HOUSE OF COMMONS

Defence Committee

Oral evidence: Defence in the Grey Zone - 13 05 24, HC 50

Monday 13 May 2024

Ordered by the House of Commons to be published on 13 May 2024.

Watch the meeting

Members present: Sir Jeremy Quin (Chair); Sarah Atherton; Richard Drax; Mark Francois; Kevan Jones; Mrs Emma Lewell-Buck; Jesse Norman; John Spellar; Derek Twigg.

Questions 43-56

Witness

I: James Appathurai, Deputy Assistant Secretary General for Innovation, Hybrid and Cyber, NATO.

Examination of Witness

Witness: James Appathurai.

Q43 **Chair:** It is a pleasure to welcome everyone to the second session of the Select Committee's investigation of defence in the grey zone. We are turning to a discussion from the NATO perspective. It is a great pleasure to be joined by James Appathurai—very good to see you, sir. Will you introduce yourself and your role, before we fire into questions?

James Appathurai: Thank you. My name is James Appathurai. I am the Deputy Assistant Secretary General for Innovation, Hybrid and Cyber. Hybrid is our word for grey zone, the below-threshold ongoing activities that we are going to be discussing now. My division is also responsible for protection of critical undersea infrastructure, energy security, and the security implications of climate change. And I know I sound American, but I am Canadian. That is the general introduction.

Q44 **Chair:** Thank you very much for joining us. By the sound of it, your division has got its hands full. There are many areas to cover. I think I am right in saying—I think you mentioned it—that you changed the name of the division from Emerging Security Challenges specifically to mention hybrid. I assume that reflects a growing concern regarding the nature of the hybrid threat, and I wondered whether you could talk us through how that has changed and how it manifests itself to NATO member states.

James Appathurai: You are absolutely right. We did change the name. Basically, we had come to the realisation that these were not emerging security challenges; they had emerged. It was important to see them not as some sort of potential future problem, but that we are in a constantly contested security space and that it is contested across the spectrum. What is important to note now and what you, I think, are correctly focusing on—that is why I welcome this discussion and your focus—is what we believe, which is that the hybrid threat is not only substantial, but more sustained and growing on a regular basis. Frankly, I worry a little that we are not tracking the trends well enough—I am a bit concerned about the boiling frog problem, that we are looking at the levels, which are growing and growing, and we are getting used to what we would have never been used to before.

What do we see? We see increasing political interference, disinformation, cyber-attacks and not just threats to, but attacks on, critical infrastructure. That includes cyber-attacks, ransomware—which is used as cover for implantation of malware into industrial control systems—attacks on energy infrastructure more broadly, and energy used as a weapon. The Russians have obviously been doing that as a form of coercion. Now we see new elements, such as forced migration, which we have seen over the past couple of years, and now there have been clear warnings from our military and intelligence chiefs in public about increasing risks, and acts, of sabotage on our own territory, and assassinations on our own territory. The UK, of course, has been subject to both of those.

These come principally from Russia and China. We see different kinds of hybrid or grey zone pressure being put on by those two separate actors, but in some cases they are related and mutually reinforcing. That is in particular the case when it comes to disinformation, where China is amplifying Russian disinformation on NATO, Ukraine and the West, including in areas of strategic importance to us.

The final point I would mention as we start the discussion is that there is a real risk that generative AI will profoundly turbo-charge disinformation, political interference and cyber-attacks in particular. We can discuss that in more detail if you wish. We have just agreed strategies on generative AI and what to do about it. It is a truly important subject as we go into US elections and UK elections, and, as you all know, half the world is having elections this year. I was just talking to the Deputy Prime Minister of a partner country who said that in his country, the Russians are already using deepfakes to sway the population in the run-up to votes and referenda.

In a moment when, as you can see from public reporting, a lot of the social media platforms are actually removing content moderation, and these tools are proliferating, this issue is of fundamental importance when it comes to grey zone risks.

Q45 **Chair:** We will definitely want to pick up on your point on generative AI. Before we do, you referred to both China and Russia, and China echoing and reinforcing the disinformation being put out by Russia. Are there signs that that is planned and co-ordinated, or do you think it is more China seizing the option and making use of it? Is there co-ordination between the two? Secondly, are there areas where it manifests very differently between the two—between what Russia is doing and how China acts?

