HOUSE OF COMMONS

Defence Committee

Oral evidence: Defence in the Grey Zone, HC 50

Tuesday 23 April 2024

Ordered by the House of Commons to be published on 23 April 2024.

Watch the meeting

Members present: Sir Jeremy Quin (Chair); Sarah Atherton; Richard Drax; Mr Kevan Jones; Mrs Emma Lewell-Buck; Gavin Robinson; John Spellar; Derek Twigg.

Questions 1-42

Witnesses

I: Elisabeth Braw, Senior Fellow, Scowcroft Center for Strategy and Security, Atlantic Council, and Professor Andrew Mumford, Professor of War Studies, University of Nottingham.

Examination of witnesses

Witnesses: Elisabeth Braw and Professor Andrew Mumford.

Q1 **Chair:** This is our first session in the Committee's inquiry into the grey zone. We are joined by Elisabeth Braw. Elisabeth, do you want to introduce yourself and your background?

Elisabeth Braw: First of all, thank you for the invitation. I am a senior fellow at the Atlantic Council's Scowcroft Center for Strategy and Security. I am also the author of "The Defender's Dilemma: Identifying and Deterring Gray-Zone Aggression".

Chair: It is a great pleasure to have you with us. Thank you for joining us. Another colleague, Andrew Mumford, Professor of War Studies at the School of Politics and International Relations at the University of Nottingham, has been delayed by the trains. He will be joining us in due course.

Elisabeth, thank you very much for kicking off the session. John will start our questioning.

Q2 **John Spellar:** The opening question, Elisabeth, is: how would you define the grey zone?

Elisabeth Braw: It is aggression by states or their proxies against other countries or their interests using means below the threshold of armed military aggression.

Q3 **John Spellar:** Only military and physical, or kinetic, or other areas as well?

Elisabeth Braw: The moment it involves kinetic violence, it leaves the grey zone, but the troubling thing is that there are many means that can be used below the threshold of armed military violence. We are seeing it as we speak in the Baltic Sea, with our new NATO allies, Sweden and Finland—Sweden in particular. We are seeing the Russian shadow fleet parking itself off the coast of Gotland, loitering there, conducting ship-to-ship transfer of oil. Sweden stands to suffer considerable environmental harm if that oil spills, and yet it is not military aggression. The harm that can be caused is obvious, in addition to the provocation, but it is not military violence. That raises the question, as we speak, of what we can do about this kind of aggression.

Q4 **John Spellar:** Where in that spectrum do you place the classic—we saw it in the Cold War, and we are seeing much of it now—agitation, propaganda, undermining of social cohesion in societies and of the will to take action, and, indeed, moving of people into what, without disparaging Finland, we would have called in the Cold War a Finlandised state? Or do you think it is a separate area?

Elisabeth Braw: We already saw the beginning of grey zone aggression during the Cold War. What is different now is the availability of means that our adversaries can use against us, simply because the world is

extraordinarily interconnected today compared with the Cold War period. Adversaries can use not just disinformation and subversion of our civil societies, but subversion, essentially, of every part of our societies. They can attack or target our companies, both those operating at home and those operating abroad. As a result of the digitalisation of society, obviously they can conduct cyber-attacks. They can attack or sabotage sea-based infrastructure, which we had much less of during the Cold War.

The three and a half decades or so of globalisation and the growing together of the world have created enormous opportunities for our adversaries to harm us and, again, there is not very much we can do to prevent that and to punish them, unless we decide similarly to operate in the grey zone and use similarly unethical or even illegal means.

Q5 **John Spellar:** Should we, though?

Elisabeth Braw: This is the defender's dilemma. What do we do if we are faced with all this aggression, of both the illegal kind and the purely unethical kind? I think that, as liberal democracies, we should remain on the high road, but that makes us vulnerable. But if we don't remain steadfast defenders of the rules-based international order and try to set a good example, I think we as the global community face growing anarchy.

We are already seeing it in shipping, for example, which is another area where there is a lot of grey zone aggression. The Red Sea attacks by the Houthis are a perfect example of grey zone aggression. They are carried out by a proxy force, not an official military force, but of course it is clear to everybody that the aggression is linked to Iran. It targets only Western shipping. Yet it would be unwise for the West to say, "Well, if they target our shipping, we will target theirs." That would lead to anarchy in the maritime domain. Similarly, if we were to respond an eye for an eye in another domain, it would lead to anarchy there, too.

Q6 **John Spellar:** Many of these facets were very much present during the Cold War, although with different technology. What lessons are there for us to learn from that, in terms of mindset and ideology, as well as the full-spectrum approach, which is what particularly the United States and the United Kingdom had during that period?

Elisabeth Braw: I think what can be learned is that you need to involve all parts of society. After the end of World War Two and into the '60s, the UK made incredible efforts to involve citizens in different capacities, so that the state, the Government and those working full time to defend the country would be backed up by ordinary citizens, because the Government can't be everywhere all the time, we couldn't afford such an undertaking and it would not be an attractive way of life.

Then, of course, we had the liberalisation of the '80s and globalisation, and the idea that you can or should involve citizens fell by the wayside, I think—and also because there was not really a need for citizens to be involved in keeping the country safe. That is something that we can definitely learn from. I don't think that Brits back in the 1950s and 1960s were better than Brits today; it is just that they were invited and

encouraged to be part of this collective undertaking of keeping the country safe—and similarly in the US, but less extensive. It is also an opportunity for citizens to contribute in a meaningful way to the country. We saw it during covid with the "NHS army". The moment it was announced, people signed up in such large numbers that, in the end, the NHS didn't need all these people who wanted to help.

When a crisis strikes, we see that there is a willingness to be part of keeping the country safe, so if we were to set up such structures before a crisis happens, I think people would contribute and we would then have this sort of civilian army, citizen army, resilience army or resilience corps of people who know what to do. That is useful not just when a crisis occurs but as a signalling function—to help our deterrence signalling. It helps us to tell the countries and their proxies who may wish us ill, "Yes, you can try it, but look, we have at our disposal not just the Government and the Ministry of Defence, but all of these citizens who would know what to do in a crisis. You won't achieve what you are trying to achieve."

Q7 **Chair:** Your comment on the citizens is a reflection back on to the Cold War era. Richard is going to come in as well, but I want to try to elucidate what has changed since, and you touched on it, Elisabeth. It is the increase in technology, which means that there are far more capabilities available to non-state and state actors than would have been the case in the Cold War, and globalisation has created vulnerabilities. We are all far more reliant on each other than we were in the past, and that produces cracks that can be exploited. We have embraced a global view of the world. In the Cold War, there were two different camps; there is now a global view of the world, and we want people to be acting within that global economy. That depends on people respecting the international rules-based order, but there are parties that see advantage in trying to disrupt the whole.

Am I right in thinking that those are some of the areas in which we have moved on from the Cold War, and that it is going to be harder than it was in the era of the Cold War to protect ourselves from those threats because of the nature of how society has changed and how open we now are? Is that a fair assessment?

Elisabeth Braw: Yes, it is. I will give you an episode that I think illustrates how society has changed. Helmut Schmidt, who was Chancellor of West Germany in the late '70s and early '80s, told an interviewer later, after he retired from politics, about a case in 1977 where the Government of Iran wanted to buy a stake in Mercedes. Helmut Schmidt told the interviewer that he told himself that the Ayatollah was waiting in Paris, and it would not be a good idea for the Government of Iran to own a significant stake in the crown jewel of German manufacturing. So what did he do? He called up the CEO of Deutsche Bank and said, "You have to buy this stake. You may not make money straightaway, and you may never make money on it, but you have to do it. It's your patriotic duty." And Deutsche Bank did buy the stake. I wonder: if Rishi Sunak were to call the CEO of a leading bank, or any leading company, today and say, "You have to do this because it is your patriotic duty," would they do it?

