

Defence Committee

Oral evidence: [Defence in the grey zone](#), HC 405

Tuesday 25 March 2025

Ordered by the House of Commons to be published on 25 March 2025.

[Watch the meeting](#)

Members present: Mr Tanmanjeet Singh Dhesi (Chair); Mr Calvin Bailey; Alex Baker; Lincoln Jopp; Emma Lewell; Mike Martin; Jesse Norman; Michelle Scrogg; Fred Thomas; Derek Twigg.

Questions 53 - 126

Witnesses

I: Luke Pollard MP, Parliamentary Under-Secretary of State for the Armed Forces, Ministry of Defence; Paul Wyatt, Director General Security Policy, Ministry of Defence; Air Commodore Matt Bressani OBE, Head Military Security Effects, Ministry of Defence.

Examination of witnesses

Witnesses: Luke Pollard, Paul Wyatt and Air Commodore Matt Bressani.

Q53 Chair: I call to order today's Defence Committee evidence session on defence in the grey zone. This is, in fact, our last evidence session for this inquiry and is a ministerial one. I am very pleased to welcome our guests on the panel today. We have Minister Luke Pollard, the Parliamentary Under-Secretary of State for the Armed Forces. We also have with us Paul Wyatt, director general for security policy at the Ministry of Defence. I am also pleased to welcome Air Commodore Matt Bressani, who is the head of military strategic effects at the Ministry of Defence. A very warm welcome to all of you. Indeed, Mr Pollard, I believe this is your first outing with the Defence Committee, so a very warm welcome, and I am sure that members will make you feel welcome during the hearing.

Before I go more deeply into defence in the grey zone, I just wanted to give you the opportunity to get something on the record. There were shocking revelations last night around the Signal messaging group that involved senior US defence and other officials. Given our previous involvement in strikes against the Houthis, can you confirm whether the lives of any British servicemen and women have been put at risk on account of what has been revealed in the messaging group?

Luke Pollard: No. All UK service personnel are covered by our normal approach to operational security, and the Committee will understand that I will not go into the details of how we keep our involvement in any support for military operations in the Red Sea or anywhere else. We have high confidence that the measures that we have with our allies, including the United States, remain intact.

Q54 Chair: I wanted to give you that opportunity, because it is important that you have helped to reassure the nation that no lives of British servicemen and women have been put at risk.

Moving on to defence in the grey zone, you will have begun to appreciate that the Committee—our predecessor Committee as well as the newly elected and appointed one—has spent a considerable amount of time on this matter. I hope that, in the upcoming strategic defence review, there will be significant emphasis on how we tackle and overcome threats in particular from our adversaries. Where exactly are we with the strategic defence review? We have had mixed messaging from certain quarters, especially within the media. When are the Government looking to publish it?

Luke Pollard: I would always be cautious about listening to speculation in the media. The position on the strategic defence review has not changed. The work is well advanced, as the Prime Minister said last week. We still intend to publish in the spring. That will be part of measures that will be reported from Lord Robertson and his review team to the Prime Minister, the Chancellor and the Defence Secretary. The Prime Minister



has been clear that he will then take the strategic defence review to the House of Commons and report it formally to Parliament.

- Q55 **Chair:** What exactly are you looking to publish from the SDR process itself? The reason I ask is that, in a November evidence session with our Committee, the Secretary of State committed to greater Government transparency for our Committee. I am very grateful to him in particular and want to place on record my thanks to him and other officials for facilitating the classified and secret briefing sessions for our Committee members, which have helped to inform our opinion on matters. You will be aware that the detailed output from the review has, at times, been forthcoming in previous strategic defence reviews, so can you confirm what specifically you are planning to publish in the SDR?

Luke Pollard: It will be for Lord Robertson, as this review is externally led, to create his report. That will then be sent to the Prime Minister, the Chancellor and the Defence Secretary. We would probably expect for there to be further announcements by the Ministry of Defence as we seek to operationalise what would be a strategic review, looking at the high-level threats that we face.

The terms of reference for the strategic defence review were published when the Prime Minister launched the review on 16 July last year, and the work of Lord Robertson will reflect the terms of reference for his review. It will then be for the Ministry of Defence to take the recommendations and operationalise them, recognising the fact that we live in a very difficult and changed world, and making sure that we can keep our country safe at home and secure abroad.