James Appathurai: These are great questions. With regard to China and Russia, it is really important to recognise that the old theories that China-Russia co-operation was in some way or another ad hoc or reluctant, suspicious and limited—and maybe it was at the time—is no longer the case. That is not just my speculation: China has a hierarchy—a public hierarchy—of partnership arrangements with other countries. It has only one partner that has the highest level of signed, agreed partnership agreement, and that is Russia. It has a political element and a very strong military element, and continues to be deepened. It is on the political, practical and military levels, and also on the economic level—as you can see, Russia's trade with China has gone up substantially. China is supplying all kinds of components and other pieces of equipment that Russia is using in its military campaign, or war, on Ukraine.

I am speaking for myself now—this is not NATO policy—but I think that what unites China and Russia most fundamentally is a shared desire to see the United States get out of their neighbourhoods so that they can do what they want to their neighbours. That is a very powerful motivation. It is clearly the case that China is on a persistent, consistent basis amplifying Russian messages, and it is not simply an echo. It is important to

recognise that until just a few years ago, China would have never commented on NATO or Ukraine at all. It considered it unwelcome to have NATO or the United States active in terms of politics or messaging in its neighbourhood, but it was careful about not intervening or interfering in politics or security in Europe. That is no longer the case. It does not serve China's interests directly to comment on NATO; we have posed no threat to China.

So you can see that the relationship is structural, including when it comes to both disinformation and activities in other political bodies, including the UN and the UN's systems. I do not know how it is co-ordinated, but the level of co-ordination and coherence is strong and persistent. But are they different? Yes, they are different, and until a few years ago the NATO approach to tackling grey zone challenges was basically to create actor-agnostic resilience.

That was to harden our systems, and by "systems" I mean everything, including the political system, the information system and the infrastructure on which we rely, including cyber, so that it could resist grey zone attacks from all directions. But actually, if you look at what they do, you also need an actor-specific approach, and we have taken an actor-specific approach. It is different with regard to Russia, because Russia is definitely considered a threat to NATO and acts in a much more threatening way—we have to be very clear about that. I mentioned many of the elements, but of course Russia targets different communities when it comes to disinformation. They target them with different messages. We have of course in many of our countries minority communities that are susceptible to these messages. We have far-right communities and political parties that are susceptible to these messages and to coercion. Obviously, Russia can use energy coercion. China is not using it; we don't depend on China for energy. Again, with regard to forced migration, only Russia can do this against us.

When it comes to threats to critical undersea infrastructure, for example, we all depend—I know the UK does—on a very long and complex network of cables and pipelines. It is thousands and thousands of kilometres long. Russia doesn't have this vulnerability; we do. Russia has something called the Russian undersea research programme, RURP—a terrible acronym. This is a very well-funded, highly sophisticated, decades-long programme—you can google it; there is nothing secret about it—the purpose of which is to map out all our critical infrastructure, which they have been doing for decades, with the opportunity to damage or destroy it. China may or may not have been involved, in one way or another, in the Baltic connector damage, but certainly the effort and the intent between the two countries are very different in this area.

Then there is all the sabotage going on around Europe. You have heard concerns about it. The use of organised crime networks in our country is very much a Russian tactic. There are the attacks on our logistics. Then there is all the jamming taking place in our border—again, this is all Russia.

If you look at China, it's very different. First, we don't consider that China is a military threat to NATO; nor is NATO a military threat to China. But there are different risks with regard to China. They include, very much, online activity. YouTube recently announced that it had taken down the biggest online influence operation in history, which was of Chinese origin. Then there is political interference. You only need to look at my country, where this is a very live topic. One of my close friends was the direct subject of this—Michael Chong. As parliamentarians, you might know him. He and his family were put under some kind of pressure. Then there is all the cyber-espionage that takes place based on very sophisticated Chinese capability. They use different economic levers—for example, cutting off access to the rare earths and critical minerals on which we depend or can depend. This has happened with a couple of them recently. Or they use other economic tools. For example, if you are Norway and the Nobel Foundation meets the Dalai Lama, you don't get to sell salmon to China, which has been a big export market for Norway for many years. Lithuania, by allowing Taiwan to open an office, faced Chinese economic coercion. And then we see the pressure on pro-democracy activists, at a very high level.

So there are different tactics, different audiences, different tools and different levels of capability. We are quite convinced that you have to be better able to resist everything, but also you need to have an actor-specific approach to be able to effectively defend in the grey zone.

Q46 **Chair:** You mentioned specifically your concern that interference in elections could worsen with the use of generative AI. What do you think we need to be wary of? What do our peoples need to be aware of in terms of what they could be seeing in forthcoming elections around the West?

