be a combined effort as well. That is where we are not quite in the position we need to be, and that is what we should be concerned about.

Q60 **Ruth Smeeth:** Are there specific hybrid threats that the UK should be worried about?

Elisabeth Braw: If I can highlight one example, I think it is the creeping nature of non-conventional threats. If we think about malign influence, we as citizens all think we can spot disinformation. I am looking here at a recent report from the Reuters Institute at the University of Oxford. It is a worldwide survey of people who were asked whether they had come across fake news stories. It starts with Turkey, where 49% think they have encountered fake news stories, and it goes all the way down to Germany at 9%. The UK is a bit higher at 15%. That shows that 15% think they have seen fake news stories, but we don't really know. Nobody

knows because they haven't been told how to identify fake news and disinformation.

In another recent survey in America, 75% of Americans were fooled by headlines, so they can't really tell what's true and what's not. In another recent survey in Sweden, of teenagers, which I think is a key constituency for the health of our democracy, 79% said that they were good at determining whether something was fake news or not. Then they were tested, and 88% couldn't tell a fake news story from a real one, or the other way around. That is the creeping nature of disinformation and it is really something we should be hugely concerned about. It doesn't really matter whether something is fake or not; what matters is that people think it's fake. That really damages their trust in our institutions.

The same goes for cyber-attacks. Most people now, among the general public, know that cyber-attacks happen, but they think the Government or somebody wearing a uniform will defend them at all times. So we become complacent as a society; we think that somebody else will fix it. I don't think that we, as citizens, do our part, and we are not asked to do our part, in assessing the situation in which we live. There is so much more that can be done, and I think the Government has an opportunity here to engage with the wider public.

Dr Hillingdon: I think the key to UK national security is its economy and, on that front, there are a number of threats that the UK could face. By putting the economy as the priority, we can think about the UK's critical infrastructure. Asymmetry of knowledge transfer is the second one, and priority capability and societal mind. I can explain each one, or perhaps later as we go through.

Q61 **Ruth Smeeth:** Are any of those specific challenges for the United Kingdom, as opposed to any of our allies or elsewhere?

Dr Hillingdon: It depends on which one of the four we are looking at. If you are looking at the UK critical infrastructure, you can think about terrorism, cyber-activity, national disaster, public health and overseas problems. Depending on how they take place, all of them could be a serious threat. You saw a few weeks ago that someone went to the top of the roof of St Pancras station. You can see the scale of the impact of something as small as that. Now imagine something sophisticated attacking one of those critical infrastructures. There are three other things that I mentioned; when I have time, I will be happy to expand on them.

Dr Dover: From my point of view, the critical hybrid threats are those that distract us from doing the more important things—to focus on the mobilisation of conventional forces and to spot where adversaries are moving against us. In the case of information and disinformation warfare, we are concentrating on the minutiae of the message rather than the moves that sit behind. It is a distraction.

We have alluded to information warfare, even in the opening remarks—all three of us, really. That is the unseating of certainty of knowledge. That is

the realisation that the changes in the way that people receive and filter information are resulting in uncertainty in public institutions and in what people understand as plain and simple facts, as you and I would understand plain and simple facts. Finally, there is the potential for attacks on critical infrastructure, including banking, transportation—anything that is networked. That feeds into the current debate about 5G and who will build that infrastructure, dare I say?

Ruth Smeeth: You may have just opened a can of worms for us all.

Q62 **Mrs Moon:** I am very interested in the issue of desensitisation and whether the public and politicians are becoming immune to attacks. We do not notice them anymore, or we say, "It's all fake news." What are the underlying risks to democratic values and the belief in democracy as a way of life that are part of the strategic nature of the attacks? Should we do more to alert the public that they are now on the frontline? It is not the soldiers, the sailors or the airmen who are coming to their defence—it has to be themselves. How do we develop the critical skills to tell the difference? Emotion seems to have trumped knowledge, and that is a very dangerous situation to be in.

Dr Dover: I re-read my written submission—that may be a dangerous thing to do—and one line I quite liked was about activities that were plausibly deniable and implausibly deniable. One might look to last March and talk about things that occurred in a cathedral town; there were things that looked and moved like a duck but were not called a duck by foreign adversaries because it suited them to cause that ambiguity.

In terms of mapping that to an improvability, the credulousness with which the public, up to and including academics, receive some information is very worrying. You move into a space where you are talking about the responsibility of news media in terms of fact checking and where people are getting information from. There have been alternative and other hearings where social media firms have come in and talked about the steps that they are taking to try to avoid having obviously malicious or false information on their platforms. It has the feel that it requires a total effort from the ground up. In primary schools, some effort is now going into asking, "How do you know when you read something where it has come from? How do you validate?" That will take some time to feed through, but we are feeling the strategic effects of that, that people are easily swayed by essentially quite well-written misinformation. So it does go to the heart of our democracy.

Elisabeth Braw: I was reminded of the US embassy siege in Tehran 40 years ago. The US diplomats did not think anything was amiss when the students started protesting outside, because there had been protests every single week for a long time. Then, all of a sudden, there was a real attack. It was too late, because they were not prepared and had been desensitised. We are in a similar situation where this drum beat of disinformation and cyber-attacks and other aggression that is part of hybrid warfare goes on all the time. We become so used to it. We think, "Nothing will happen; this is the new way of life." Again, we could do so

much more if we empowered the population to feel responsible for their part.

I will highlight something that Latvia has done. In 2018, the Parliament decided that something called the defence curriculum would become mandatory in all state secondary schools—in effect, all secondary schools. Right now, it is under way in 13 schools and an additional 50 schools will introduce it this year. That is a very sensible step. How do we involve the public and get them to feel they are part of the national security? We teach it in schools, not as a frightening subject but as an empowering subject that you or I or anybody else can do something about, and play our part in national security and keep our country safe.

Q63 **Mrs Moon:** Would Ukraine be a more recent example rather than the American embassy attack?

Elisabeth Braw: Yes, it would. That just occurred to me because it is a nice symmetric anniversary of four decades ago.

Dr Hillingdon: Two things. While I agree with what my colleague is saying, we are going to have to be careful. Not everything is a threat. Not every narrative is a threat that is coming. We should not overreact. But when there is a threat, you might not find the concrete evidence for it.

To address your question on what we should be doing, to get the grassroots moving in schools is really key, but you can take that education to people's sitting rooms, kitchens, car, radio or TV, or on to social media. When they are on holiday or are sitting in restaurants, many people are watching all the time. There needs to be an integrated approach to take education not only to primary school, but everywhere.

Mrs Moon: Perhaps we should have "Have I Got Fake News for You?"

Chair: Very good. Gavin, please.

Q64 **Gavin Robinson:** Good morning. Dr Dover, your evidence talked about cyber-warfare not being a new phenomenon—that if we looked back over the centuries, elements featured throughout the passage of time. You also indicate that we weren't looking for aspects of hybrid warfare and therefore have not documented that sufficiently. Are we under hybrid attack continuously? Is there a sense in which we can understand the preparedness of our Government in the event of hybrid attacks if we are not documenting what has gone previously? Are we to conclude from that that we are not prepared at all?

Dr Dover: I will come back to the last bit. There were elements of hybrid warfare within all the main set-piece historical wars. Part of the reason hybrid warfare receives attention now is in part a success of the nuclear deterrent: the sense that we have warded off an existential threat through having overwhelming kinetic ability to deter people from attacking us directly. In that sense, our adversaries are having to find different ways of attacking us, because they do not have that direct route, as they would have done before.

In terms of preparedness, are we under constant attack? I think you can see this in certain types of activity—espionage, cyber, attacks on infrastructure and large companies—but also in terms of that mis- and disinformation campaign that is not focused on the particular issue. It seems just to be focused on attempting to unseat certainty of knowledge or understanding among the populace.

So, yes, I do think we are under some kind of continuous attack. Whether it is useful or helpful to describe that as being in a state of some sort of proxy war, there is a much bigger debate around that. There is a huge academic debate around securitisation—that is, it is very useful if I am a Secretary of State and wish to lever more resource; obviously, securitisation assists me in doing that. Equally, it can have a negative narrative effect on the public, as your colleague said. People become too used to it. This permanent state of war does not do anything about elevating people's status and response.

Have we reached the point of those continual attacks where there is a utility in raising the bar—of heightening anxiety, if you like, so that people think about taking mitigating responses and what those could be?