- Q56 **Chair:** I note the comments regarding media coverage, but there has been some concern in defence quarters, because Jonathan Powell, the national security adviser, is reported to be lobbying for the SDR to be wrapped up into a wider cross-Government assessment of threats. This would appear to be at odds with the Prime Minister's response on the Floor of the House. Can you confirm to us that the strategic defence review will be published and not just wrapped up into a wider cross-Government departmental process?

Luke Pollard: The intent of the Department has not changed from when it was announced in July last year. The Prime Minister has been clear that, in addition to the strategic defence review, which is an MOD-led review, albeit externally led by Lord Robertson and the reviewers, there is a parallel review taking place largely out of the Home Office: the strategic security review.

He announced last week or the week before that his intention is to create a national security strategy, which will reflect the threats that we face not just on a military basis but as a whole-of-Government approach to looking at the challenges that face UK security and how this Government are seeking to meet them.



HOUSE OF COMMONS

Certainly, one of the challenges that has been apparent since we came to office in July is that there is a lot of security architecture across Government. There are some incredible pockets of best practice. One of the things that we are keen to do is to join up that expertise more to make sure that we have a better effect from the facilities, people and capabilities that we have across Government at the moment. That is the intent behind where the Prime Minister is going with the national security strategy.

Chair: Some such scrutiny is not possible on the Floor of the House, so it is important that you, as Minister, were given the opportunity to get certain things on record and to allay some of our concerns and those of the wider defence community.

Q57 **Lincoln Jopp:** Minister, you said that the defence review will reflect its terms of reference, although the Robertson review is a 2.5% review. It has been slightly overtaken by events, because the Prime Minister has now said that it will be 3% in the next Parliament. Are you going to have another review to work out how to spend that additional number, or will the SDSR and the operationalising thereof be sufficient to take account of the 3% ambition?

Luke Pollard: I am really confident that it will provide us the opportunity to bring forward a capability situation for our armed forces at 2.5% earlier than originally planned. The 2.5% level that we will reach by April 2027 provides the opportunity for us to embark on deeper reform of our defence apparatus to meet the challenges that we are facing. Having the glidepath that will take us to 3% in the next Parliament, when economic conditions allow, allows us to look at the threats that we are facing. For the very first time, there is not a single person in the Ministry of Defence, in civilian roles or in uniform, who will have served with a decade of rising defence spending, which means a different challenge as to how we, as a Department and as a Government, approach that period.

The recommendations that I am expecting Lord Robertson to come out with will be true to a 2.5% world and will provide the opportunities for us to develop capabilities and to reform defence, which will help deliver a 3% world. It is worth stressing that, if we do not have deep defence reform, we will not be able to deliver the maximum value out of that 2.5% world, let alone a 3% world, because we know that we have inherited a situation where our forces were underfunded and hollowed out.

We also know that, from the experience in Ukraine—where warfare is changing and definitions of what is the close and the deep fundamentally moved from where we originally felt they were only a few years ago to where they are in practice today—we need to look again at capabilities and our doctrine. I am expecting Lord Robertson to make recommendations to meet those challenges, but I am confident that the increased spending that we have been able to secure, and the greater focus on not just capabilities but how we reform defence procurement,



HOUSE OF COMMONS

via my colleague, Maria Eagle, will help us drive more change to deliver more value out of the increased defence spending that we have.

- Q58 **Mike Martin:** On a slightly different topic, what actions would you take if you found out that the air commodore and Mr Wyatt had been sharing classified operational plans on Signal?

Luke Pollard: I can understand why you are going down that line with the question. The Ministry of Defence has very clear policies in relation to what information can be shared and in what format. We do not comment on how allies share their information, for good reason.

- Q59 **Mike Martin:** Forgive me for interrupting. I am not asking you to comment on our allies. What is that Government policy? When I was in Afghanistan, I saw a staff sergeant who, by mistake, took a disc from a top-secret machine and put it into a secret machine. It went into the wrong system, which was not cleared to carry that data. His clearance was withdrawn, he was sent home from Afghanistan and his career was over. Is that Government policy in the United Kingdom?

Luke Pollard: We certainly take security classifications very seriously in the UK armed forces and across the Ministry of Defence, and have a variety of policies that set out how information should be used and shared. All officials and military personnel will be familiar with those. As a relatively new Minister, what has been made clear to me is what my role is in making sure that, when information is given to me, it is used appropriately. I am confident that we have robust measures to safeguard our information and data. We also have a very clear set of systems for individuals who do not follow procedures, with sufficient consequences to reflect the actions that have been taken.