James Appathurai: This is a really important question. I do not want to scare people; my wife usually tells me not to talk about generative AI at dinner parties because everyone reaches for the Prozac and goes home by the time I am done. When it comes to the disinformation space, the thing to understand about these tools is that it is, as you know, extremely difficult to detect when AI has generated a deepfake. We have had all the major companies in at very high level and sitting next to each other—I will tell you three things.

One is, they all seemed to agree that their tools for detecting deepfakes are basically not very effective. The line they used with us was, "There will be no deepfake detector in the sky." When it comes to video, which is probably the hardest now to generate, some of the big platforms are at something like a 20% to 25% success rate in detecting a deepfake. When it comes to text, it is 0%, just to give you an idea.

Secondly, many communities are not inured against this. They are not aware of the risks, and the tools are proliferating very quickly. For example, in English-language countries such as the UK, the US or Canada, people are a little bit more used to the idea that there can be a very effective fake. In a lot of countries, they have never seen super-effective

AI-generated deepfakes. Their populations and media are not aware of this risk, or not enough, especially on the social media platforms. They are extremely vulnerable, and we are already seeing that. For example, the Moldovan political system is now feeling very much at risk, but it is also the case elsewhere.

The third point is that these tools are democratised. To my mind, ChatGPT is a little bit like the way Windows was when it came out. Before Windows, you could not programme unless you knew how to programme, basically. When Windows came, anybody could use the internet or find what they wanted to. We went from a very small group of people who could operate effectively on the internet, to everybody. The same thing has happened with these platforms like ChatGPT. Before them, only a very sophisticated and small number of very capable people could use generative AI, but now everybody can use generative AI. It is a democratised threat, and the number of people who can create deepfakes has become basically infinite. That is also a risk for us.

In terms of timing, one of the risks we look at is that deepfakes will be used just at key moments, such as in the run-up to key votes or referenda, just to create confusion or a different point of view, or swing a close vote right at the last minute. We already see some of that. I believe that in two or three years, people will be more used to it, but right now there is a high vulnerability because, as I mentioned, a lot of platforms are not able or willing to police these to a sufficient level.

To give you one or two more datapoints, we hear from the companies that within one year, 80% of what is generated for the internet in one year will be generated by AI. That is an interesting datapoint. Worse, they all agreed when they came here last year that within five years of then—so four years from now—90% of what is on the internet will be fake or false, because you can generate anything. If you think through what that means for politicians and the political process, I believe that most people will learn not to believe anything they see, including when they see you saying something on TV.

I think you had better get used to shaking hands and going to town hall meetings; in-person contact is going to be much more important for the political process than it has been until now, because of generative AI. That is my view.

Q47 **Chair:** We all do a lot of that already, but you are saying even more. That 90% fake statistic is just extraordinary. I have one more question before I turn to John—we are just scoping out how bad the situation is and will then go on to what we are going to do about it. You referred to Chinese components going into Russia, which we know about; I am almost more worried about Chinese components coming into NATO countries and what could be coming in with them. With the internet of things and all the ability to smuggle stuff into components, are we right to be concerned about that? There are procurement regulations going through the House of Commons today. Is it something we are focusing enough on?

James Appathurai: There are certainly allies who believe that we need to be more concerned. My personal view is that we are now waking up to a correct of level of concern, so it is great to hear that there are steps being taken. I cannot testify to this, but I saw in the media that 80% of the cranes in the United States use Chinese components and can be remotely operated—80%. If that is even close to correct—that is only the US, so I wonder what the case is everywhere else.

Coming back to more concrete measures, I think the questions related to Huawei, 5G and the components are very important. It is also important to recognise, when we look outside of our own borders, what is happening in the rest of the world. Chinese components and technology are highly effective and more affordable. As a result, countries with fewer resources, who do not have the option to pay more, come to rely on Chinese technology and infrastructure at all levels and in all areas. That is something that we also need to think about, because with dependence on any country for its technology comes political affiliation. We can talk about Africa, Asia and Latin America later if you wish, but we definitely believe that we need to look more carefully at the resilience of our infrastructure at all levels. We do that for our cyber-infrastructure, critical infrastructure, critical energy infrastructure and port facilities, and the European Union does that of course for its members. We are certainly concerned about potential levels of vulnerability.

Q48 **John Spellar:** I must apologise for having to go after this question to speak in the debate mentioned. You have described the changes that are taking place in the nature of the threat, but I want to ask you about the response. A lot of what we see, including in your response, is the identification of problems and then reaction; do you see any role for NATO or allied countries in taking the issues to our opponents? That means not just being on our backfoot and playing defence, but actually taking offence. In particular, we should not only stress the advantages of democracy but at the same time point out the very deep structural and social divisions inside the autocracies. That applies not only to them but to the battle for the neutral countries, notably in the Global South.