Chair: That is a very interesting question, and I think we all know the answer.

Q8 **Richard Drax:** Elisabeth, in your definition of the grey zone, you mentioned the Red Sea and the firing of missiles by the Houthis, and you also mentioned underwater cables. Are you saying that the firing of missiles at US-flagged ships, say, is in the grey zone, as is blowing up underwater cables, which, as you know, is alleged to have happened in the Mediterranean? We think that the Russians did that. Are you saying that that is all grey zone? Your definition originally was everything other than bombs, bullets and explosions.

Elisabeth Braw: Yes. Regarding the Houthis, it is in the grey zone, because they are not an official military. That is of course why it is attractive for hostile states to work with proxies, because if a proxy attacks, we as the West or any other country—

Q9 **Richard Drax:** So that is grey zone, is it?

Elisabeth Braw: Yes, if it is done by a proxy.

Q10 **Richard Drax:** Okay. What about the blowing up of underwater cables? Is that not an act of war?

Elisabeth Braw: It depends who does it. If we were to establish that it was a Russian military unit that blew up Nord Stream in the Baltic Sea in September 2022, Sweden and Denmark would have to respond in a military fashion. However, if we do not know who did it or if it was a non-military unit, it is much less obvious how we can respond. It is interesting that both the Swedish and the Danish investigations have concluded and they have not said who the likely perpetrator is. I think we may never know.

Q11 **Richard Drax:** If the Houthis sank a British destroyer, that is grey zone, is it?

Elisabeth Braw: I think they would not be able to sink a British destroyer, but—

Richard Drax: It is not beyond the realms of possibility. Is that grey zone or an act of war?

Elisabeth Braw: It is an act of war, but because they are not a recognised military, it is essentially an act of terrorism, which you don't have the same rulebook for how to respond to. Officially, they are just an outfit, right? They are not the Government, and that is what makes it so difficult.

Q12 **Richard Drax:** The reason I am pushing this is that back in my day, when I served during the Cold War, that sort of thing didn't happen, but it seems to me that they are now pushing the grey zone right to the edge through proxies, almost to the point of war.

Elisabeth Braw: They are, so we are not talking in the abstract any more. I think it is unlikely that they would sink a destroyer, but as you

say, it is within the realm of the conceivable. That would put the UK in a very difficult position. This is happening as we speak—these developments are happening as we speak—yet we don't have a strategy, simply because it is not even clear which part of the Government should be responsible for grey zone defence. In that case, it would clearly be the MoD, but it is not always the MoD. Who should be the co-ordinating part of the Government that looks after grey zone defence and possibly grey zone retaliation?

Q13 **Mr Jones:** Elisabeth, can I pick up the issue you mentioned around the citizen? I was in Tallinn a few weeks ago, and they have a clear total defence principle, which involves not only training citizens in fighting, but medical support, cyber—the entire spectrum. I have seen similar things in Sweden and Finland, and that is because they are up against the border with Russia. I heard what you said about the Cold War, but do you think that it would be harder in this country now to get citizens to think in terms like that? A lot of people clearly think that it is quite far away from the UK. In Estonia, it was clear that the lesson from Ukraine was that they will not allow territory to be taken, so there is clearly a psychological thing there.

Can I also ask you about proxies, where the responsibility lies and where responsibilities merge? For example, there is evidence of the Iranians using organised crime groups in Europe for assassinations and other things. That is a law enforcement issue, but it is also an extension of the Iranians' proxy war against dissidents, for example. An individual was killed in Belgium not by Iranians, I understand, but by connected organised crime groups. How do you co-ordinate that? Where does that fall—with the military, central Government or law enforcement?

Elisabeth Braw: That is exactly the challenge. The challenge of grey zone aggression is that it can happen anywhere, any time, and using any means below that threshold of armed military violence. They will keep trying different ways and, if something doesn't work, no harm done, because there is no price to be paid. The very fact that they can use any means anywhere makes it very difficult for the targeted country to know how to respond. In the military domain, you can have a good idea of what is coming—you can see what they are planning and you have intelligence and surveillance. But in the grey zone, it is just whatever somebody thinks up, so it is very hard to predict. As a result, it is very hard to know which part of the Government should respond, when, in fact, it only becomes clear what needs to be responded to after it has happened. It is a massive dilemma.

If I can just say something about citizen involvement, the fact that our society here in the UK can be struck—even though it is, as you say, not geographically close to Russia—is, I think, a reason for people to get involved and to be invited to be part of the protection of the country. I am an O2 customer, and I remember when O2 went down for a day a couple of years ago and every O2 customer was outraged because they had to spend a day without the use of their mobile phone. Considering that these are the sort of disruptions that our adversaries can cause using the grey zone, I think it suggests that people would have an interest in being part of minimising that disruption. Territorial aggression does not really apply

that much to the UK, but disruptions to our daily life, in our very convenient society where we rely so much on various digital and modern means—I think the thought of such disruption should motivate people to want to be part of efforts to minimise that disruption.

Q14 **Chair:** The risk is that, rather than people blaming the other actors who may be provoking those kinds of actions, they undermine our confidence in our own society.

Elisabeth Braw: Yes. I wonder if it might not be a good idea for the Government to be more transparent in communicating the threats that UK intelligence is seeing. Until now, the UK Government have been very discreet and have not really told the public about any of the threats we are facing unless they are very serious, but I think that suggests to the public that all is well and they do not need to worry. I wonder if it might not be a good idea to be more transparent about the threats that the UK faces and the damage that they could cause. I think that would cause many citizens to wake up to the idea that things have changed, and that we don't live in the times that we had 10 or 15 years ago.

Chair: Before I turn to Sarah and then back to Kevan, I will welcome Professor Andrew Mumford, who has braved the trains and is now with us—you magically appeared in the midst of the last question.

Professor Mumford: Yes, sorry.

Chair: We will give you a moment to catch your breath and get into it. All the questions are to both of you. If there are elements that one of you wants to pick up or leave to the other, that is up to you, unless we specifically ask for both your views.

Q15 **Sarah Atherton:** Elisabeth, I was struck by the time you took to answer Richard's question, and by the thought process there. From reading the brief and reading around this subject, I was also quite confused about how exactly you define "grey zone", "state threat" and so on. In 2016, NATO declared that hybrid action against one or more allies could lead to a decision to invoke article 5 of the North Atlantic Treaty. Do you think there needs to be a common understanding and language among partners about what exactly we are talking about today? If you do not know quite what it is, and everyone's thinking is different, how do you go down the route of deciding that there has been an article 5 breach?

Elisabeth Braw: We definitely need a definition, and I have to say congratulations to you for catching me out.

Richard Drax: I wasn't trying to; I was just curious.

Elisabeth Braw: This really shows how grey zone aggression is evolving—that we can have a proxy force that may be in the position of sinking a naval vessel. We have not had that in the past. The Houthis are clearly so well equipped, and other militias with similar proxy forces may soon be similarly well equipped, so it is a very relevant question.

Yes, we do need a definition. There are competing definitions—or different definitions, I should say, not competing. But NATO does not have one that it uses as an official definition. I think that is because grey zone aggression has been considered something that you can look after when you have finished looking after military defence and watching adversaries' military aggression, but now grey zone aggression has grown to the point in quantity and variation that we do need a definition of it.

By the way, this is not just in NATO territory; we are seeing things in the Red Sea, the Strait of Hormuz and elsewhere. To give some examples of the threats in the grey zone that face our allies beyond the continent of Europe and the Middle East, there is China's construction of artificial islands, its threat to use an inspection flotilla to block shipping in the Taiwan Strait and its harassment of civilian vessels in the South China Sea—all that is happening as we speak and becoming increasingly disruptive, yet we have not defined what it is. Most importantly, we have not defined the level above which we consider it unacceptable and will respond.