Q65 **Gavin Robinson:** Okay, so in terms of preparedness, have you turned your mind to assessing the response our Government has had in the past? Do you think we respond well when faced with hybrid assault?

Dr Dover: I will give the headline and then it might be unpicked by precise examples. To some degree, the UK is challenged and under tension between what might be an effective response and the response that is legal, and demonstrably legal, and fits within the value set that the UK understands itself to have.

While adverse reactors are not bound by the same sets of niceties in the international norms, we are unable to respond in kind because the UK does not do that sort of thing, or it would be soiling of our reputation to do so. The UK does respond, and has considerable capabilities to respond, to all sorts of hybrid threats, save for the speed of ramping up a kinetic response that Finland has, for example.

But certainly, in anything to do with cyber-space, we have considerable, if not second or third best in the world, capabilities to respond to those threats, but I wonder whether we hold back either because of legal prohibition or normative prohibition.

Gavin Robinson: Okay, thank you. My questions arose out of—

John Spellar: Could I just pursue that particular one or are you carrying on?

Gavin Robinson: I was going to ask the others for reflections on what we have discussed, but certainly.

Q66 **John Spellar:** To come back to Dr Dover, we have seen in previous evidence reference to legal constraints. What are those legal constraints?

Dr Dover: Against adversaries? The various intelligence Acts provide for Secretary of State authority to act in ways that would otherwise be illegal abroad. From that point of view, there is relatively little constraining effect. Following that logically on, the constraints would be normative—that is, being caught doing whatever it was that we were doing.

Q67 **John Spellar:** I understand the reputational argument, although I think it is questionable. Even so, I understand it. In terms of legality, I'm not sure I do understand it.

Dr Dover: No, and I might have to come back to you on that because I have nicely shepherded myself down a cul de sac.

Q68 **Chair:** Before we move on to anything else, I would like to nail down one point. From your written evidence, you seem to make it quite clear that you don't believe that, as a matter of policy, Britain should fight fire with fire, where the question of fake news is concerned. You believe that we should counter it but that we should not emulate it. I will quote back at you for the benefit of the record what you said about the states that engage in this: "Whilst those states offer protestations of openness, transparency and freedom in their medias, very few accept them at face value. For the UK to engage in an exact reciprocation would contain strong risks, precisely because there is an expectation that UK claims to openness and transparency should be able to be taken at face value." On the other hand, we know that in wartime situations we have engaged in deception to a very complex and great degree, but you are saying that in times that fall short of national emergency you would not want to descend to the same level as those who are attacking us with fake news.

Dr Dover: To be honest with you, personally I am less certain than the written evidence, so from that point of view I think it is about choices and consequences. Where I think that the negative consequence outweighs the utility is potentially in the case of North Korea. There is really strong utility in the BBC World Service reaching people in North Korea and them having faith and trust in that Korean language service as a true representation of world events. If a North Korean regime—they will say this anyway—or other voices into that space successfully manage to say that the BBC World Service is, for example, a mouthpiece of the UK Government and engaging in its own acts of disinformation, that has a negative utility.

So, personally, I am agnostic about fighting fire with fire. I think it is very much a choice for the UK: we could go in gloves off and engage in that activity, but I think—this is my naivety—that the UK acts as a beacon of that sort of transparency. To some degree, the vulnerabilities that we have allowed—well, exposed ourselves to—come from that openness.

Q69 **Chair:** I know that John wants to pursue this a little further before we come back to you, Gavin, if that's okay, but may we hear from Anna and Elisabeth? How do you feel about this business of us adopting higher standards than those countries that seek to undermine us?

Elisabeth Braw: I would say that it should be a matter of pragmatism, rather than just ethics. I would say it is a good thing to be a country that

pursues and promotes facts rather than disinformation. Also, if we respond to most or even just a few disinformation campaigns with disinformation campaigns in return, it is a race to the bottom and the UK will lose its standing as a credible diplomatic power.

Another way of doing it is to respond in an asymmetric fashion by, for example, revealing facts about the adversary that the adversary would not want to be known—such as Russian money or individuals owning property and bank accounts in the UK. That is something that we could reveal in response to a disinformation campaign against this country.

Dr Hillingdon: I think it is a matter of pay-off. The UK can have a certain number of strategies for how to deal with these things, but at times you have all your strategies in place and the adversary does something that makes you realise suddenly, "I've got to respond and this response has to be my best response," so effectively my strategy turns into action, and that action needs to be the best response. On that note, it is case by case. At times, if they are going hard, the UK needs to go hard because if it does not, it might be a sign of weakness.

Q70 **Chair:** In which ways do you think it should go hard?

Dr Hillingdon: Maybe I bring this in too early, but the bigger question is increased defence spending. The UK's adversaries have increased defence spending, so what should the UK do? Should the UK embrace it, saying, "They are spending—we will stay here," or should we respond to it by spending more, at least to keep that balance or equilibrium going? The latter is the case for me.

Q71 **Chair:** That is clearer when talking about more conventional hard power, but what is more tricky in the context of this inquiry is how we respond when we are being attacked with disinformation, for example, or attempts to infiltrate our 5G network, heaven forfend.

Dr Hillingdon: The UK is quite capable. You have the BBC operating in 40 different languages across the world. You do not necessarily have to go very aggressive, because you have the BBC and it has a big audience across the world. You can use the BBC in your favour, but that is not the only thing. The UK has privilege, effectively, over every country that is not an English-speaking country. Your language is the top language of the world. You can use the language in your favour. Basically, you already have a head start in that game.

Q72 **Chair:** Is it your collective view that, when attacked with disinformation by adversaries, you should reply by exposing and countering that information, but not with disinformation of your own? Is that your argument?

Elisabeth Braw: Yes.

Dr Hillingdon: I am saying it depends and it is case by case. One shirt does not fit all the responses. They need to be looked into case by case. Who is it? What is the disinformation? What is the outcome of that action for the UK? There should be the sense of a strategy, but also a sense of

action at times when we might not follow the strategy, because it demands that I take an action and maybe this time the action would be, "I go harder than they are coming to me."

Q73 **Chair:** Rob, you have had a chance to consider a bit more.

Dr Dover: It is preferable to be able to refute the disinformation with exposé. I want to pick up on something Elisabeth said about deterrence, because it fits within a strategic studies frame. I don't think we have pulled the levers of deterrence very hard. We are not dissuading our adversaries from attacking us, because we are not pulling the available levers.

Chair: Such as?

Dr Dover: Elisabeth used the example of inward investment in property in this great city. We have not pulled that lever at all—or very infrequently.

Q74 **John Spellar:** A lot of the discussion is framed in terms of response—in other words, there is a hostile action, how do we respond to it? If, however, someone is a serial offender in this regard, should we not also be looking at offence as well, not least because all the societies of the countries from which we most suffer have huge internal problems? Therefore, we could either broadcast the facts overtly through the main media, the World Service, or utilise social media not to spread rumours, but to disseminate information. For example, how many industrial disputes are there every day in China? They are desperate to keep a lid on that, let alone all the disputes about planning and so on. Within Russia, you have mentioned the corruption of the oligarchy and the diversion of funds.

There does not seem to be within the British system any system that would relate, for example, to what we did in the second world war: actively thinking about the weaknesses in the other system and exploiting those. Should there be one? Isn't that where we should be looking, rather than purely a defensive strategy, either to shut something down or to respond?

Elisabeth Braw: I will start, having been a journalist for many years in a previous life. The challenge we have as liberal democracies is that the Government are very limited and cannot tell many parts of society what to do. That includes journalists, including journalists at the BBC. Even if the Government thought it would be a good strategy to have the BBC uncover various unsatisfactory conditions in countries that compete with and even attack us, there would be reluctance among the journalist corps to take instructions from the Government.

Of course, the great thing about the free press is that journalists often go and find these conditions on their own. For example, we have seen increasing reporting of the re-education camps for Chinese Muslims. That is not something the UK Government told journalists to do; they just found it on their own, and it has really gained public attention thanks to that muck-raking effort by an increasing number of journalists.

Q75 **John Spellar:** Can I just interrupt? When were you a journalist?

Elisabeth Braw: Until 2014.

Q76 **John Spellar:** Is not one of the problems that, as news agencies and newspapers have been hollowed out in their capacity, their ability to undertake—or even their interest in undertaking or willingness to undertake—investigations has declined enormously? Basically, you certainly have to pre-package information and hand a wodge of it to them, as well as the analysis that you have done yourself, for them to actually start to run with the story. Politicians find that with journalists almost every day, and I suspect that is true in most spheres.