James Appathurai: You ask what is in many ways the most important question: what do we do about it? I do not want to give an endless answer to this, so I will try to be succinct. First, we have to build up our own resilience, as I mentioned. Secondly, we have to respond when they do things that we think are unacceptable, and that does not mean we respond in kind. There have been successive waves of responding to malign Russian intelligence activities by collectively agreeing to expel hundreds and hundreds of Russian diplomats who are not diplomats,[1] or not solely diplomats, but who are conducting intelligence activities. That has demonstrably—we look at these things—diminished Russia's ability to

[1] Clarification agreed with Mr Appathurai: For example, a total of 153 Russian diplomats were expelled in response to the March 2018 poisoning of Sergei and Yulia Skripal.

conduct malign intelligence activities within NATO countries. That is the kind of thing that needs to continue in order to diminish the threat to us.

As I say, there are responses that have an effect that are not just attributing a cyber-attack. We do that, and it is important, but I am not at all convinced that Russia could care less if we attribute a cyber-attack, or that it does anything about it. I think they probably post it on the wall as a badge of honour if we identify them, and then they move on to a different name and a different kind of attack.

But you come to a very important question—something that I think about all the time. How do we get on the front foot when it comes to communications? To put it a different way, what you see in particular in Russia is that the Kremlin has closed off the Russian information space. I used to be the NATO spokesman a few years ago. I watched as they took control of the media and the internet and expelled all opposing views, but also installed, like China did but in a slightly less effective way, a great firewall of control over the internet.

The net result now is that it is extremely difficult to communicate to the Russian population. For me—again, I am not saying this is a NATO position—this is a fundamentally concerning issue because Putin is preparing generations of Russians to think that we hate them and that the collective West, as they call it, wants to damage or dismantle Russia, which is obviously not true, and contain Russia, which is true when it means we do not want them invading their neighbours. And they are training kids in schools with weapons. You have seen that. So being able to communicate to Russians is extremely important, but it is extremely difficult.

We can discuss this more in another format, but we do need to look at innovative ways, exactly as you say, to carry our message to the Russian people. Some of that work is going on. It used to go on decades ago and it needs to happen so that they can hear the truth. I am not talking about disinformation in any way—just the truth about who we are, but also about what is going on in their own country. These are messages that our diplomats pass in Russia, and I know them, but they are very, very small voices.

Then you come to the point of the rest of the world. It is very important that we communicate to them. Again, I will give you my own view. Good messages are not enough. We have to come with actual resources to address their challenges. If you look at what Russia comes with in Africa, they come with the Wagner Group, or whatever it is called now. China comes with billions. There is a classic expression from an African Minister, whom I will not name, who said the Chinese come with an airport and the Americans come with a lecture. That is the reality. They face real restrictions.

When I showed up in central Asia, I was facing Chinese billions and Russian soldiers. I was happy to see the EU, but the EU had €1 billion and I had nothing and I was at the back of the line to meet someone. So yes,

we need effective messaging, but effective messaging with concrete partnership to address the real security issues that our colleagues and partners have.

I have a final point on that, leaving aside security. I spoke with an African Minister of information technology—if you want to call it that—and he had just bought Huawei for the whole country. I said to him, "Why did you buy Huawei?", and he said, "Look, I'm not an idiot. I understand the risks, but it is 30% cheaper and it works, and you do not even have an alternative. I would pay more, but you do not have one." So the end result was a lock-in to a Chinese system. All the data from that country is going back to Chinese servers in China to feed their AI models and so on. I guess my point is: yes, good messaging, but good messaging backed up with concrete co-operation at a resource level that is at the level of relevance.

Q49 **Mrs Lewell-Buck:** You have talked about China and Russia, their growing influence in emerging nations and the money they are putting into infrastructure, water supply, roads and rail, and what have you. They are part of the BRICS alliance. I have heard that dismissed as a talking shop. That alliance has grown. Do you think it is just a talking shop, or should we be paying more attention to it?

James Appathurai: If I may, I will broaden your question a little bit. What we need to recognise is that there is a growing community of countries, big and small, a growing number of whom are increasingly autocratic, that form part of another team. China is clearly part of that team. You could call it Global South. Some people do. China very strongly identifies itself with the Global South.[2]

What goes along with that? There is a certain amount of economic co-ordination and a certain amount of political co-ordination. That is a little awkward between them. The India-China relationship is not an obvious one. They have great difficulties, including military difficulties, so I would not overstress that relationship.