Professor Mumford: If I can chip in here, that is because ambiguity is at the heart of our idea of hybrid threats. Let alone practitioners having problems deciding exactly what constitutes some of the important labels like "hybridity", "use of force" and so on, from an academic perspective I cannot think of another concept in the study of conflict today that has generated so much existential debate about the very existence of the grey zone or hybrid threats.

A lot of the critics of the concept argue that it is sort of like old wine in new bottles—that it is nothing new and there has always been a hybrid element to conflict since the days of ancient Greece and Rome. I do not dispute that, but I would suggest that it is appropriate to think of hybrid threats or grey zone conflict as a new way of understanding old threats in a new conflict environment. That conflict environment has evolved so much that it requires us to start—not pinning down, because I don't think it is possible to come to a universally accepted definition of hybrid threats. In the same way, we cannot even do it with terrorism, but we all know what it is when we see it.

I think Elisabeth is absolutely right that we need to be pushing towards a commonality of language, especially across NATO. There needs to be more unity of effort in that respect. If the policy responses are going to be coherent enough, we need to all be on the same page when it comes to defining those threats.

Chair: Kevan, do you want to come in here?

Q16 **Mr Jones:** What have we learned about the grey zone from recent conflicts, particularly Ukraine? What are your thoughts?

Elisabeth Braw: NotPetya is a very good example. That was a virus unleashed by Russia in June 2017. It was directed against Ukraine and brought down all manner of infrastructure—airports, hospitals, banks, cash

machines and so on. But because it was a cyber-attack, what were the Ukrainians to do? At most, they could have launched a cyber-attack of similar power against Russia, but that contributes to the growing anarchy we discussed earlier.

What was interesting and noteworthy about that attack was that it went on to bring down a string of multinationals, including FedEx and Mondelēz, which makes every conceivable snack. Anyway, it cost billions of dollars in losses for those companies. As a result, it was very harmful to the countries where the companies were based, and of course it was harmful to the Ukrainians, but it was not an act of war.

In fact, as we speak some of these companies are fighting out the definition of war with their insurers, which are saying, "It was an act of war—we're not paying." The companies are saying, "We had insurance and we are expecting you to pay." These are the real implications of the existence of this aggression, yet we do not have a definition for it and we have not even learned from its use against Ukraine about how we would like to respond to it.

What we can learn from what the Ukrainians have done is, again, to involve the public. The Ukrainians launched an IT army—anybody can join their cyber effort against Russia. I am not sure that we can yet quantify how successful that IT army is, but it is an opportunity for people to contribute to the effort. Most importantly, the Ukrainians—not just the Government but ordinary civilians as well—have launched various organisations in the preparedness and healthcare space so that the population can respond when there is disruption and people are hurt. That maximises the power or reach of the Government—the fact that people are involved and know how to respond.

Q17 **Mr Jones:** You talked earlier about calling it out. Do you think that situations that can be attributed to Russia should be called out early to get the citizens to recognise where they are coming from?

Elisabeth Braw: Yes. One of the differences between the cold war and today is that our adversaries have lost their sense of shame. During the Cold War, the Soviets and other Warsaw pact regimes wanted to be seen as respectable; that is why they signed the Helsinki accords and so forth even though they did not want to. Now they do not mind being seen as rogue, so we have lost the opportunity to call them out—if we call them out, it does not bother them.

Similarly, China does not mind being called out—the regime is not bothered. That is very troubling. I don't have an answer. Grey zone activity is often very difficult to attribute because the perpetrators hide their actions well, but we could accumulate cases in which the perpetrator's identity was not settled beyond reasonable doubt. If we had 10, 50 or 100 such cases, we could then combine them and say that we had an accumulation of cases in which it was likely that Russia or its proxies were the perpetrators. In that way, we would not have the burden of proof when it came to attributing every single incident.

Professor Mumford: I want to double down on the importance of greater levels of attribution and calling it out. That is increasingly important because it is clear that grey zone conflict and hybrid threats are as much a psychological as political or military form of warfare. We have to start nudging the dial on public perceptions of these threats.

You mentioned Ukraine. Of course, when we think about hybrid threats and Ukraine, our minds immediately go back to 2014 and the annexation of Crimea. That was incredibly instructive for framing Euro-Atlantic perceptions of what that was, for two key reasons. First, it demonstrated that hybrid warfare can fundamentally inhibit the decision-making processes of an opponent. Russia's actions in 2014 completely hamstrung the West: effectively, we were unable and unwilling to respond.

The second lesson that Crimea in 2014 taught us is that the ability to undermine an opponent through hybrid means was really an attempt to undermine a legitimate use of force in response. That put the West on the horns of a dilemma, and it did not fundamentally solve the dilemma of what to do. That is exactly why—fast forward to February 2022—many of us, and I include myself, still thought that Russia would not fully embrace the use of conventional land warfare, considering the successes that it had had in 2014 of utilising elements of the hybrid playbook.

When we think about Ukraine today, post February '22, we can see that there is obviously much greater strategic emphasis on conventional warfare. There are still elements of hybrid conflict, too, as Elisabeth has already outlined, but if we are going to learn anything from recent conflicts, we might need to widen the scope away from Russia.

For the evolution of the threat environment, which I was talking about briefly earlier, the two things that have changed are the sources and the methods. They are evolving. To that extent, we really need to keep an eye in particular on China and Iran, in large part because they, unlike Russia, have kept their focus on the ambiguous use of force. They have not necessarily stuck their heads above the parapet in the same way that President Putin has from February 2014 onwards.

Q18 **Mr Jones:** Before we move on to that, may I ask a question about 2014 and Crimea? What the Russians effectively did very quickly is to get out the news narrative in the West that Ukraine was always part of Russia. That was done even with some quite respectable people in this country, regurgitating that nonsense.

Added to that, if you looked at social media feeds at the time, for example—it was very clever—there were Russian soldiers playing football with kids and puppies being handled with care. It was very clever, how they did it. How do you push back quickly on that? For example, with the narrative that Crimea was always part of Russia, the dynamic was very quick, and there was very little pushback quickly from the West in the news media to say, "Wait a minute; these are the facts." How do we respond to that?

There was also the issue that Russian servicemen and women were there

in non-visible uniforms, being nice to puppies and playing football with children—it was a nice, friendly invasion, as opposed to what happened in 2022. That means we have to push back and be prepared to do it very quickly, to stop such a narrative getting embedded, especially in the internet age when it goes around the world very quickly. Even here, some commentators should have known better and read their history books.

Professor Mumford: The use of the so-called "little green men" in Crimea was part and parcel of the strategic masterstroke that the Kremlin devised in order to annexe Ukraine: it was plausibly deniable, in that those men had no insignia or flags on their uniforms. There was a level of plausible deniability, incredulous though people were, and the Kremlin could still hide behind it.

The most important thing, though, was the way in which they very swiftly went about trying to organise a referendum in Crimea. They essentially used—I know we will come on to discuss this later—the West's liberal sense of the importance of democracy against itself.

Q19 **Mr Jones:** But we actually knew the individuals, for example. In Ukraine, the Russians actually invented people, local political figures, and Western intelligence knew all that. We also had the history of Ukraine, so we could have pushed back, but there was no push back very quickly.

We had all the intelligence on individuals in Ukraine who were arguing for being part of Russia. Those individuals were invented; they were funded by Russia. Do we need to be very quick in pushing that back to counter what you have just said?