Elisabeth Braw: It is an enormous challenge. On top of that, we have the challenge that newsrooms are understaffed and the journalists who write are often not specialists. We will find general reporters with very little understanding covering issues of national defence and security. I wish there were such a thing as a national defence course for journalists, run by NGOs or the Home Office, not for them to become influenced by the Government in any way, but for them to learn how national security works. It is not immediately obvious to most people, including journalists, what the various parts are, what to pay attention to and, by the way, what a tank looks like.

Dr Hillingdon: May I add one point? I agree with your point, or at least how I received it at this end. I am not a great fan of football, but what I understand about the game is that if you only play in defence, at best you don't concede a goal. You won't score a goal and most of the time, even if you fully defend, you will concede a goal. My point is that if the UK is only going to react, rather than being proactive, it is bound to concede a goal.

Q77 **John Spellar:** Certainly, the post-war Labour Government of Attlee and Bevin recognised that when they set up the IRD in the Foreign Office. In the 1950s, the 1960s and in the cold war they also worked closely with our allies in fighting the information war across the spectrum: in cultural organisations, in journalism, in the media and even in abstract art. What are we doing or should we be doing with our allies in this regard?

Dr Dover: Where do you start? With the IRD it was simpler, because there was a unified—or roughly unified—opposing ideology that filtered through into a way of doing international politics. From that point of view, it was a simpler operation. Now it is rather diffuse. It would be tricky to try and run an IRD-style operation against those who have an implementation of capitalism that is highly autocratic, with strong national controls.

Going back to your first question around why we look at it defensively, I was scribbling notes furiously. I think it is partly a disposition. You won't find anything in the literature about defensive operations. I remember as a younger man, with slightly more hair and probably more energy, writing a grant around state deconstruction, because the academic literature always just talks about state reconstruction and there is nothing on deconstruction. We will tell you how to rebuild a state but we won't tell you how to effectively unpick one, so you don't have to do the other bit.

Similarly, with European integration I wrote a paper around European disintegration, because I thought that might be funny; I actually could have made my name with that.

I have some scepticism about the appetite of HMG to engage in that activity. Even within the defence realm, when I think of HMG disposition towards countries who have problematic policies towards homosexuals or countries in the Middle East who we like to sell arms to, and standing up to those nations, I find it difficult to think that we would effectively stand up to large and hostile countries in that regard. That is more of a political point—a small "p" political point—than an answer to your question. It just doesn't fit within the established mode of writing to write about how you would do it.

Q78 **John Spellar:** Is that a lack of mechanism or a lack of doctrine and a lack of will?

Dr Dover: Doctrine, not will necessarily. I think there is a lot of conditioning and there are incentive structures, be they soft or real, around that. It would be quite interesting to call for papers and say, "Write us something on that," to see who responded.

Q79 **Chair:** Before we leave the question of alliances, Huawei obviously is a topical subject. You are not here in your capacity as technical experts about telecommunications, but on John's point about the need to work with allies, how do you see the impact in hybrid warfare terms—terms below any level of open conflict but which are nevertheless adversarial—of a breach over this question of allowing Huawei into the building of our 5G system, given that three of our four Five Eyes allies have so far declared themselves against it? If I may use your metaphor, Anna, what is the potential for an own goal?

Dr Dover: There are some contradictory things to say about the potential for 5G and the threat that comes from it. If you read the technological literature and see what 5G is intended to deliver, which is essentially almost every device interconnected, be it transport links, communication and things in your house—your toaster and all the rest of it—and you have a vulnerability within the very infrastructure, that is a really large vulnerability for the UK. The contradictory thing to say is that we already have highly vulnerable infrastructure within our broadband internet 3G and 4G capability as it stands, so why draw the line now when we have not done so before?

Q80 **Chair:** Surely you have given the answer: the next generation is going to be so much more influential on our lives than the previous ones.

Dr Dover: Absolutely. I think there are two sets of questions. One is technical. In terms of the technical capability, even confining the vulnerability to aerials—the whole technology works on the premise of aerials, so that is not a peripheral concern; it is core to the technology. Then there is a political concern, which people paid better than I am will answer, around whether we want to alienate China as a major trade partner in the future.

Q81 **Chair:** Yes, but my question was: do we want to alienate the US, the Australians and our other—

Dr Dover: The answer to that is that we are a very large player within the Five Eyes community, from what we can glean from open-source information, and we leverage an enormous amount of influence as a result of our major role within that compact. To endanger that is foolish in the extreme.

Q82 **Chair:** Would you agree with that, Elisabeth?

Elisabeth Braw: I was going to make a slightly different point: I think it is an unfortunate failure of American diplomacy. The Americans could have made a better case that would have made it easier for the UK to join its Five Eyes allies in not using Huawei. As I see it, the US has essentially focused on just the one aspect of Huawei being a potential national security liability, instead of putting it in a hybrid warfare perspective and saying, "China engages in all these activities. We have to look not just at Huawei's technical aspects in isolation; we have to consider the range of activities the Chinese Government engages in, through its companies, the Communist party and the Government itself." That would have made it easier for the UK Government to look at those concerns not just as a technical or commercial issue about the 5G network structure but as a national security issue.

Dr Hillingdon: Acknowledging, on the side, that I know very little—almost nothing—to answer your question in terms of co-operation with the USA and Australia, co-operation is prone to defection, but if there is a happy alignment among partners, that should go ahead and work because both partners have the same interest on that matter. I would be in favour of working with the USA and Australia.

Chair: Thank you.

Q83 **Mrs Moon:** Does this really boil down to a lack of understanding and conversation about the value of data, and in particular personal data, in national defence? Do you think that if we focused on how data can be used as a tool of attack, we would be having a totally different conversation about Huawei and their role in accessing huge amounts of personal data—in relation not only to Government or agencies that work for Government, but to the ordinary citizen?

Elisabeth Braw: I can start on that. We are living in what I see as a convenience trap. We get new technologies. When they arrive or are being developed, people say, "Oh, I'd like to have that," but very quickly that changes or morphs into, "I need that," and that's where we are now. Of course if we, as ordinary members of the public, hear that we can download a full-length film in 4 seconds as opposed to a number of minutes, we will say, "Yes, I want a future where I can download a film in 4 seconds," but if we are not brought into the conversation on exactly what you mentioned about our data, we don't reflect on that. I shouldn't say "we"; most of us don't reflect on it. That comes back to the need for

education of the wider public, starting with teenagers, who are a captive audience and also very receptive to information.

Dr Dover: I think it's precisely the conversation we should be having. If you think about it, even someone like me, a humble academic, with a few internet tools, can scrape an enormous quantity of social media data to analyse for academic papers. If I had the power and capability of the Chinese state—well, the mind boggles, doesn't it? I wonder what our ability is to scrape the same amount of data, or interesting information about Chinese citizenry, in China. I don't think the same ability—

Mrs Moon: Exists?

Dr Dover: No. Therefore, in terms of strategic context, we make ourselves quite vulnerable, because they understand us and they understand the centre of gravity in the UK. To put it purely in military terms, they will be able to understand our centre of gravity far more accurately than we understand theirs. The one thing that did strike me about the whole Huawei debate was, why is there no—well, one of the double bonuses of having increased defence spending is that maybe we would have a UK supplier of this technology. In not having that investment in the UK, we are almost entirely dependent on this contractor that everyone has, or a large number of people have, some sort of sensitivity around. But there is no alternative, or there doesn't seem to be a plausible alternative, and that exists in the US as well. It strikes me as slightly odd.

Dr Hillingdon: If you recall, at the beginning I raised four points when you asked what we should be worried about. My second point was about asymmetry of knowledge exchange. Building on Rob's point—I am not pointing at anything to do with 5G; I am pointing at what Rob just said and building on that—I think there is a danger in terms of asymmetry of knowledge. We just mentioned China. I think there is a danger. Knowledge is power, and I think there is a danger that in the United Kingdom and for a while, we may have sent out more knowledge than we got in—there is more flowing out than incoming. Yes, some students might come in and bring investment, bring money, but what sort of price are we putting on this elite science, technology and engineering in the very elite universities in the UK? I think they are under-priced. They are marketised and maybe they are just being sold. That is very, very dangerous, because they get content from the UK, but what is the UK getting from them? How many PhD students are in China right now doing engineering in a top Chinese university?