It is also worth noting that basically since the advent of effective surveillance technology—I would say the early 2020s—you can see, particularly from China, the export of surveillance technologies: cameras, AI, facial recognition, gait recognition and surveillance of social media platforms. That has been exported to countries across Africa, Latin America and Asia. China trains the technicians in Beijing, but also in those countries, to operate these systems.

I commend to you Freedom House, for example, which keeps numbers on this—others do too, so I am not just speculating. They are clear figures: since that period, the number of autocracies, which was declining, is now

[2] Clarification agreed with Mr Appathurai: According to the United Nations Conference on Trade and Development the Global South broadly comprises Africa, Latin America and the Caribbean, Asia (excluding Israel, Japan and South Korea) and Oceania (excluding Australia and New Zealand. Most of these countries are commonly identified as having lower incomes, high levels of poverty, high population growth, inadequate housing, limited educational opportunities, and deficient health systems, among other issues.

growing and it continues to grow. The number of pro-democracy demonstrations, in more and more countries, is diminishing. The duration of those demonstrations is diminishing or being eliminated altogether. I therefore think the bigger issue, for me, is that there is a growing number of autocracies and countries that see themselves as at least ambivalent about, if not in opposition to, the West. Technology is reinforcing them and that relationship, and that manifests itself also in international bodies, such as the UN; in the bodies that set technical standards, such as the International Telecommunication Union; and in votes for leadership positions. We do therefore need to have a comprehensive view.

I conclude with this: we must ensure that we do not divide North America from Europe. We are a team, and we had better play as a team, because there is another team, and it has a team captain.

Q50 **Jesse Norman:** Thank you very much indeed, particularly for the clarity and the specificity of your remarks, which are extremely helpful to the Committee.

You have painted a very deliberately realistic-cum-concerning picture about the issues in relation to democracy and the functioning of democracy. I want to pick out a couple of points. One level you might consider is that of consent, as it were—encouraging elements within a democracy to attempt to split it up, to divide or to overturn an economic or political structure. Another one is specific interference with elections. Those are slightly different things. The question then is: what tools do the team you are describing—what we might call the liberal democracies; our team, if you like—have to counter some of these hybrid threats at the consent level and the election level?

We can think about intelligence and cyber-interventions and the like, but you have already told us that there are strict limits on some of those. I suppose the further question is: if some of those tools are coming from the US, which is a highly technically advanced team captain in this area—if they think of themselves using that term; I do not think we do within the UK or Europe—the use of those defences may itself be a form of compromise. Can you comment on some of that stuff?

James Appathurai: A NATO civil servant and a Canadian knows thin ice when they see it, and I do not want to comment too much on everyone's democracy. There are a couple of things. One is that I commend to you a couple of books by a guy named Peter Pomerantsev, who is the expert on Russian disinformation. His first book was titled, "Nothing Is True and Everything Is Possible". The point of it was that the strategy that the Kremlin pursues—although it is now more than the Kremlin—is not necessarily to convince you that their version of truth is correct, but to confuse you into believing nothing, and increasingly I see that. I see it with my nephew: he thinks everything is an opinion—"It's someone's opinion. Truth is your truth or my truth."

One thing we really have to do is think hard about how to ensure that our populations can know that what they see is true or not true and can have confidence in truth. There are companies, platforms and Governments

thinking hard. I just spoke to a very high-level US colleague who is thinking about how you ensure that, for example, if President Biden or Prime Minister Sunak gives a speech, people can check that what they see online is actually the real speech that they gave, or some sort of version of it. There are ways to do that; they are expensive, but that can be done.

The second thing is to really work on media literacy, so that the media understand the role that they play, the role that they need to play and how they can discern between truth and not-truth.

Thirdly, you raised the important point that a lot of the disinformation—the majority of it, based on what we see—is not to create lies but to identify existing fissures in our societies and drive wedges into them hard, and that works. In the run-up to elections, as you pointed out, we really need to raise our game and level of alert and try to diminish some of those wedges, and that is extremely difficult.

Another point is to educate the population. We look at our new members, Sweden and Finland, with great fondness, because aside from their military capabilities they bring great societal resilience to hybrid or grey zone attacks, for obvious reasons, particularly in the case of Finland. Sweden has given a pamphlet to every single citizen to say, "This is what you need to look for." There was a little bit of criticism, saying, "Oh, you're frightening people," but actually they need to be aware. This is a different environment, so in my view we cannot go with the same approach that we had 15 years ago, when I was happily thinking that we were in this indefinite period of good times. Well, they are over now, so the population needs to be more concerned and more aware.