Professor Mumford: I think it mattered in 2014 more significantly because, unlike now, we were seeing a lot more geographically focused hybrid activity in Russia's near abroad, which is exactly why the Baltic states and Finland got very nervous as well; they also had pockets of Russian-speaking ethnic minority communities close to the border. I think that sort of agitation on the near abroad has moved on since 2014; 2014 was a wake-up call—the West was caught asleep in terms of how to respond effectively to hybrid threats.

Q20 **Mr Jones:** Can we respond now to those types of things in a co-ordinated way—not just one country doing that but the West doing it?

Professor Mumford: We are learning, but there is still a long way to go.

Elisabeth Braw: It is a challenge, because it would need to involve co-ordinated action by Western Governments and news media, and our Governments cannot tell news media or news outlets what to do. Again, one of the vulnerabilities of liberal democracies is that we have, clearly, a division between the Government and civil society, whereas authoritarian countries do not. They can operate in cohesion, whereas we cannot, but I think it would be possible at least to have conversations between our Governments and leaders from news outlets to see what can be done at least to limit the spread of disinformation that reaches our citizens.

Q21 **Mr Jones:** The thing that amazed me about it was that there was no

pushback, including just facts about their "facts"—for example, facts about how, when Ukraine gave up its nuclear weapons, Russia gave guarantees for the sovereignty of Ukraine. None of that was done and then, in various outlets, you have useful idiots that repeat the stuff. In this country, there was no co-ordinated pushback saying, "These are the facts," whether from a Government point of view or even, I have to say, from more inquisitive minds in the media.

It was quite a clearly demonstrated, as you say, playbook that the Russians had put in place; it had been worked out very carefully in advance. Clearly, Western intelligence knew about the individuals who were supposedly Ukrainian "freedom fighters" or wanted Crimea to be part of the former Russian empire as it is. People have to move very quickly, haven't they? I'm not sure: are you saying that we have not even now got that playbook to push back very quickly on these things?

Professor Mumford: A lot of work has been done. We are in a much better place now than we were in 2014. I think what was a game changer was the use of defence intelligence in the run-up to the February 2022 invasion. I think that put the UK Government on the front foot in trying to control the narrative, in trying to cohere those facts about what we knew and what we did not know and to debunk the myths put out by the Kremlin.

Although that was in the context of trying to debunk Russian myths regarding the conventional use of force, it sets a really positive and beneficial precedent for the way in which disinformation, as part of a hybrid campaign, can also be pushed back on in a more effective, high-profile way.

Q22 **Mr Jones:** But is it a cultural issue in our intelligence services and intelligence world that we do not put in the public domain things that we should in order to push back? As you say, we did in terms of the invasion of Ukraine, but do you think that the reticence to put some of that information in the public domain is hampering us rather than helping us?

Professor Mumford: If it means effectively wresting better control of the strategic communication of what these conflicts are about—hybrid threats are ubiquitous, but I don't think we have decent enough control of the narrative about why they matter to the general public, as Elisabeth mentioned. Obviously, there would be some pushback against opening up. The decision to make a lot of the defence intelligence open in the run-up to the Russian invasion of Ukraine was very controversial. We of course have to be mindful of the lessons of publicising intelligence and declassifying intelligence very quickly to make political gains. We need to be conscious of the lessons of Iraq here, but we also need to realise that there are very large gaps in the way in which we are persuading the British public and the general public in the West as to the danger of hybrid threats and what we can do about them.

Elisabeth Braw: Can I add one more point? The UK's response to the Salisbury poisoning was extremely good. It was a co-ordinated Government action that meant Russia ended up looking very silly, and

those two intelligence officers were ridiculed around the world. On top of that, from what we know in the public domain, the UK cut off Russian access to certain financial holdings here in the UK. It was very well executed, it was swift and, at least from what we know in the public domain, it was the UK Government just acting at impressive speed and thinking innovatively. That is a good lesson for the future.

Q23 **Mr Jones:** So we can do it; that is what you are saying.

Elisabeth Braw: Yes, we can, but interestingly, in this case, it involved not just the Government but the private sector through the financial sector and various news outlets. We still do not know exactly how close the collaboration was between the Government and the news outlets that then investigated the two intelligence officers, but the result was that the investigations happened very quickly. We got these revelations about who the intelligence officers were—who the perpetrators were—and in the end, the Russian intelligence apparatus ended up looking very silly.

Q24 **Derek Twigg:** I want to switch back to something we discussed with John Spellar before and the issue around whether it is more challenging for liberal democracies than for the Chinas and Russias of this world—in other words, autocratic societies. Is it the case that we will always be on the back foot and not on the offensive as liberal democracies? Going back to the moral question about what the limits of what we should be doing are, given what they do to us, are there any advantages to being a liberal democracy in this field? Are all the cards with the autocratic states? Should we go on the offensive more than we are now and is that morally okay?

Elisabeth Braw: That is an excellent question. We are at a disadvantage because we profess to believe in—

Q25 **Derek Twigg:** Will we always be at a disadvantage, do you think?

Elisabeth Braw: Yes, we will, because they can use means that are illegal and unethical, and we should not use such means. It does not behove a liberal democracy to engage in such activities. That also means that we cannot signal, if we are talking about deterrence, to our would-be attackers that, "If you attack, we will retaliate", simply because they know that we will not retaliate because we will not use similar illegal or unethical means. So we cannot signal, "If you blow up our energy infrastructure, we will blow up yours." That is a disadvantage.

On the other hand, what we can signal is that we are resilient. We can signal that their efforts will not be worth their while. That is a weaker form of deterrence—deterrence by denial—in suggesting, "Don't try it because it's not going to be particularly effective." But we can do that and that is why, I think, the public—

Q26 **Derek Twigg:** I know it is going to be a state decision and not for your or my individual view, but we bombed German cities during World War Two and they bombed our cities. What is the moral case against bombing or destroying a power station, say, in an adversary state if they do the same

to us?

Elisabeth Braw: We could, but that would then escalate and that gives them the opportunity to say, "Well, we will do even more because you did this to us." Yes, we could. I do not think anybody would begrudge us the opportunity or the necessity to retaliate in kind, but then, where does that lead?

Another disadvantage that we have is that so many aspects of our societies are connected to the countries that are now trying to harm us. If, for example, we were to retaliate against a country that had harmed our energy infrastructure, that country—say, Russia or China—could then harm one of our companies operating there in response. That is what makes it so different from the Cold War. Essentially, our private sector is operating behind the frontline and is incredibly exposed, yet we need to those companies to be reasonably safe where they are, otherwise our economies would be in trouble.

One of the advantages we have as liberal democracies is that we are attractive places to live. Our citizens like living here, even though they often complain about it. If they were to face the choice of living here or there, virtually everybody would want to live here. Indeed, citizens of the countries that wish us ill want to live here too. That is something we can use to our advantage and should have used long ago.

In other words, we could signal that we would cancel visas of family members of leading politicians in Russia and China. When Russia invaded Ukraine, we obviously cancelled quite a few visas. We could have done that earlier or signalled earlier that, "If you, Russia, engage in grey zone aggression against us, we will cancel the visa of one of your citizens, and we will decide who that will be. It could be the son or daughter of one of your top officials," because it is not a human right to get a visa to the UK. It is within the gift of the UK, so it would not be escalatory either. That ship has now sailed with regard to Russia, but it would still work with China and other countries that may decide to use grey zone aggression against us.

Professor Mumford: Hybrid threats pose a massive challenge to liberal democracies, in large part because liberal democracies are forced to try to find an appropriate balance between combating these grey zone threats on the one hand and protecting our own values system on the other. This is absolutely intrinsic, because for these hostile states in the international system that are using grey zone threats against us, it is not just about territory, as we saw with Crimea in 2014. It is about norms, about destabilising our values and institutions, and about the sanctity of our elections and the rule of law. That is why the use of hybrid threats in the grey zone appeals to illiberal states.