Q84 **Martin Docherty-Hughes:** Good afternoon. Is there enough understanding across Government and in society in general of the significance of hybrid threats and how they differ from conventional ones, and what should Government do to enhance people's understanding of hybrid threats and our ability to resist them?

Elisabeth Braw: I was just looking at the latest Pew global polls on what people around the world are most concerned about. The UK was along the same lines as every other western country: the top concern is climate

change, then ISIS and then cyber-attacks. That illustrates maybe an insufficient understanding of the aggression we are exposed to. This is the irony of our Armed Forces and our Government being very good; they take care of so much of it that we, the general public, do not really notice it. In fact, we assume that they can defend us against every potential danger—excluding perhaps climate change.

If you walk down Whitehall and ask anybody if they feel that they are under attack or the country is under attack, they will say, "What are you talking about? I feel perfectly safe here." That is the challenge we face. How do we educate the public in such a fashion that it empowers them, rather than making them panic? The Swedish brochure, "If Crisis or War Comes", was a good example of how one can do it. It might have to look a bit different in this country, but it put in very simple terms—in bullet point format—what you should be looking for, when you should be concerned and how to prepare. That is something everybody can do.

Dr Dover: From the Government's perspective, fusion doctrine is an interesting start.

Martin Docherty-Hughes: We will get on to that later.

Dr Dover: But it could itself be seen as a form of hybrid war, depending on how one defines it. To some degree, the labels are unhelpful—I say that having submitted written evidence where I provide a definition; well done me—and moving away from very contested labels to what activities are occurring is somewhat more useful. From that perspective, in terms of educating the public and the public's understanding their role and engagement within this, be it from a very minor adaptation of behaviour up to something starker, focusing on the activities rather than a contested label will be demonstrably more useful.

In terms of people's disposition, if we just stick and pick on cyber, people's disposition toward personal data security and privacy settings—even students I have taught in the past—is so woeful that it is not even a starter for 10. There is a really large piece of work to be done to try to improve and tighten up security in the country.

Martin Docherty-Hughes: Anna, do you want to come in on this one?

Dr Hillingdon: The UK Government has done well, but there is never any such thing as enough, in my opinion. Some of these things might need some form of new legislation or new laws to enable the British Government to take some of the actions. I am not a law person, but I have seen there are times when you say to somebody, "Why don't we do this? Why doesn't the British Government do that?" and they say, "The law doesn't allow that." You just think, "But it's rational to take this action and we can't, because your law doesn't allow you to take that action." There needs to be a look into some of these things to re-think through of some of these actions, laws, legislation and so on.

John Spellar: But—

Q85 **Martin Docherty-Hughes:** Chair, may I finish the question? Not only am I interested, but I pushed heavily for this inquiry to take place, because it poses a serious threat on a range of not just military, but economic, social and liberal democratic fronts. Anna, you mentioned new legislation, so let's talk about bad business practice as an element of hybrid warfare. It would be remiss of me as a Scottish constituency MP not to mention Scottish limited partnerships, which basically allow some of our adversaries to utilise those partnerships to flush out dark money, which then goes back to them to enable them to fund their own hybrid warfare approaches, whether through TV channels, media or social media. Would you agree, for instance, that we need to get our own house in order by getting rid of Scottish limited partnerships, or changing them so much that they cannot be utilised?

You did not mention the word "resilience", Elisabeth, but you were heading there. In Scotland, we have something called the Resilience Division. It has been primarily utilised because of the environment and for weather over, say, the past 15 years. Could something like a resilience division across the different Administrations of the UK be utilised to better inform? That template already exists in Scotland. So, first of all, let's get our own house in order in getting rid of things like the Scottish limited partnerships dealing with the dirty money in London, and utilising existing practices.

Dr Dover: On the first point, again I think it is a choice. If we are happy to take the consequences of the absence, or reduction, of inward investment—

Martin Docherty-Hughes: Of bad inward investment.

Dr Dover: Absolutely, it is bad inward investment. There is a line of argument that bad inward investment is in part underpinning some dynamics, particularly within the property market. There would, therefore, be a consequence to unpicking some of that bad inward investment. You could say that it is actually very effective hybrid—grey—warfare to make your adversary entirely dependent upon your money.

I don't dissent from the notion that it would be preferable to get our house in order. I have read *Private Eye* like everyone else, to understand the implications of those LLPs. This does have consequences, particularly when it comes to property. People would just have to be accepting of those consequences. And the second point has completely gone—sorry.

Elisabeth Braw: I can take the second point, on resilience divisions. I am not sure what you have in mind but, as I understand it, it would be a Government entity in charge of any contingencies short of what we define as traditional war. Is that right?

Q86 **Martin Docherty-Hughes:** The Scottish example is that you have the third sector, private business, central Government, local authorities, the health service and community healthcare partnerships fully engaged across every local authority in Scotland on our resilience planning, facilitated by the Government in Holyrood.

Elisabeth Braw: That is a very good model. It allows exactly what I think is needed, which is the participation of the private sector and the wider public in national security, short of traditional war. It fulfils a need and creates a level of engagement that signals to our adversaries that we have a united front against you, regardless of the method with which you might like to attack us.

If I might highlight, the Scandinavian countries have a somewhat similar system in that they have home guards who focus on contingencies short of war—in fact war as well, but mostly contingencies, including traffic accidents, guarding crime scenes, piling sandbags and so forth. These are volunteer organisations and there is huge potential for that sort of engagement.

I will cite another survey here from a Scandinavian country. Nine out of 10 people want to participate and be helpful in case of a crisis, but six out of 10 do not know which organisation—how to find an organisation where they could participate in the relief effort. Assuming that Brits are similarly Samaritan minded, I think there is huge potential for something like you mentioned.

Q87 **John Spellar:** When people say to you, "The law doesn't allow us," do you press them on which piece of legislation and which clause does not allow it? Very often there is urban mythology within Whitehall.

Dr Hillingdon: One thing that comes to my mind and into my gift, as I raised the point, is the fact that—in my opinion, and I might be completely wrong—we should look at the issue of inclusivity in this country. To me, an excessive amount of weight has been given to this inclusivity, to the point that it has almost opened up a void into foreign infiltration—to a very powerful narrative and rhetoric that are considered legitimate. But what they do is try to push and get the policy maker, the politician, to change their decision, but, by doing that, they are trying to change the UK identity. I therefore question why we cannot stop them when they say this. They say, "That is considered legitimate, but what you say is considered politically incorrect."

John Spellar: That may be true, but it is not the law. Anyway, I will leave Madeleine to pursue that.

Q88 **Chair:** That goes back to your point about asymmetry, doesn't it, in the sense that we seem to be more willing to make concessions to accommodate other nationalities and other countries than we seem capable of gaining information about them?

Dr Hillingdon: I think the UK should—maybe this is a big word, but I mean it in the biggest sense—aim to conquer rather than to service. We should not be servicing other countries. If we have something really good, Britain should put a high price on it. I agree with your point: yes, the UK has been giving more than taking.

Chair: Yes, okay. Madeleine, you wanted to come in briefly.

Q89 **Mrs Moon:** I was thinking about Wedgetail when that statement was made that we give more than we take.

Chair: Yes—that's a defence procurement issue.

Mrs Moon: Before I come to my question, you are three academics, so how much does peer reviewing slow down your capacity to get the results of your research to public awareness and understanding, and to people like us, who often look to academics for in-depth research? Do we have a slower capacity to get critical new understanding in front of the public and Government because of the system? Are we dragging our feet because of the limitations we have placed on it?

Dr Dover: No, I don't think so. There are plenty of ways of getting information out. I welcomed the opportunity when I saw this Committee's call for papers, for example. That is one way you can disseminate research that does not require peer review and is therefore very rapid response.

In one sense, the peer review system is painfully, torturously slow. There is no getting away from that. It is more about the incentives placed upon academics. The currency of the profession is peer-reviewed journals. If one was going to publish only through those, the answer to your question would be yes, it is very slow—maybe 18 months to two years slow—but there are alternative forums that one can disseminate research through, and that is a choice for the academic. Do you find a way of re-spinning it, essentially, to manage to get something out sooner, or do you remain purist? It is the incentive structure, rather than the mechanism, that is the problem.

Q90 **Mrs Moon:** Are there implications for your career, though, of getting it through the peer review process?

Dr Dover: Absolutely. If you opt to publish outside the peer review process and do not work it back through the peer review process, clearly your career will go much slower than it ought to.