If you look at the Baltic states, they have taken stronger measures when it comes to foreign ownership of media in their country and when it comes to the broadcasting of foreign media in their country. It is a difficult discussion. I have a really close Bulgarian friend. She said she grew up in the communist era, and they have a certain sympathy towards Russia in half of the Bulgarian population. She said to me, "It used to be that we could not watch Western TV, and we did not like it, because the Russians were censoring it, but now we cannot watch Russian TV, because the EU blocks it, and I cannot explain to my family why that is different." I explained to her that it is different because we have a high level of vulnerability to Russian disinformation that is penetrating our environment, and they lie all the time and we can't just be naive about that. She accepts it and understands it, but I recognise also that these are difficult discussions for everybody, and every country has to set the threshold. Even in my own country, we are looking at minority communities and how they are being influenced by disinformation in, for example, the Chinese language, which we don't necessarily always pay attention to, or the Russian language—less so in Canada.

There are what you might call best practices, or at least practices, taking place across the alliance in different areas, which could enlighten any individual member if they wished to raise the level of resilience when it comes to information. But the bottom line—and I speak for myself here—is

that we need to do it, because we are very open and vulnerable to what are clearly well-resourced, highly sophisticated and increasing information campaigns against our populations.

Q51 **Richard Drax:** How are strategies such as deterrence and collective defence adapted for hybrid operations compared with more conventional defence?

James Appathurai: The short answer is that the reason why grey zone attacks are effective is precisely that they are harder to deter. Part of the reason why they are harder to deter is that the attacker has plausible deniability, or enough plausible deniability, partly because when they are identified, they spray out a range of other versions of the story so you don't know what to believe. We saw that with MH17, for example, where Russia put out 34 versions of what had happened in the first two weeks, and we see it with attacks on critical undersea infrastructure.

One way we can be more effective in deterrence is by being more effective in identifying the attacker more quickly; we need to put resources into that. That is exactly what we are doing with regard to critical undersea infrastructure.

We want to deny deniability, which can be done across the spectrum, but you have to put resources into it. You have to be quick and confident, but also willing to accept 90% certainty, because you might not ever have 100%. That is one way.

There is another way, and those of you who have studied nuclear or military deterrence know this. You basically have deterrence by denial and deterrence by response. Deterrence by denial is when you build up your resilience to make it clear that an attack will be unsuccessful anyway, so there is no point in trying. Deterrence by response is saying, "If you attack me, I am going to respond somehow, and it's going to be more painful for you than for me, so you might want to not do it."

Deterrence by denial is something we can do at all times. NATO has agreed with all allies what we call baseline requirements. Those are civil, civilian requirements for national resilience, and I think that there are measures we can learn from allies. In Finland, Government and industry leaders sit down every six months to exchange views on what the threat environment is, and they decide together what the country needs to be resilient. The industry leaders go away, and as part of their budget and planning they say, "Okay, I need to have this much in reserve, because I am part of society." If you cut Finland off from the world for six months, they can handle it. They have the fuel, the medicine, the food, the grain, because they know it can happen. It is a full society effort, and they don't just expect industry to suddenly step in at the last minute.

I really believe in having a much stronger relationship with industry—the cyber industry, the food industry, the energy industry—so that they are getting regular threat briefings and they can tell you what they see, and so they feel part of the effort. Then we get much stronger societal

resilience across the board. We set them clear targets and standards that they can meet, and we provide support to help them meet those standards, as we do, for example, in cyber. It is either positive or negative, with positive meaning some resourcing or some tax breaks, and negative meaning us saying, "If you don't report on a cyber-attack against critical infrastructure in the United States, you are violating a directive, and you should say, because otherwise we don't know what is happening."

Then there is deterrence by response and I mentioned one of the measures that we have already taken, which is to eject Russian intelligence officers. Another step we took was to cut off Russian oil and gas, which then improved our resilience and imposed a cost on Russia; you have seen that Gazprom's profits have gone down considerably.

Those are the three major elements that we need to consider when it comes to deterrence: deny deniability, improve your resilience—deterrence by denial—and be more effective and prompt in response, including in the ways that I mentioned.

Q52 **Richard Drax:** You talked about deniability on the subsea cables and you said that we could never be 100% certain that, say, Russia had damaged a subsea cable. When there are thousands of miles of these cables, how do you physically do what you have suggested we should do?

James Appathurai: That is a very good question. There are a few things that you can do and that we are doing.