- Q60 **Mike Martin:** What would those consequences be if somebody took classified operational plans that were occurring in the next 24 or 48 hours and shared them on a messaging app? What actions would you take as a Minister?

Luke Pollard: Again, I understand why you are going down this line. It would depend on the context, the information that was being shared and who was sharing it in terms of where in the chain of command. My general rule would be that, if operational decisions are being taken, we should all, regardless of our role within defence, take our information sharing seriously, and there would be a clear consequence and disciplinary process for anyone not following those procedures.

- Q61 **Mike Martin:** It is not acceptable, is it?

Luke Pollard: If anyone were sharing information in our system outside of the authorised systems that allow that data sharing, we have clear procedures in place for how we would address that.

- Q62 **Mike Martin:** Moving on to a slightly easier topic, what is the nature of the hybrid threat to the United Kingdom?



Luke Pollard: You said that it was an easier question.

Mike Martin: We can go back to the other one if you like.

Chair: We will move on from the Signal messaging and come on to the hybrid threats.

Luke Pollard: How you define hybrid threats would be the first challenge to scrutinise there. The Ministry of Defence does not use the definitions “grey zone” or “hybrid” threats in the same way. We use “state” threats as our definition. Our allies would use slightly different language as well, and it is certainly true that even some of our closest allies have a different terminology for some of these things.

Broadly, though, we are talking about activities prior to conflict. In that situation, we are certainly seeing the threats evolve. We are seeing a deepening of threats that the United Kingdom and our allies face. We are also seeing a greater public awareness of some of those threats, and some of that is because we have, as a Government, decided to call out activities of our adversaries and to deliberately place that information in the public domain in order to deter or to call out malign activities.

Also, as we have moved to a more digital environment, it is certainly true that more people are familiar with their own personal digital safety and that of their workplace, whatever that may be, and that has brought into stark contrast the levels of threat to the United Kingdom that we face. When we are looking at grey zone, sub-threshold or hybrid, however you define it, that could cover nearly everything that the Ministry of Defence currently does, other than the kinetic activity in certain locations—for instance, Op Shader activities over Syria.

It covers an enormous amount of what we do, but I should also say that the Ministry of Defence is responsible for and delivers only a certain amount of HMG activity in relation to grey zone, hybrid or state threats. Our colleagues in the Home Office, DSIT, FCDO and a whole range of Government Departments play their role in being able to meet some of those challenges, and we see our role as taking a lead where it comes to those that affect a military instrument or where we have a particular specialism, but also being very clear that our role is to co-operate, collaborate and integrate with our colleagues across Government. That is what we are increasingly doing and I would expect us to do more of in the future.

Q63 **Mike Martin:** That leads me perfectly to my next question. Who is in charge of all this? Yesterday in the Chamber, you were asked who the Minister responsible for our undersea cables is. You answered by saying that the Prime Minister is, of course, and he delegates it, but who is responsible for responding to the hybrid threats, whatever terminology we use? Obviously, it is the Prime Minister, but which Minister is it delegated to? The cross-departmental, amorphous soup that you described reflects the nature of the threat, but that does not necessarily



help us respond to it. Who is in charge?

Luke Pollard: The answer is that it is the Prime Minister and that he delegates it to a cross-Government approach. The reason that it is important to stress that is that the Ministry of Defence does not take any action in this area on our own. We take it as part of a joined-up, integrated, HMG-wide approach.

It is hard, because grey zone covers so much. If we take an example such as cable defence, the safe operation of cables and undersea infrastructure would be a DSIT responsibility. Industry would have a role in terms of the regular surveying and data collection of their infrastructure. Ministry of Defence would have a role in terms of the wider defence bubble that we might place over particular assets. Our colleagues in transport would have a role in terms of the maritime environment. That is cohered together via the Cabinet Office, which, in many cases, would lead the response to any incidents and would also ensure that we are working together effectively. The answer might not be as clear-cut as saying, "It's Bob over there".

Q64 **Mike Martin:** Is the Cabinet Office the clearing house for these decisions?

Luke Pollard: In some cases, across Government, the Cabinet Office does function as a convening power to bring people together. What has been true—and I am stealing Pat McFadden's approach here—is that the Cabinet Office functions differently under this Government than perhaps under the last one, because it has fewer discrete, additional things attached to it that did not really sit anywhere else, so they were put into the Cabinet Office.