Mrs Moon: Does anybody else want to come in on that?

Elisabeth Braw: I was just going to make a somewhat related point about the academic bubble. As Rob mentioned, there are alternative ways of making your findings known. Personally, I write op-eds every now and then, not just because I am a former journalist and I like writing in that format but because it reaches people outside the academic bubble. In my case, I am very keen to reach business leaders; they are a key audience for any discourse in national security because they play such a large role.

Q91 **Mrs Moon:** The question I wanted to ask was how much we have weakened our system by diversifying responsibility for critical national infrastructure. In particular, big business—not just British big business but world big business—now controls large amounts of critical national infrastructure: our heating, our water, our electricity supplies and our telephone systems. How much has that weakened us? Given that a recent review showed that 72% of large businesses have suffered cyber-

attacks and 73% of large charities, who also do a large amount of government business, how much have we weakened ourselves, and what responsibility should the Government place, when setting up contracts, in ensuring that cyber-defence and responsibility for protection of systems is built in to the contracts?

Elisabeth Braw: This is another weakness of our liberal democracy. It is a strange brand of weakness that the private sector operates independently from the Government and the Government can plead with the private sector, but unless they legislate, they do not have very much power to force companies to pursue particular actions. When it comes to weaknesses in cyber-defence, the reality is that most companies will ask for forgiveness rather than permission. They will assume that they will be fine, and if there is a crippling attack they will apologise and, of course, accept the damage to their financial performance; but that is still cheaper than putting these comprehensive defence systems in place to better protect themselves.

The question is, what do the Government then do to incentivise the private sector, specifically in strategic sectors, better to protect themselves, given that they are for-profit companies? The Swedish Parliament currently has an inquiry under way into the role of the private sector in total defence, which looks exactly like that—how can we incentivise the private sector? I am not sure what the findings will be, but I can see two ways of doing it. One is incentivising the company, so that if you better protect yourself to the highest extent possible, you are rewarded by the Government. The other avenue is legislation. Unfortunately, I think that legislation may be the most suitable option, simply because we have to have every company on board. Not just nine out of 10 energy utilities or electricity utilities—it has to be 10 out of 10, otherwise the adversary will zero in on that 10th company that has poor protection.

Dr Hillingdon: I think your question is superb—every question is superb, but I was waiting for this one. It partly addressed the question you asked earlier in terms of diversification and foreign investment. Before I came here, I looked at the top 20 world economies from the 1960s until now. When we look at the United Kingdom in the 1960s and ’70s, you were at the top—the second. There was a big difference in terms of your GDP with the rest—the ones below you, fifth, sixth, seventh, eighth and ninth.

This trend has slightly changed; the dynamic has changed. I think that in 2003 or 2004 China came into this league. Now, when we look at it, the picture is a bit daunting, in the sense that when we look at the position of the UK as fifth or sixth in terms of nominal GDP, the distance between you and the top countries above you is increasing. With the ones that are below the United Kingdom, there is literally no distance.

On the issue of nominal GDP—the picture is a little bit worse when we look at GDP in terms of purchasing power parity. The UK comes to ninth, which means affordability in this country. The GDP is not doing as well as it used to do, and that puts pressure in terms of decision-making and what the

British Government can and cannot do. If the economy is not as strong as it was, then of course it puts you in a place where you will have to say yes to trade deals to which you would not have said yes if you had had enough money. You would not have said yes to some of the investment in this country if the economy was stronger.

It also goes back to the question of asymmetry of knowledge. That is part and parcel of this issue. You are selling that knowledge because it means immediate, quick money, but in the long term the damage is massive. On that note, we could look at the bigger issue, which is GDP. That itself underpins other issues, which I will point out later on, if I get a chance.

Mrs Moon: Thank you. Rob?

Q92 **Mr Francois:** Good afternoon. I can't promise you a superb question but I can promise you a straightforward one. If each of you could make one concrete suggestion to us as a Committee about what we could do to improve our defences as a nation against hybrid threats, what would that specific suggestion be?

Dr Dover: Make better use of the comparative advantage of GCHQ. Task it in particular ways. We are only working from the open-source information, so it is not clear how it is tasked, but from what we can tell from open source, we have a comparative advantage, certainly in the cyber realm, sitting in Cheltenham and, whether it is under-utilised or not, I would suggest that was almost our strongest card to play.

Q93 **Mr Francois:** So you would leverage that more.

Dr Dover: Yes.

Q94 **Mr Francois:** Thank you, that is very clear. Dr Hillingdon?

Dr Hillingdon: Capability priority. Can I give you an example?

Mr Francois: Please do.

Dr Hillingdon: Imagine you have got a very competitive capacity in this country and there are four places for that capacity and you are being told you can take two people on their capability. So, you employ two people conditional on their capability. You can also employ the other two but you need to take other criteria into account. Effectively, you are looking at their categorical criteria. In other words, "Is she female? I might give her a job." I am undermining myself right now.

Mr Francois: Careful, don't get us going on all that stuff.

Dr Hillingdon: I won't.

Martin Docherty-Hughes: Please do!

Mr Francois: Be careful what you wish for.

Dr Hillingdon: What I am saying is that, if the capabilities are put in front of everything else, that would help us. Going back to the example I have

just given, if you are recruiting four people, two of them not so capable—that is happening here and there in the United Kingdom—you have included two people. Yes, that is called inclusion, but it comes at the cost of excluding two very capable people. What is happening? The organisation is not performing well, you have lost two very good people and you might also see talent migration. These two people are in demand, so they will go somewhere else. That is your loss and somebody else's gain. To answer your question even with the wrong words, I would say on this note that competitiveness needs to be at the core of this country on all fronts. If you get that motto in front, everything and everyone wants to do better and that quality is appreciated, then Britain will remain as Britain.

Q95 **Mr Francois:** So in essence, it is to be more competitive. Thank you.

Elisabeth Braw: I would say you should suggest the introduction of a national security curriculum into state schools. I realise the devolved parts of this country do not fall under the jurisdiction of this Parliament, but it could start within your jurisdiction. It is a major undertaking but it would pay great dividends in the long run. There is very little that unites this country at the moment, but the need to maintain our way of life in the face of national security challenges is something that unites all of us and where we can make major strides.

Q96 **Mr Francois:** Just briefly, politicians are always being besieged by different interest groups that want to change the national curriculum, at least in the English example, to add in whatever their particular subject is. There is no shortage of suggestions to amend the national curriculum. I even suggested amending it once. If you were to do that, what specifically would you include under that heading?

Elisabeth Braw: I would include information literacy, natural disaster response in one's local community, response to crippling cyber-attacks, what to do if critical national infrastructure stops functioning and if the internet goes down, which I think is every child's biggest fear. It shouldn't be, but unfortunately it is. By the way, this ties in with the increasing frequency of natural disasters, which is something that will pose an extreme burden on the Government if it is the Government alone that are to respond.

Mr Francois: Okay, so we've had leverage GCHQ, be more competitive and amend our national curriculum. That is a spread of answers.

Q97 **Martin Docherty-Hughes:** The fusion doctrine, introduced by the national security capability review, which was mentioned earlier, relies on the formation of strategy and the integration of defensive, security, economic and influence aspects of national capability. Can the UK do this effectively? Elisabeth, if you can answer, what can the UK learn from the efforts of Scandinavian and Baltic states—given that you mentioned Latvia—to build resilience against hybrid attacks by engendering co-operation across Government? You may also add in about Ukraine's experience, if you want to.

Elisabeth Braw: I think that the fusion doctrine is a very impressive undertaking by the UK Government, and something that other countries can and should learn from. The UK Government have shown that it works well in the case of a minor attack, such as the Skripal case, where the UK Government responded forcefully and in a combined fashion, using several tools at their disposal, including asymmetric ones. That worked very well. My concern is that it may not work as well, as it is currently set up, if the UK is faced with a more ambitious or larger attack than the Skripal case.

If I can add one more thing, the fusion doctrine completely excludes the public. It treats the public as a passive participant in our national security. That is a lost opportunity. The Government cannot dictate to citizens what to do, but they can create ways and structures for members of the public to becomes involved and to become a resource, to assist the Government, so that the Government do not have to be this impenetrable shield extending over the rest of us—because there is no such thing as an impenetrable shield.

Dr Dover: I think the fusion doctrine is essentially Gerasimov-lite—bearing in mind that he talked about his doctrine as something that he feared Russia would face, rather than actively going the other way. It is a useful way of conceptualising something like the Finnish total defence concept.