The first is to connect industry operators with our maritime command, and that we have done, so that we can share information with them on an ongoing basis. We just set up a critical undersea infrastructure network with industry, and by the way we have connected them to our critical undersea infrastructure cell in our maritime command in Northwood, so thank you for hosting it.

Secondly, we need to enhance very fundamentally the picture. We are building a tool that fuses information, ranging from satellite information, much of which is publicly available, to basically the transponder data that all ships at sea are supposed to be broadcasting, to information from drones, including drones at sea and drones under the sea, to the information that the companies provide, in particular on the cables that they run—they can easily put sensors in that give much more detailed information. We fuse all of that information using an AI tool, basically like a task-oriented chatbot, which can take it all and say, "You need to look here."

At any given point every day, there are about 50,000 ships at sea in Europe, and we know where the critical infrastructure is. Using these tools and some others, we can say, or industry can say to us, "There's a ship that's loitering over a key node for longer than it should be. Go have a look. This ship left from a Russian port. This one you need to look at." You can sift through all that data, and the AI can really help you to narrow it down to two or three that you need to look at, and then we can deploy

assets. Our Supreme Allied Commander deployed assets after Gazprom to make a point. We did the same thing around Balticconnector. We can use existing tools and technologies, and we are, in very effective ways.

Just to finish the story, when Balticconnector happened, we had all the intelligence people and military people doing things, and my intern said, "Give me two hours." He went down the hall and came back and said, "This ship left that port at that time. It turned off its transponder here, and then it looks like it dragged its anchor there," and he was right. This kid was like 24 years old and I hadn't even asked him to do it. There is a lot of information out there that we can use. Your military and Government are using them, and so are we.

Q53 **Sarah Atherton:** Good afternoon, James. We understand that a whole-Government strategy is the way to build resilience and deterrence, but here in the UK the MoD—defence—is used first and last in any crisis. Whether it be covid or flooding, it becomes the risk manager of last resort. Accepting that defence plays a pivotal role in deterrence by punishment or response, as you put it—I prefer response to punishment—how can we encourage other Government Departments to play their role, and what role do you think UK defence should play?

James Appathurai: In resilience, do you mean, or deterrence?

Sarah Atherton: Both, please.

James Appathurai: I think the role in deterrence is probably pretty clear for the UK military, and we are very glad for it, because it is honestly a great military. I come from a Defence Department, so I have a particular sympathy and I think your question is really important. The Canadian military is now increasingly drawn into all kinds of things for which it was not necessarily intended. I will give you one example, which is resilience against the effects of climate change. Every summer now, my country burns, and the military, which is supposed to be doing military things, is firefighting. That is not what they are designed to do, and if they are doing that, they are not doing something else. It is really important, exactly as you say, to recognise that a whole-of-Government approach is required for resilience.

As I said, we set these baseline requirements—or rather, we offered them to allies and allies agreed to them. They have gradients. We in NATO, in the cyber-sphere, have offered baseline requirements when it comes to the cyber-protection of critical infrastructure. That obviously engages industry, and our Governments all signed up to that. It again offers levels of support; we offer support to assess and then to grow.

From a NATO point of view, we are doing our best to encourage allies to have a more whole-of-Government approach, but I come back to what I said before. First, I would suggest a visit to Finland, which has a Ministry for national resilience that brings together all the relevant elements of Government and the private sector.

My second point is that what we have at NATO is, in many ways, an ad hoc relationship with industry, except with the big defence primes. What we are seeing now is that one sector after another—from energy to cyber to the industries that are affected by climate to start-ups and scale-ups, and very much the big tech platforms—is coming to us and saying the same thing over and over: "We know the world has changed. We know that we have a role to play in defending society, and we want to. What we don't know is what the threat environment is and what it might be, and we don't know what Government requirements are and will be in this area, so we don't know how to plan for them." My experience is that we are at a moment when we can build a much more structured relationship with industry at the top level and down, to have the sustained engagement that will make a difference for the whole society.

Let me give you an example that I brought into NATO from the UK. I went to visit the UK National Cyber Security Centre and found industry embedded in it. I was told that the industry representatives were basically working there for free or at a very low cost, so I asked them when I was visiting, because we are designing a cyber-centre here, "Why are you here?" They said: first, purpose, because they knew they needed to be part of it; secondly, they got information that helped them to do what they needed to do, so as embeds not on ad hoc visits; and thirdly, interestingly, one of the guys said that when they were competing on the open market for cyber-talent in the UK, which is hard to get, and they said to young engineers, "If you come to work for us, one day a month you'll go work in the NCSC and help defend the UK," they signed with them, so it was actually a recruiting tool. I think you have a real opportunity with industry now, which we did not have even three or four years ago, to build a very different relationship for a whole-of-society approach.