It appeals to them first because it allows them to make strengths of weaknesses. Where these states have, for example, poor conventional military capacity or weak economies, they are able to circumvent the restrictions that that might place on their conventional use of force.

Instead, they are able to create surprise out of it or deniability. That in part means that we can think about challenges to the West and the UK in the grey zone as being as much about what we stand for and what we do as about the sanctity of our alliance or the territory of our allies in the international system.

I spoke earlier about the horns of a dilemma. This is where it really does not pay to be a liberal democracy, because this is the exact reason why states like Russia, China and Iran use hybrid threats in the grey zone against us. What it does is fundamentally put us on horns of a dilemma. Overreaction makes us look like the bad guys and like we have acted pre-emptively.

Q27 **Derek Twigg:** If they destabilised a power station in this country, how would it be an overreaction to destabilise a power station in their country? I know I am talking simplistically here, but why would that be an overreaction?

Professor Mumford: A lot of hybrid threats exist under the threshold of legitimate response. Undertaking a cyber-attack against a power station is one thing. Let's not kid ourselves: we are trying to destabilise the cyber capabilities of our competitors in the international system already. We are doing it. Take Salisbury as an example: tit for tat responses can create unnecessary vertical escalation. I think we need to think smarter about the way in which we respond, and we really need to strengthen and be more proactive in deterring these threats. I know we are going to talk about deterrents in greater detail later on, but I think that more proactive deterrents—denying our competitors not just the capability to undertake hybrid threats and hybrid attacks against us, but the outcomes that they want from all of this—are hugely important.

We have to be careful, however, because if they undertake a hybrid attack on a power station, for example, to use your words, and there is this veil of ambiguity around who is responsible, because attribution is not an exact science when it comes to these sorts of things, especially in the cyber realm, and we overreact, we could look like the aggressor if we respond in kind. But the danger on the flip side is—we perhaps saw this in Crimea in 2014—that the lack of a response leaves us open to death by a thousand cuts. That is the real dilemma. This is the reason why these hostile states are deliberately using this form of conflict against us, because it forces us to think twice about how we react. It is very, very difficult—it's a balancing act that we've not got quite right yet. So that is why using it against liberal states holds a fundamental appeal to illiberal states.

The question for us, for the UK and its allies in the West, is whether to actively change the status quo on our own terms. Should we change the nature of the debate about deterrents and about hybrid threats, and get out on the front foot about communicating the threats that these have?

An analogy that I keep thinking about a lot is that at the height of the troubles in Northern Ireland, Reginald Maudling, the Home Secretary,

famously talked about finding what he called "an acceptable level of violence" where the British public would think, on opening their morning newspaper, "Oh, another bomb attack—how many soldiers dead? How many civilians dead?" It was quite callous and controversial at the time, but he talked about finding an acceptable level of violence in Northern Ireland.

That phrase is really applicable when we start to think about hybrid threats. What is an acceptable level of hybrid threat for the UK to soak up? How many cyber-attacks against our critical national infrastructure are we willing to soak up without singing from the rooftops about them with our defence intelligence? This is the horns of the dilemma that I talked about earlier, and I think we really need to get out on the front foot on that more.

Because before we know it, that death by a thousand cuts might have occurred too late for us to do anything about it, because important elements—including public trust in our democracies and in the mainstream media—will have been eroded beyond repair, because of the constant stream of disinformation or constant attempts to interfere in electoral processes. So what is at stake is the sanctity of those norms and ideals that we find important in the West that are appealing, and I think we, the Euro-Atlantic community, need to more aggressively defend the soft power appeals of liberal democracy.

Q28 **Mrs Lewell-Buck:** Professor Mumford, you said we need to get out on the front foot. In this session, I am struggling with what the grey zone actually is, so how would you get out on the front foot with the general public, who are not interested like we are in this Committee? I am struggling with what that would look like practically.

Professor Mumford: It is true: grey zone threats are omnipresent, but they are intangible. Trying to deter them is the strategic equivalent of trying to catch fog. However, there are practical examples in the day-to-day existence of all of us, all civilians, that apply—whether it is the security of our data on NHS databases that could be hacked, the importance of the security of our electricity substations, or something more intrinsic about our electoral systems. The threat environment at this stage in the 21st century is changing substantially. The whole purpose of trying to exploit the weaknesses of liberal democracies is precisely because it is about norms and those values that all our citizens participate in or would hold dear, as Elisabeth referred to, but also realising that hybrid threats affect all of us, whether it is the ability to use our mobile phone or to access our bank accounts. All these could come about as a result of a hybrid attack by a hostile state.

In trying to change the level of public debate, public diplomacy and strategic communications are part and parcel of increasing public awareness of and approaches to hybrid threats. The problem is that two of the biggest problems in trying to do that and changing that debate among the public are public levels of trust in Government, which is key, and levels of public media literacy. There was a really important study done by the

joint EU-NATO Centre of Excellence for Countering Hybrid Threats in Helsinki a couple of years ago that looked at how those two things—public trust in Government and levels of media literacy among the public—were two of the biggest things that contributed towards levels of societal resilience in the Finnish public.

First, from a UK perspective, what concerns me is that we are now at a point where the majority of British citizens do not get their news from mainstream media outlets; they get it from social media. That worries me, because of the massive open goal you have for high levels of disinformation coming through those channels. Secondly, public opinion polls show a decreasing level of public trust in Government and our national institutions, which is also a problem.

Elisabeth Braw: I can add to that. It is helpful to have a designated person in the Government who communicates with the public about the threats. Essentially, they become a one-person institution, because there is no institution in charge of grey zone defence.

A good example of what can be done is Sweden's new Minister for Civil Defence. It is a new position. He is the No. 2 in the Swedish MoD, and he is in charge of all non-kinetic matters. He is extremely good at communicating with the public on social media and elsewhere, in newspaper interviews and so forth, about various threats, so they know that if something comes up, he will communicate it to them. It is extremely effective and it is inexpensive too—in fact, it is free—because he just communicates whatever comes up and whatever is new. The fact that he has this portfolio is also really helpful.

At the moment, I do not think that any country has figured out what a Government agency or Department should look like to cover all kinds of grey zone aggression, but if you at least have a Minister in charge of it, that is a good start. In general, straightforward communication with the public can happen without any sort of institutional reforms, as long as there is a credible person in the post. We have lots of credible people in UK politics, so I am sure that that would not be a problem.

Mrs Lewell-Buck: I will leave that one there then. That could be a whole other debate, Elisabeth.

Chair: Talking of which, we have covered a lot of ground, but there is a lot to get through, so we all need to try to be a bit sharper in our questions.

Q29 **Sarah Atherton:** The UK is the third most targeted country in the world for cyber-attacks. Just over 24 hours ago, we saw a member of staff here charged under the Official Secrets Act for spying for China. Without repeating what has already been said, is the UK prepared?

Elisabeth Braw: I do not think that the public quite understands the threat that exists and that various parts of the Government fight off on a daily basis, whether it be cyber or otherwise. You could say, "Well, there's no point frightening the public. It would cause them to panic, and why

would they need to know?" Actually, I think it would be useful to know because, first, they would realise what level of effort and expertise already goes into defence against grey zone aggression, and also just how perilous our way of life is, and we want to have this way of life. In terms of having that straightforward communication with the public, I am not saying the member of parliamentary staff who has been charged with spying for China would have acted differently if he had realised just how high the stakes are, but plenty of people would be less careless when it comes to their daily life, and indeed down to the very basic level of what they share on social media, if they knew the cumulative effect that these forms of aggression have against our societies.