My only minor concern is that it has the capacity to make the NSC in effect a sort of micro-Cabinet Office, which all decisions route through. That is a potential risk that ought to be thought through more carefully, if people concur that that is a risk.

I think it should be widened. I don't know the mechanics of it. I don't think it exists in the open source. Certainly the diagrams that appear in the official documentation suggest bringing in the private sector, again mimicking the Finnish total defence model. In one sense it is too early to say—which is a bit of a cop-out answer—but I think the way it is configured is the ideal type for this moment. It just requires fleshing out and bedding in.

Dr Hillingdon: Just briefly, I read the document about the British Government's fusion doctrine and the three components that make that circle have always existed. They have just been put together and called fusion. The UK has always done well with each of those components: economic, defence, diplomacy and so on. So they are being put together. Is that good? Yes, because it has always been good. Can it get better? Yes, if the key component of that fusion, which is the UK economy, becomes stronger.

Q98 **Martin Docherty-Hughes:** Do you want to say anything about the impact on Scandinavia and the Baltic states, and how they are dealing with it? Also, I know that Ukraine is on the frontline. Its largest neighbour turns its electricity off on a regular basis. It is learning every day. What can we learn from them?

Elisabeth Braw: Total defence was a concept that Sweden came up with during world war two in response to total war. How do you respond to total war from a mighty adversary? You use all the resources at your disposal, which is all of society, not to fight your adversary in combat, because that is what your Armed Forces do and there is little the civilian population can contribute in that sense, but essentially to slow their advance within the country, to entangle them. Finland and Norway then adopted it, and to a lesser extent Denmark.

What can we learn from them? It is really about the whole-of-society approach. This country is very good at a whole-of-Government approach, but a whole-of-society approach is something that offers a lot of potential. It would also be healthy, as we are becoming more diverse in many ways as a country. What can unite us? I would argue that national security can unite us. In fact, we have to unite, because there are serious threats against this country.

Several aspects of total defence could easily be adopted by this country—for example, the national defence course, which the Swedish Government have run for a long time. The Finnish Government have recently run it more successfully. Essentially, it is a residential boot camp for one month for emerging leaders across society—from politics, the Armed Forces, civil society and the private sector—where they learn the basics of national security. If you were Finnish, you would all have attended this course. It creates not just the basic understanding of what national security means—in the case of Finland, but it could work here too—but it also creates links between leaders across society that can actually enhance cohesion in situations of aggression against the country.

Q99 **Martin Docherty-Hughes:** Finally, we have talked mostly about state actors, but hybrid warfare is about more than just state actors. We have a network of huge corporations such as Google, Amazon, Facebook and Twitter, which own huge amounts of our individual personal data. Some would say that they pose a hybrid threat to not only the state, but the individual. Do you have any comment on how we enable ourselves to be better owners of our own data in terms of hybrid threats?

Dr Dover: There are obvious regulatory things that can be done to try to blockade off those big companies' abilities to harvest, keep, recycle and repurpose that information. I think that one of the key threats that comes from those companies, and the way that we are now receiving and interpreting information is—I'm not a neuroscientist—neuroplasticity. That is, the way that we are less able to look at long-form information. Within the open-source account of the intelligence community, the international intelligence community is concerned about the way that their analysts are consuming information. Some nations have changed the way that they allow their analysts to consume information, in order to guard against the shorter-form, less-depth approach. From that point of view, I am more concerned about that, because that really affects the core Executive and Government's ability to respond to strategic-level threats and to map a strategic course.

Putting that to one side, for the rest of society there are academics talking about those companies in terms of them being states. They are so persuasive, large and powerful that they are states in and of themselves, and therefore should be treated as such. Actually it is missing the regulatory framework. There are ways of imposing business costs on those companies that mean that they can only respond in certain ways in certain jurisdictions. To a certain degree, the pace of technological change has been so swift that it has really overtaken the ability to regulate them effectively.

Q100 **Martin Docherty-Hughes:** Would you say that GCHQ etc. are also limited in their own acceptance that technology has moved so fast? While we may think in the western liberal democracies that our security services are up to the job, there is a concern that, because tech moves so quickly, we are behind on this.

Dr Dover: I think that's fair. Partly, when Snowden produced his partial leak that was then reinterpreted and reinterpreted, one of the shocking things was that there was almost a transnational class of very technically literate programmers such as Snowden, who had a libertarian precept that was completely out of line with the political context of that agency and those who run it and the strategic-level oversight, but also that the things Snowden was reporting on were so far away from the understanding of regulators and legislators. They just had no idea that that was even technically possible. There is a sense that there are almost transnational tribes of people working in ways that we almost cannot imagine, because we just do not understand the technology well enough.

That is not necessarily negligence on the public's part; it is the speed at which these people are working, and the processing, storage and analytical capacity that they are working with. In some senses it outstrips law enforcement. If you want to pick an example, is Facebook's ability to map a social network superior to UK law enforcement? The answer might well be yes.

Mrs Moon: I would remove the "might well".

Dr Dover: I'm just being kind.

Q101 **Martin Docherty-Hughes:** I know you want to move on, Chair, but can I come back to the point about our not knowing? If we go back to the introduction of the internet or the introduction of, say, cryptocurrencies such as Bitcoin—this may sound like a diversion in terms of subject matter, but it is not—our intelligence services would have been aware for the past 20 to 25 years, if not 40 years, of the move within academic circles to that type of programming and technology. My concern is that they did not see it as a tangible threat. This might be in retrospect, but that technology was being talked about 40 years ago.

Dr Dover: Yes. There is an arms race around that. If you think about the Tor Browser and those sorts of proxy, there is some literature in the IEEE—electrical engineering—conferences in the summer where they are talking about the ability to unpick Tor, but it is obviously painstaking and

you would need to specifically target; you would need very clear targeting information to be able to unpick it.

Q102 **Martin Docherty-Hughes:** But it can be done?

Dr Dover: It can be done.

Q103 **Martin Docherty-Hughes:** Forgive me for a slight diversion, Chair, but if we go back again to the tech, there were issues in the mid-2000s around Bitcoin, but they physically broke into Bitcoin. To change the subject, that took an amount of energy, but it was done by individuals and not by state actors.

Dr Dover: My point would be about the arms race. By the time that has been caught up with, adversaries or bad actors using that technology will then move.

Elisabeth Braw: I was just going to make a short point about that. Intelligence agencies did not bother with it very much initially, because it was seen as entertainment. Facebook was a diversion initially, when it started, and the other social media networks as well. Now we are in a convenience trap where it is an integral and apparently necessary part of everyday life. I think there is potential for a European Government, whichever it may be, to take a stand and crack down on these very unhelpful practices by social media companies. I think other Governments would swiftly follow. It might have to be done within the EU framework, but I don't think so.

Q104 **Phil Wilson:** Do you think the UK Armed Forces have the resources and capabilities they need to deter both conventional and hybrid warfare?

Dr Dover: No, in a word. Again, I look to the Finns as the exemplar of being able to ramp up response force very quickly—in a matter of hours. Whether it is persuasive or dissuasive on a Russian invading force is moot, I think, but they have spent an awful lot of time thinking about how to ramp up a response very quickly, with the timeliness being the core thing. The UK is a medium-sized military actor, which sits largely behind nuclear deterrence.

As I said earlier, I think the hybrid efforts against us have been largely because of adversaries trying to find a way of prosecuting a continuous war without agitating us enough to take proper steps. From that point of view, I think we have arguably the wrong configuration to counter that type of threat. Presumably you are going to ask me in a follow-up what the ideal would be, and then I will look down at the table while I scribble rapidly, thinking about that.

Q105 **Phil Wilson:** I was going to ask why you think the Government are not investing in the necessary capability.

Dr Dover: The spread of threats is so large—this is almost a recapitulation of the east of Suez debate. Dr Lewis would be in a far better position to talk about that than I would, I suspect.

Chair: I'm old enough to remember that.

Dr Dover: It is the full-spectrum acting that is the issue. If we aspire to a full-spectrum set of capabilities and responses, the amount we are investing is too small.

Q106 **Phil Wilson:** So do you think we are going to stay at conventional capabilities in the gamut of capabilities that we need?