Q54 **Sarah Atherton:** When you said "we offer" as NATO, is that the Joint Intelligence and Security Division? If not, what do they do and how do they support alliance partners?

James Appathurai: The Joint Intelligence and Security Division, in essence, fuses intelligence from allies. It does that on a day-to-day basis. That does not necessarily mean that all allies have to agree on what that intelligence is, but they can offer you, with input from a select group of countries, "This is something you need to know, based on input from this number of countries." They also prepare broad, agreed intelligence on which we all rely, and which is based on all allies providing their input and giving their agreement to it, so it's a sort of foundation for us to have a common view of what is going on in the world. They don't generate their own—NATO is not an intelligence gathering body; we don't have spies. It's too bad, really, because in the first "Mission Impossible" movie, apparently, the bad guy stole the list of NATO undercover agents, but sadly we don't have that. My son was really impressed that we had it, but actually we don't. They are just fusing what you provide to us and the other allies.

Q55 **Sarah Atherton:** Can I just ask one quick last question? Does NATO have a strategy to assess what type and scale of hybrid attack would

constitute a decision to invoke article 5?

James Appathurai: Good question. The short answer is no, but deliberately no. The reason it is deliberate is twofold. One is that we do not want to show where the line is, so that a potential adversary would know where the line is and stay just below it—they would move up to that line, and just stay below it. The second is that you do not know what it is until you see it. To give you a concrete example—I have been at NATO a long time—before September 11th, if we had tried to agree that a bunch of terrorists hijacking planes and flying them into a big civilian building in any one of our countries would have constituted an article 5 situation, we would not have gotten agreement on it, or worse, it would have been excluded when we needed to invoke article 5. We believe—our allies all believe—it is better to be ambiguous and make the decision when they decide together that it has been reached, for both of those reasons.

Q56 **Mrs Lewell-Buck:** Hello again. What NATO countries are the best at countering hybrid threats, and can you give us any examples from them?

James Appathurai: It varies from country to country based on the tool. I've talked about Finland and Sweden extensively, so I will not mention them again. Look to the Baltic states in particular—for example, to Estonia, whose cyber-resilience is extremely strong. The steps the Baltic states are taking to diminish Russian influence in their minority communities is very sophisticated. It is debated very democratically. That offers some very important lessons for us all on how to do it, because one thing is what you do, and the second is how you do it. It needs to be transparent to the public, so that when accusations come that it is not democratic—these usually come from those funded from outside, who do not like that you are doing it—you can come back and say "No, these are the steps we followed and everybody agreed to it." I think those are very important.

I could go on for a very long time, but one other example comes from our German colleagues. The German Government are very active in sending officials to the very local level, to private companies, to say, "Be careful about investment from actors that are unfriendly to the UK, or less friendly to the UK." You might not have thought about it, and many of my friends in start-ups do not think about it, but when I tell them, "If you do this and you take investment from, say, China, these are the risks," they then say, "Oh, okay, maybe I don't want to do that." It is about educating the private sector. Germany does that extremely well, at least in the particular area I mentioned.

Looking at my list of other areas where people are doing very well, cyber is probably one of the most important and every country has to make its own decisions on how it does this. You can debate what the US has done, but honestly, what it has done, and to a different degree what the EU has done, in engaging with critical infrastructure operators to raise the level of cyber-resilience and report on effective cyber-attacks against them, is extremely important.

One of my real concerns is that there is a huge amount that goes unreported. When it comes to ransomware, a huge amount of malware is not detected because countries and companies are not investing enough in basic cyber-hygiene. It is getting slightly better, but it is still the case that CEOs are not rewarded for cyber-hygiene, and they should be, because it is all fine until it all goes wrong, and then it is really expensive. I find your best practice question very interesting. As I reflect on what we should be doing next, maybe we should be putting together a best practice compendium. We have done that when it comes to adaptation to climate change; my colleagues and I prepared a compendium of best practices for allies to share, and we also did that on how to cut greenhouse gas emissions. Maybe it would be interesting to do something like that on hybrid as well, so I will take that away and reflect on it.

Mrs Lewell-Buck: We will look forward to it.

Chair: James, thank you so much. We have had our time, but you were extremely helpful. There was really good insight there, which will be very helpful for our report. Thank you very much for spending the time with us.

James Appathurai: Always a pleasure, and we are at your service.

Chair: Thank you.