Q30 **Sarah Atherton:** You mentioned the Salisbury poisonings before. The UK was quite robust in its response around sanctions and expulsions. That obviously acted as a deterrent, which is good, and a punishment; that is what happens—you mentioned this before—if you do that in this country, and those are the effects. Do you think it built in resilience, though, to ensure that a similar or alternative attack would not happen again? Did we learn from it?

Elisabeth Braw: The public were never involved in the Salisbury response. I guess one could argue, "Why would the public need to be involved?" but if you imagine a similar incident that may happen in the future, it may affect more people. You would need people in the town affected to know how to respond if they see people who are clearly affected by some form of aggression, whether it be poison or otherwise. I would love to see some kind of organisation in the UK that people could join so that they know what to do in a crisis, whether that be flooding, poisoning, or power or internet outage. They could be the local first responders, below the gold, silver, bronze that we have within our institutions. If we had that, those institutions would also know that there are trained people in every part of the country, in every town and city, who know what to do and who can be called up if some sort of larger response is needed. If you look at, again, the NHS, people are willing to get involved, and in this country lots of people volunteer. Why can't they volunteer for something that I think we all agree is the most important aspect of life in this country, which is keeping the country safe?

Q31 **Sarah Atherton:** Andrew, if we look at disinformation and particularly the use of AI—you have mentioned electoral interference a couple of times—do you have any concerns as we head towards a general election?

Professor Mumford: Not as much as if I were an American citizen, largely because I believe in the sanctity of a pencil and a piece of paper, which are very hard to interfere with, and long may that continue. However, the bigger concern is the levels of disinformation that will do the rounds on social media in the run-up to a general election. That is where the public messaging, the public diplomacy and the fact-checking of claims and counter-claims will be really important.

On the bigger question about wider preparation, the weakest link in all this is cross-Government co-ordination, and that is the key. I do not think

Government machinery right now is fully equipped to deal with the threats that span both the military and civilian divide and the domestic and overseas boundaries spanned by hybrid threats in the grey zone. To give you an example, grey zone activity in the cyber domain, for example, falls under the remit of the National Cyber Security Centre and GCHQ, while national crises responses that may be manifested through cyber activity fall to the Home Office. The MoD is responsible for cyber-warfighting. An overall strategy for cyber falls elsewhere. The same is true for counter-disinformation. You have disparate groups inside the FCDO trying to counter disinformation coming from specific countries. You have the Cabinet Office doing the same. You have the MoD, through 77 Brigade, trying to do it from a military perspective as well. So there is a real dissipation of responsibility at the moment, and that is the problem.

I do not have a silver-bullet solution. We are seeing and observing this level of cross-Government dissipation of responsibilities for various things, and I agree with Elisabeth that we need to see greater levels of co-ordination. That is probably why the National Security Council is going to have to play a greater role in co-ordinating UK responses to hybrid threats. These threats span both geography, and the Foreign Office might traditionally have taken a lead on Russian, Chinese or Iranian activity, and theme—disinformation and cyber. Ensuring that there are units or agencies across Government that have responsibility for trying to co-ordinate, or cohere greater levels of co-ordination, is massively important.

Q32 **Sarah Atherton:** Our military is running hot: it has lots of demands on it, and it is spread quite thinly. What role should it play? You have touched on 77 Brigade, and there is also Army special ops and Space Command, for example. What role should it play? Should it play a greater role? Should it be the risk manager of last resort? Or is it in the right place and doing the right thing at the moment?

Professor Mumford: It is important to remember that grey zone threats are a whole-of-society problem. They are not just an MoD or even a Government problem; they are a whole-of-society problem. I was really pleased to read in the integrated review that a cross-Government approach to countering state threats is hugely important, and I completely agree with that. Defence has to be at the forefront of co-ordinating that effort.

But here's the rub: it has to facilitate the co-ordination of these efforts, but I do not necessarily think that Defence or the military itself can take an obvious lead. The reason I think that is that it is hard to justify a strong Defence effort in co-ordinating non-warlike scenarios. This comes back to what I was talking to Mr Twigg about: the sub-threshold dilemma. The military steps in when things breach a threshold, but because so much of the threat is now manifest at sub-threshold level, it becomes very difficult to ask the military to do an increasing amount of things at the sub-threshold level.

This is where stronger communication with the public comes in again. That would help to contextualise domestic threats within an international threat

environment. Defence has to take a lead in co-ordinating, but it cannot be seen to be leading.

Q33 **Sarah Atherton:** To go back to Emma's point, you have sub-threshold and threshold. Where is the line? No one seems to know where that line is, and I think that is the dilemma.

Elisabeth Braw: There is no line. We have to tolerate a certain amount of unethical and illegal behaviour. We cannot respond to everything, but we need a threshold below the traditional military threshold, above which we communicate that we will retaliate—we have to figure out what the retaliation would be—and will not tolerate that activity.

I think that we just have to accept that a certain amount of cyber-aggression is inescapable, as is a certain amount of maritime violation and harassment, and so forth. What is the level above which it is no longer tolerable from our perspective? I have thought about this for years. What is the level? Is it when one person loses their life? Is it above a certain amount of money lost? Is it above a certain number of occurrences of a particular form of aggression? Whatever it is, that level needs to be defined.

I will just add one more thing to your point about disinformation. London is extremely vulnerable to disinformation as a financial centre. Look at how quickly traders react to bad news, or any sort of news, about companies. This is an area that countries wishing us ill can exploit by essentially feeding bad news about particular companies into the public domain. Then, traders will respond quickly, and those companies, or indeed the London stock exchange or FTSE 100, will plummet. Of course, they will recover quickly when people realise it was based on false information, but it nevertheless destabilises the whole financial system or the whole UK plc. I think that makes it even more important to have regular conversations between business leaders and senior Government officials about the threats they are seeing.

Q34 **Richard Drax:** I think you have answered part of this question already, but what does UK defence do well in the grey zone? What should it do more of, start doing or cease doing? Perhaps you would like to start, Elisabeth.

Elisabeth Braw: What the UK MoD does well is step in when nobody else feels that it is their job to step in. We have seen that across every kind of contingency, including covid. In essence, the UK MoD or the UK armed forces are so good at their job that we have come to depend on them for every kind of contingency—even to the point where we expected the Army to transport oxygen and even to stack supermarket shelves during covid. Credit to the UK armed forces for being so good that people expect them to solve every issue, but clearly they are not large or numerous enough for that to happen. What they do well is respond to crises of every kind, including non-military crises, such as flooding, covid and so forth.

However, the question for me is, why do they need to do that? Couldn't we free up those resources so that the armed forces could focus on the

things that only they can do? If others with more rudimentary or other skills could look after those tasks, the armed forces would not need to. The question, then, is who should it be? It could be, for example, a volunteer organisation attached to the MoD of the kind that Sweden has with the home guard. That would still give the MoD the opportunity to co-ordinate and to make sure that things are done properly, but you would not have to have soldiers doing tasks that others could equally do.

Professor Mumford: Briefly, I think the MoD needs to do three things. First, it needs to build a greater awareness of grey zone threats, especially with regard to the way in which it communicates those to the public. Secondly, it needs to develop the UK's capacity to deter them. I think this is an important moment: I believe I am right in saying that there is some big package of work going on inside the MoD at the moment to look at the UK's deterrence strategy, so this is an important moment right now to start factoring lots of discussions about deterrence of hybrid threats into those plans. Thirdly, the MoD needs to enhance the UK's engagement with allies in order to strengthen resilience to hybrid threats.

Forgive me for my historical analogies—I've already quoted Reggie Maudling and I am going to quote Denis Healey now, for purposes of political balance. I am sure some of you around this table will be familiar with the Healey theorem, which Denis Healey named after himself. In that theorem, he was talking about deterrence in the Cold War. He said it takes only 5% credibility to deter a Russian attack, but it takes 95% credibility to reassure the Europeans—he was talking about whether the Americans would use their nuclear weapons. I think Denis Healey had it spot on at the height of the Cold War, and I think the Healey theorem still applies to a large degree today.