Dr Dover: The breadth of operational response, we have that. But we do not have the sheer quantity. We are always going to have to do something with others, so there is a co-ordination effect. I would be concerned by the experiments of Russian and Chinese militaries in the ionosphere. Essentially, this is about being able to knock out various bits of kit, be it GPS or communication kit. Can we operate in an analogue fashion in an operational theatre dot dot dot? That would be a great essay question for someone at the Defence Academy of the United Kingdom. My hunch would be no. The network-enabled force that was de rigueur during the '90s and noughties in all academic defence studies literature is correct. But in terms of the undermining of our own defence industries, we are entirely reliant on supply lines that exist outside this country. If you are asking about the UK's sole ability to repel these sorts of hostility, the answer is clearly no. If that is within the alliance, it is conditional on all sorts of politics and all sorts of sharing of equipment and modalities.

Dr Hillingdon: I tend to agree with Rob. I agree that you might say that the United Kingdom is not capable, but it does have some alliances that it can count on. On that note, my answer is then yes. You would say that the UK cannot do something on its own, but you have to think about NATO and about certain UK allies, so my answer is that yes, the UK does have the capability but not necessarily on its own. You have to realise that the UK is quite advanced in terms of defence and technology, and has always been at the forefront in that respect. You might not have 20 aircraft carriers, but you do have advanced, high-quality technology compared to some of the other technology that tries to outdo you by having large numbers rather than high quality. The issue with defence is UK quality. It is not always about quantity. The UK is brilliant on the quality front, and as far as quantity is concerned, the UK has really good alliances through which it can work.

Dr Dover: But even with the best, we might have two brilliant aircraft carriers but there are only two.

Elisabeth Braw: If we look at conventional defence, the UK itself has not been attacked or invaded since the second world war, which shows how good our Armed Forces are. An article in a newspaper the other day said that France is supplanting the UK as America's favourite ally. I do not think that is the case at all. The UK's success so far within NATO in defending itself against conventional aggression indicates that it is doing very well. An almost paradoxical consequence of that is that the Armed Forces are so good—even though people say they do not have enough money, which is probably true—that we rely on them for everything. If

there is a drone at Gatwick airport, we will say, "Oh we have to call in the Air Force," or if there is a flood we will call in the British Army. Even if we need guards at the Olympic games, we call in the British Army. We put so much trust in them that it is almost a paradoxical consequence of their success. Maybe private-sector back-up in the case of an emergency is what we lack in this country. Look at the number of cyber-engineers, as you have dealt with in previous sessions. I know the House of Lords has dealt with it as well. What do we do about the extreme shortage of cyber-engineers? I suggest there should be something like a national cyber-firefighting unit that could be called up to assist CNI companies in case of a major attack. That is something that could be run by the MoD. It would obviously be an addition to 77 Brigade, which is not really that. That is a long answer to a short question.

Q107 **Phil Wilson:** I was going to come on to 77 Brigade. How important are the capabilities that it offers to our counter-hybrid efforts? Does it need to be expanded? Or is it a case of keeping what we've got but deepening its capacity? Would you say there would be a shortage of experts that we require for the work to be done properly?

Elisabeth Braw: So 77 Brigade is a statement of intent, but it can't, by itself, do all the work that needs to be done. If I could just add, having been a technology correspondent for five years in San Francisco, there is an enormous gap between tech types and the national defence establishment. It is just an unfortunate reality.

Q108 **Phil Wilson:** Is that in America as well?

Elisabeth Braw: There and here. Even tech types or cyber-engineers who are extremely uneasy about Ministries of Defence can see that their skills are needed to maintain our way of life. I think there is potential for something like a civilian version of 77 Brigade, where skilled cyber-engineers could volunteer their time and would be called up in case of a major incident.

Q109 **Phil Wilson:** I can't remember the exact figure, but a fair percentage of personnel in 77 Brigade are in the Reserve, aren't they?

Elisabeth Braw: Yes.

Phil Wilson: I might be wrong, but I think it is about 40%.

Elisabeth Braw: Exactly, so if we had something like that outside the Armed Forces structure, but essentially with a similar mission.

Phil Wilson: Dr Hillingdon, do you want to add something?

Dr Hillingdon: Only to the part of your question that I can answer. Should we spend more? My answer is yes. Why? Because your adversaries are spending more on different capability in terms of defence. If the UK does not spend that, the state of equilibrium—the balance that you have kept for years—you will get it this way or that way. Yes, you should spend more to keep that balance between you and them. Otherwise, the UK will

be more vulnerable. Of course, people will challenge me about where the money comes from. If that challenge comes, I can answer it.

Q110 **Martin Docherty-Hughes:** Can I come in there? You talk about finance and what that investment is. There are some who would say it is not necessarily about our notion of traditional defence. Taking Elisabeth's perspective, it would be investment in education and in infrastructure, so that overarching theme of total defence is not just about conventional or any other type of military aspect.

Dr Hillingdon: I will try to answer that. My question would be, what is the price of the United Kingdom? What sort of price are you happy to pay to protect the United Kingdom? I guess some of you are sitting, thinking, "The price of the United Kingdom for me, as a British person, is priceless. I want to give my all to protect it." If that is the case, to guard the country defence is a priority. If there is no defence, you might think maybe not to spend on education.

I will expand that by giving a simple example. If you have a pet and take it to the vet, the vet will tell you, "Okay. I am giving you 12 Stronghold flea drops. Use one a month for 12 months of the year." He or she will tell you there is no point in using six of them instead of 12 of them because that is ineffective and is not efficient either.

If you are spending on defence, you might as well spend enough to reach that optimum level. Otherwise, it is only ticking the box and is not effective. I can understand competing priorities between NHS, education and so on, but the question goes back to this: "What is the price of the United Kingdom?" For that, it should be protected and protected well.

Dr Dover: I would frame it around deterrence. I would use a set of lenses that looked at deterrence—what will deter my adversary? As well as deterrence, there has to be offensive capability matched into that. In terms of the deterrence, you might look towards a more holistic set of propositions, so you would look at traditional kinetic military capability, but you would be looking across the patch that you have talked about. If one is looking at offensive capability, one is probably not looking at an advanced kinetic capability, unless we are going back to the late 1990s or early 2000s where we had a muscular liberalism and interventionism, which, given what happened around Syria, I do not foresee there being much enthusiasm for.

Q111 **Martin Docherty-Hughes:** But what if your adversary's real objective is not total war in the traditional sense, but turning you into them?

Dr Dover: Well, if the public are going to acquiesce to that in one way or another, it is going to be quite difficult to defend against it anyway, isn't it?

Elisabeth Braw: If I can just add, I think they are already turning us into them, because we are constantly discussing what our adversaries are up to and what they may intend to do. If we turned it around and said, "We are willing to defend ourselves against every threat and that involves all of

society and what the rest of society can do outside the Armed Forces," it is really adversary agnostic, because what they want to do to us is disrupt our way of life. What we can do then is deny them that opportunity. The result would be that—speaking of deterrence—we would communicate to them, "There is no point in you trying to do it, because you won't be successful," and for us it would bring the benefit of not always having to worry about what they might do and how they might poison our liberal democracies.

If I can just follow up on the question that Mr Spellar asked earlier about offensive actions preceding a potential attack, which I think we forgot to answer, something that the US cyber command is doing very well is communicating to hackers operating as proxies on behalf of hostile state actors that they know who they are and where to find them. That is a very powerful deterrent. They do not attack them; they just tell them that they are aware of their actions. That is something that can be replicated—not just with lone-wolf hackers acting as proxies, but possibly with companies.

Q112 **Mrs Moon:** One thing that worries me is that we forget that part of the aim might actually be not traditional warfare but fighting warfare through the ballot box. You can actually use the ballot box as a way of state capture and we have forgotten that. But none of you has mentioned the UK cyber-defence centre yet. Is that because you do not think it is a critical player? Is that because you do not think it has been around long enough to have made a big difference? Why not? Why has it not been mentioned?

Dr Dover: Because I didn't get to answer the question that you posed to us—because I was missed. Yes, absolutely. The question you asked earlier was about the vulnerability of key infrastructure and the foreign ownership of firms.

Mrs Moon: Yes.

Dr Dover: I was going to answer in a way that alienated at least half the political science community and say that there is no evidence that the public sector does this any better than the private sector, because of those commercial realities. There is no commercial company that wishes to have vulnerabilities present, even those that are partially owned by state investment firms.