The reassurance of our allies with regard to the credibility of our deterrence, and our willingness to use proactive deterrence threats against hostile states, are hugely important if we are to strengthen our resilience. Sarah mentioned resilience earlier, and it is the bedrock of every deterrence policy, but too much emphasis on resilience means we soak up too much. If we do not start proactively deterring, we find our acceptable level of violence getting higher and higher because we decide that we are resilient and we can soak things up. That could be a bit dangerous, in terms of providing more of a slippery slope. Those are the three things, to answer your question, that I think the MoD needs to do in this space.

Q35 **Richard Drax:** You sort of touched on part two of my question, about whether the UK is being sufficiently proactive both here and abroad in countering disinformation and hostile action. I think what you were saying in that answer is that there is a lot more that needs doing. The answer to the question is that we are not doing it and we need to do an awful lot more, but I think you are saying that the MoD is looking at doing an awful lot more.

Professor Mumford: It is looking at deterrence in the round. Of course, our understanding of deterrence stems from traditional nuclear state-based threats. If we are to deter hybrid threats in the grey zone

effectively, the UK needs to move beyond a nuclear-centric interpretation of what deterrence is and what deterrence looks like. We are not here claiming that Russia is imminently about to use a nuclear weapon against the UK or its allies, but we are here saying that Russia, China, Iran and other hostile states in the international system are finding ambiguous but effective ways to undermine us, which tackle our norms and our values. It is not just all about territory. Conceptions of deterrence need to evolve and move on, and fully embrace hybrid threats.

Q36 **Richard Drax:** As far as grey zone threats from abroad are concerned, I think you both said that much closer co-ordination with our allies is needed to define what we do. I asked Elisabeth in my first question to decide how you counter increasingly aggressive grey zone threats.

Elisabeth Braw: This is where it is really useful to have allies. That is one of the strengths of being a liberal democracy; we have friends and allies, while our adversaries only have occasional partners. If the UK were to be targeted by a particularly blatant act of grey zone aggression, it should be possible for the UK's allies to respond on its behalf—for example, by revoking visas, freezing funds or whatever that country may have at its disposable. It should be able to do that in solidarity with the UK, just as the UK could similarly support that country or come to its aid if it were targeted in the grey zone.

When it comes to your previous question about countering disinformation, it cannot just be the MoD, so then the question is, who in addition should it be? The second part of that is that we have across the Western world developed quite an impressive awareness of disinformation since it burst on to the scene in around 2014. It has taken a similar trajectory to dirty men on the internet, in that kids know that they should be aware when they use the internet. However, the better we get at defence against a particular form of grey zone aggression, the more attractive it becomes for that country to then switch to a different form of grey zone aggression. That is, again, part of the defender's dilemma: the better we get at defence, the more likely they are to move on to a new and more productive form of aggression.

Chair: I will come to Emma next, and then I will come straight to Derek.

Q37 **Mrs Lewell-Buck:** Just thinking about those points on capacity to deter and on countering disinformation, we know from our previous inquiries that at the MoD and in fact across Government they are struggling to recruit and retain people who have skills in cyber, artificial intelligence and engineering. Is the answer our reservists? Is it the private sector? What is it? How do we solve that problem?

Elisabeth Braw: I will give you my idea of what I think should happen, even though it is unlikely. We should look at Norway's system of military service, which they have perfected since the end of the Cold War, when they turned lemons into lemonade. They had military service for all men, and when the Cold War ended they didn't need as many conscripts any more, so they reduced the number to a third and it became competitive to

be selected for military service. In 2016, they decided to include women, so then it was down to about one sixth of all 18-year-olds being selected for military service, so it became extremely attractive. It is like being admitted to Oxbridge.

The UK does not need conscription for all men, let alone for all men and women, but it could adopt and adapt this competitive, selective Norwegian model and use it not just for the armed forces but for different parts of the Government that play a role in national security. Then you would have that reserve of young people, and then people of all ages, with the skills you need in a crisis. When you are standing reserve, you would be available to be called up in case of a crisis.

Q38 **Mrs Lewell-Buck:** I imagine that in the Norwegian model they are paid very well.

Elisabeth Braw: They get a stipend. It is definitely not a lucrative thing to do, but it is prestigious and that is what matters—you have it on your CV. It almost does not matter what you did as part of your military service; what matters is that you were selected. It is the perfect social leveller. If you have the aptitude and talent, you have the chance of being selected; it does not matter where you went to school. I think the UK could do the same across various parts of the Government, including the MoD, GCHQ and the NHS—the crucial parts that have some responsibility for national security. If young people are selected for that programme, you would not only have this standing force of people who were available to be called up in a crisis, but you would establish a link between national security and the wider population, and you would make it incredibly attractive to be part of that effort.

Professor Mumford: I think co-ordination with the private sector is absolutely crucial, particularly with parts of UK plc that deal closely with China. We need to understand that hybrid threats to the UK are a threat not just to UK national security but to the UK's growth strategy and UK prosperity in an economic sense, because cyber-attacks cost significant amounts of money. It is not just the private sector; the public sector is suffering massively as well. The levels of intellectual property theft from UK higher education institutions are massive, so universities are losing out as a result of cyber-attacks. We have recently seen ransomware attacks in the university sector. There has to be greater liaison with the private sector and elements of the public sector too.

Yes, greater levels of reservists would be a fantastic force multiplier, but we have to realise that the private sector has capabilities that the UK military does not have, so working closely with the private sector will be a really important force multiplier too. The private sector operates or owns large amounts of the UK's critical national infrastructure, so it needs to be brought into the conversation. The way in which individuals—the likes of Elon Musk—now have the capability to fundamentally shape battlefields, based on whether they give access to satellites, is a manifestation of how important the private sector and private individuals are to the landscape of hybrid threats. That is hugely important, and I would say that it is not just

the private sector but the public sector too. You can tell it is an election year when there are lots of discussions about conscription going around.

Elisabeth Braw: To add to that, the UK Government deserves credit for its efforts so far to involve the private sector, both through the civil reserve initiative and the work that is under way and is being tested to create a dialogue, or continuing exchange of information, between business leaders and the Government.

Q39 **Derek Twigg:** We have talked a lot about who takes the lead and who has responsibility, and about making sure all parts of Government are involved in it. What role do you think that defence should have in protecting critical national infrastructure? Clearly, we do not have an air defence system, and clearly any attacks from missiles or drones would be a challenge for us, so to protect critical infrastructure in this country, what role do you think that defence should have or that you would like to see it have?

Elisabeth Braw: Clearly, it should be co-ordinated by the Ministry of Defence, but it could involve ordinary citizens. Bearing in mind that the armed forces cannot be everywhere all the time, there is a role for citizens. They know their area better than anyone else and can tell if something is out of the ordinary. Essentially, it is "See it. Say it. Sorted" translated from terrorism to national security. But someone would need to co-ordinate; it cannot just be a phone number that people can call. If implemented, people would have a way of playing a role and reporting whatever they saw that looked out of the ordinary. Cyber is obviously a little different—we cannot just involve citizens in cyber-protection, but physical protection, yes.

There is a good example. If you remember the "whiskey on the rocks" incident in 1981, the Soviet submarine was discovered by two fishermen who were out at 4 am. They thought—as all good citizens would—that it did not look right and should be reported, so they called the navy and the navy sailed out. What if they had not been there, or if they had said, "Well, it's not my responsibility; it's the Government's responsibility"? Most citizens would do the right thing if they had a way to do so, if there were an organisation or a system for them to operate in.

Derek Twigg: Almost a citizens' army—rather than just being vigilant, being organised; being organised to be vigilant—

Elisabeth Braw: Exactly. Also, to be trained in what to look for. I might think that something looks out of the ordinary, but it might just be maintenance happening or something like that. This, by the way, involves the maritime sector and merchant mariners, too. If they see something that does not look right near energy or sea-based installations, such a system would allow them to have an easy way to report it. Obviously, they try to report as much as they can already, but if that were to be institutionalised and we made it as easy as possible, people would want to participate.

Professor Mumford: A focus on critical national infrastructure underlines the emphasis that needs to be placed on cross-Government co-ordination, because of the way in which that brings in health, energy, transport, supply chains. A response would therefore have the MoD needing to liaise and co-ordinate with the Department for Energy Security and Net Zero, the UK Health Security Agency, the Department for Science, Innovation and Technology—that is a really good example—

Derek Twigg: And the Department for Transport.

Professor Mumford: Absolutely. The current war in Ukraine has demonstrated just how and why critical national infrastructure is massively important, or given the ways in which undersea cables carrying internet communications have been targeted. CNI is now a huge target. The cyber-security of installations—you mentioned power stations earlier as a prime example—and of our critical national infrastructure is manifest. Things have helped—the removal of Huawei from the 5G network was a very sensible start—but that is the epitome of the need for greater levels of co-ordination.

Q40 **Chair:** Thank you for your answers so far. Our final theme in the last few minutes is about our allies and friends. You have mentioned a few countries, but as we look at this and at other benchmarks, who is particularly good at operating in the grey zone? Where should we look at for various examples of best practice that can be applied to the UK?

Elisabeth Braw: I can start. One very practical example is what the Czech Ministry of Defence does with its grey zone exercises. The armed forces conduct those with the private sector, and they take turns so that it is industry or sector specific. That is something that they implemented very quickly—within months—after deciding to do it. They thought, at first, "Oh, maybe companies won't be interested," but it turned out that the companies were very interested, so they then had to be selective. That shows, again, how concerned the business community is about grey zone aggression. And, by the way, it is also fantastic to be able to demonstrate that to our adversaries: "If you try to target our companies, they are already prepared, and we are working with them." Another good example is of course the Norwegian model of military service.

Then, the third area is public education, and there we have different allies who do good things. Singapore has an annual defence day, where all the citizens are reminded of the threats facing the country and their role in keeping the country safe. Similarly, in Sweden, there is a total defence week, and now there are total defence exercises that have been resurrected after the end of the Cold War, which involve Government agencies across the board, the private sector and civic organisations.

An example from Finland is their disinformation curriculum in primary schools. I think that that will become standard across the board, but it does leave the question of, "What about those of us who are more than 11 years old? How are we going to learn how to identify disinformation?" But that may be for another ally to figure out.

Those are the examples that I would highlight. Maybe one last one is the role of the home guard in the Scandinavian countries. We do not have a home guard here, so it cannot be adopted as is, but it does demonstrate that it is possible to involve ordinary citizens in the Ministry of Defence, not in a full-time kinetic capacity, but in a protective capacity with a specific task of looking after the homeland, and reporting to the Ministry of Defence but not being part of the professional armed forces structure.

Professor Mumford: I would advocate the Dutch model. A couple of years ago, the Dutch Ministry of Defence established its own "countering hybrid threats" unit, which sat within its MoD. In November 2023, that unit led a cross-government exercise in creating a response framework, which brought into the conversation all those different Government Departments that we think need to be in on this.

What is really interesting about the Dutch example is that they work very closely with non-governmental partners as well. They brought in academics and think-tank experts to really thrash out in detail some of these problems—the problems of the threats—and some potential responses. They created this matrix of response, which required input from every Department in the Netherlands, that tried to sort of play out potential scenarios and game particular cross-governmental responses, and it started a conversation.

Interestingly, from conversations that I have had with members of that "countering hybrid threats" unit in the Netherlands, they were very conscious that Defence could not be seen to be leading on that. The phrase used to describe the way in which the unit did that was that the Ministry of Defence offered leadership from behind. I thought that that was a really interesting phrase, and when I asked for greater clarification as to what that meant, it was an understanding that, in other words, they had to provide the thought leadership on the problem, and they had to share the resources that they had with other Departments, but they could not be seen to be dominating the co-ordination of those efforts, because that would be off-putting, given inevitable cross-governmental silos.

I would also recommend that Members read the 2020 deterrence playbook, if you have not done so already, which was published by the joint EU-NATO Centre of Excellence for Countering Hybrid Threats. I think that was a real landmark publication in terms of framing the debate about deterrence.

My final thought to leave you with is that right now the perceived benefit of using hybrid threats massively outweighs the cost of such action. Hybrid threats against the UK and its allies have become habitual. We need to break that cycle. We need to adopt a more proactive level of deterrence against these threats.

Q41 **John Spellar:** You cited very respectable and efficient western European democracies. Shouldn't we also be learning from the Russians and the Chinese? They are experts at this and they are still, in spite of the changes, basically Soviet Administrations. China still talks about the

leading role of the Party along with Xi Jinping's role. They therefore have an integrated political aspect to all this work. Politics ultimately decides, and politics finds the weak spots and creates the line and works out how to deconstruct our societies.

What frustrates me is that we and the Americans did that in the 1950s and '60s. You mentioned Denis Healey. He was very prominent in the Information Research Department out of the Foreign Office, which was absolutely part of that political warfare. The United States employed a previous head of the American Communist party to fight the battles in the trade unions in Europe.

The military do a terrific job, but almost by definition, they are not politicians. The political aspect of this—for the Soviets, politics is at the heart of everything. If we are going to counter them and play defence, and also take the battle to them, do we not have to create a political environment? There is also a need for those who can draw up propaganda. The Political Warfare Executive had tabloid journalists and so on.

Don't we need to be evolving to that, rather than doing better what we have been doing up until now?

Professor Mumford: Fighting fire with fire in such a way would be dangerous.

John Spellar: We did.

Professor Mumford: We did, and to the detriment of the West, which is why the West—the UK, the US—is hated in some parts of the world: because of our association with those actions. I agree with you that we need to learn from Russia and China, but we need to learn from them because we need to get into their mindset. We need to understand what makes them tick and what makes them act in the way they do, and what it is that they want to exploit.

It is one thing to enhance our deterrence. It is another thing altogether to ape their actions.

I think that trying to significantly enhance our deterrence horizontally—it is not just about the danger of escalating vertically. I don't think we should be necessarily averse to escalating horizontally and embracing unconventional ways in which to undermine hostile states as well.

Q42 **John Spellar:** But didn't we do that, for example, in Poland, which helped, basically, to break up the Warsaw pact and the Soviet empire? Solidarity as a movement had very considerable support from Western agencies and from Western trade unionists and other bodies, in order to capitalise on that deep disaffection in Poland. That helped to bring down the Administration in Poland and basically cracked open the Warsaw pact.

Elisabeth Braw: One of the challenges is that by comparison our adversaries are much more closed than our adversaries were during the Cold War. It is so hard to communicate with or to reach citizens in China, and even in Russia, whereas in the Cold War we had Radio Free Europe

and BBC World Service for that matter, through which people were able to learn about life in the West and decide that it seemed quite attractive.

I agree with the point that there are possibly legal and ethical ways in which we can hit back. For example, one way here in the UK would be to publicise every now and then the holdings of various key officials and their family members here in the UK. That is not classified information and it is something that anybody can find if they go and look for it. It would embarrass those leaders to be found having significant attachment, themselves or through their family, to a country that they are officially trying to harm.

Chair: On that note, thank you both very much indeed. It has been a good session. We have covered a lot of ground. We appreciate it—thank you for your time.