The National Cyber Security Centre, cyber-defence and GCHQ are mandated and actively work with companies of all sizes, so we no longer have that division between the public sector and the private sector in terms of being able to access high-quality cyber-defence advice, up to and including for critical infrastructure such as programming and defensive technology that assists them in maintaining service. So yes, it is slightly too soon to give it an absolutely clean bill of health, but those mechanisms are in place. I think they are certainly fit for purpose and they are heading in the right direction. They are the things that one would suggest was best practice, so I feel—within the ambit of, "There is going to be continual attack and those attacks are likely to get more sophisticated,"—that the

UK Government has responded in an appropriate way to that with those institutions.

Q113 **Mrs Moon:** Does either of the other two witnesses have anything to say?

Dr Hillingdon: Just briefly. If you look at the Government's recent report about FTSE 350 companies in the United Kingdom, a large number of chief executives of these companies do not know a lot about how to protect themselves from cyber-attack. The UK Government has put in some really good schemes to make sure these businesses are being trained, such as—if I can read my writing—Cyber Essentials, but there is a severe lack of training, especially for SMEs, on that. Is the UK doing well with cyber-security? I still believe that the UK, in terms of cyber-security technology, is at the forefront. The UK is doing really well on that. Just because we don't know exactly what the Chinese are doing—because we don't have enough students there, although they have enough students here—doesn't necessarily mean that they are doing better, but it does tell us that we don't know enough about that.

Q114 **Chair:** I want to close by picking up on a few points that were touched on earlier. First, we talked a lot about hybrid warfare as a technique that tries not to cross the boundary into conventional warfare, but it is also the case, isn't it, especially where state actors are concerned, that hybrid warfare could be used as the precursor, to soften up a country prior to engaging in a conventional attack? Have any of you any observations on that scenario, which of course was seen in Georgia, for example, quite a long time ago?

Dr Dover: And, indeed, in Crimea. You could argue that what is going on in Ukraine now is similar. It's a salami-slice approach. It's almost the classic "Yes, Prime Minister" talk about nuclear deterrence: "When do you press the button, Prime Minister?" It gets closer and closer and closer. In that respect, those forms of hybrid warfare or grey warfare are precisely to be able to attack the centre of gravity of a country without actually going over the line and to be able to go over that line, where a military response is justified, at a point where it's too late for that to be an effective response. From that point of view, this is a new era of warfare, to some degree, because previous operational theatres didn't quite have that nuance; there wasn't quite the investment in that.

Q115 **Chair:** Before I bring other Members in, perhaps you would consider this point as well: to what extent does terrorist activity qualify as hybrid warfare?

Dr Hillingdon: To a large extent.

Dr Dover: I think it absolutely qualifies.

Q116 **Chair:** But there, the terrorists are not really worried about crossing any boundaries; they are just doing the best they can—or the worst they can, as we would see it—given their limited resources, aren't they?

Elisabeth Braw: If I can take a contrarian view, I think terrorism is a terrible form of aggression, but I don't think it qualifies as hybrid warfare

in itself. It can be used as part of hybrid warfare, but the nature of anything hybrid is that it has several components, and—

Q117 **Chair:** And terrorism is pretty much a one-trick horse, isn't it?

Elisabeth Braw: That's right. Going back to your original question, as Mrs Moon also pointed out earlier, we should be concerned about becoming so used to the steady drumbeat of low-grade or low-intensity aggression that we don't notice when something—well, we are not prepared for the next big step. By the way, can I just add that when it comes to cyber-attacks or cyber-aggression, that activity includes pre-positioning of malware that can then be activated? We think, "Oh, they are just testing out our networks," but actually they are putting malware there that can be activated when they need it. What do we do about that? I think our main challenge is raising public awareness of the fact that the current level of convenience is fantastic and it is a great privilege to live with this level of convenience, but it is not impenetrable and we are vulnerable.

Q118 **Chair:** But we are building in future vulnerabilities at every stage and nothing seems to stop us doing it. For example, self-driving cars: can you imagine those being turned into lethal weapons?

Elisabeth Braw: That is the convenience trap. Maybe they cannot become weapons, but they can just become unreliable. Because the opportunity exists, most of us ordinary citizens would say, "Yeah, I'd much rather just be a passenger in a car than have to deal with driving and parking." The lesson from that is that the public have to become a much more active part of national security and think about the price we pay for this level of convenience.

Dr Hillingdon: Terrorists don't grow behind the bushes. They have sponsors. They have either states sponsoring them or non-state actors—rich businessmen and so on—supporting them. On that note, terrorism is a hybrid threat, and a lot of the time the state is behind that. Big money is going—if you look at the payment to the people who fight for these terrorist groups, they are getting paid more than the Armed Forces in those countries. Where does the money come from? You might not be able to detect their transactions because they go from one pocket to another in the physical form, but there is big money. Until that big money is out, terrorism will remain, and I do not think as an entity on its own. They have sponsors, big sponsors.

Q119 **Chair:** I want to take you back, Anna, to the point you made earlier. You talked about us being prevented from changing laws that would better protect us. We have been speaking a great deal in theoretical terms. Can you give a few specific examples of the way in which the law could be changed better to protect us?

Dr Hillingdon: I have never worked for the intelligence services, so I don't know how that operates. I only know from what I hear. What I am saying is that when you hear that somebody bombs some place and then the terrorists are identified, they say, "He was known to the intelligence services." The immediate question you ask is, if he was known to the

intelligence services why have they not put him in jail and locked him up at least?

Q120 **Chair:** I think I can answer that—unless you want to do it, John—but there was a thing called internment, which was used in Northern Ireland. I know the security services get a lot of stick when a terrorist carries out an atrocity and they say "Well, he was on our radar; we did know that he was an extremist." Personally, I would be more worried if they hadn't known he was an extremist. The trouble is you can't just lock people up, surely, for their views, and you can't necessarily follow all people with extreme views round the clock. Am I wrong?

Dr Hillingdon: No, I am on the side of the intelligence services. I was going to finish by asking whether it is because they are not given enough power. Should they be given more power to be able to protect better? I think that if you talk to them, they might be frustrated: "Oh, I knew this person but I didn't have enough authority to take it to the next stage." That is my point. They do a good job, but I don't think the law is behind them to protect the security services.

Q121 **Chair:** But what if the person hasn't committed an offence? That is the problem you've got. What if the person hasn't committed an offence but is just regarded as a subject of interest who might one day commit an offence?

Dr Hillingdon: This will come back to the definition of a hybrid threat. You might not always find concrete evidence when there is something. What would you do? Do you take the risk and let the person take a van and kill 50 people? Then you get him? Or you say, "This is a hybrid threat. I might not have concrete evidence. I may have a law to support my intelligence services to do something."

Q122 **Chair:** Okay. Time is against us. I am going to give a final word to each of you. If you could address any outstanding points that you wish you had made earlier and just answer how specifically you think the hybrid threat to the UK is likely to develop over the medium term. Do you think we are up to the task of being able to identify it and prepare ourselves accordingly?

Dr Dover: I think there is an international and domestic dimension. Internationally, I think allies, partners and places of interest will become subject to quite sophisticated hybrid attacks and threats, and I worry that we would be unable to mitigate them in consultation with the country they affect and to interdict if necessary. Domestically, there is a much longer debate around terrorism—I could probably spend half an hour talking about that, but obviously I can't, and won't. Domestically, unless countermeasures are put in place on the issue of misinformation and disinformation campaigns, but also, as we talked about earlier, bad investment and how that is used as political leverage and political security leverage, essentially the picture gets worse, not better.

Dr Hillingdon: If the economy is the UK's priority, and there is a link between the economy and the UK national interest, anything that can jog

the UK economy is a threat and therefore needs to be taken into consideration. The economy should be at the forefront of all decisions to make sure that the UK can stay in the top five and does not shift into the top 10 or the top 20.

Elisabeth Braw: I agree with Rob that the attacks, or the aggression against us, will increase rather than decrease, and it will increase along with our continued technological development, because that will create additional vulnerabilities. In terms of concrete suggestions, and following up on what Anna said about the health of the UK economy, I think that what needs to happen, given that we cannot fully protect ourselves against every act of aggression, is that we exercise for contingencies, and that includes companies. If I am not mistaken, the Government is not allowed to practise, for example, energy cuts under realistic circumstances, and maybe there is an opportunity to change legislation to allow for such exercises, so that companies would be fully prepared in case of a serious attack.

Chair: Thank you all very much indeed. We have had a great deal of information, and theoretising as well, so I am most grateful to all the panellists and to colleagues on the Committee.