Our intent is to have very clear, mission-led Government run out of the Cabinet Office and that convening function. Especially in areas such as securing our underwater infrastructure, we need activities from across Government, with different responsibilities, because of different pools of expertise and centres of excellence across Government, to be able to convene those functions. Officials and our military colleagues will work operationally on a day-to-day basis with people outside the Department, across Government and, in many cases, across our international partners. That is just normal, everyday business.

I entirely understand the temptation to say, "In the absence of one person who we can point at, who is it?" but the way that we approach grey zone challenges is by playing to our strengths and having an integrated approach. That is what we will be seeking to develop more of, because, if we took the opposite approach and replicated every capability within every Department in order to do it, that is inefficient. If we took the approach that only one Minister is responsible for any one thing, they would have to reach out across Government and be briefed from a variety of Departments at the same time. I feel pretty confident that this integrated approach is the right one, but I understand that it does not



HOUSE OF COMMONS

make an easy answer in the Commons when you are trying to get a quick soundbite and a video clip.

Q65 Mike Martin: I accept that it is cross-departmental and that, ultimately, responsibility rests with the Prime Minister. If there is a successful hybrid attack on our critical national infrastructure, will it be the Prime Minister's fault?

Luke Pollard: The Prime Minister takes his responsibility for national security incredibly seriously, and I have to say that he feels that very personally in terms of his approach to how he is addressing the increasingly difficult world in which we find ourselves as a nation, but it is absolutely true that it is a team sport when we are keeping our country safe. The mix of Government Departments and cross-Government activities would depend on the nature of the hybrid threat. Indeed, you might see more industry involved with one approach, or more international partners. Some of our hybrid threats are not geographically bound. A threat to a cable is very specific in a location, but a cyber-threat, for instance, might not be geographically bound in the same way, and so you would draw in different expertise in relation to that and it would be a team sport when it comes to it.

Q66 Fred Thomas: Minister, you described a couple of hybrid threats, and you talked about a slight change over the last year, since Labour came into Government, in terms of how the Government communicate those threats to the public, and increased public awareness. We remember the Government telling the public earlier this year about the deployment of a submarine to surface next to a Russian spy boat in British waters, which marked a departure from previous policy, where that would all be classified much too highly to release. That was timed fairly shortly before an announcement of increased defence spending. Can you give us a sense now of the Government's assessment of how hybrid threats are changing, what is current and what the future looks like in terms of these sub-threshold activities?

Luke Pollard: Yes. I might bring colleagues in to give some more detailed examples in response to your question. Broadly, we took a decision, as Ministers, to declassify not just the activities of the Russian spy ship Yantar, but also our response to it, as a clear deterrent activity that would prevent Russia being able to operate in the same way in the future.

In terms of the decision on timings for that, the activity that we declassified was from Yantar's movement from the North sea through our waters and then further south. It was during that period when the activities of the Yantar were followed by not only Royal Navy and Royal Fleet Auxiliary vessels, but also by the RAF. It was at that point that we took the decision to surface a Royal Navy submarine next to the spy ship Yantar, and then the ship left. That is the best way of describing what happened then.



We declassified that information on the Yantar's return leg. The timing was driven mainly by the Yantar's journey back from the Mediterranean, up through the Atlantic, and back into our EEZ. We wanted to make sure that our deterrent message was as effective as it could be in order to do that. It was a useful demonstration of a different approach.

It is normal for us not to comment at all on the activities of our submarine fleet, for very good reason. As Ministers, we felt that the consequences of the Yantar's activity, not just in isolation in UK waters and in our wider EEZ, but in the context of cable breaks in the Baltic and other activities affecting our allies' undersea infrastructure, not just those in UK waters, meant that we needed a stronger response.

One of the key bits about the credibility of a UK response, in terms of both deterrence but also how allies look to us, is being able to identify a perpetrator and say that it was this ship or this malign actor that had undertaken this piece of hybrid activity. It not only makes our adversaries think again about acting against the UK, because we will identify their actions, so there is a deterrent piece there, but also that, every time the Yantar leaves port now, the entire world can identify that as a Russian spy ship.

Q67 Fred Thomas: That is brilliant. If I could bring you on to talk about how hybrid threat is changing, we are quite aware of the threat to undersea cables. What are some of the things that are known but have not made the front page yet? Can you elaborate on the Government assessment of how hybrid threats are changing?

Luke Pollard: I might bring colleagues in to answer that, but at a high level, we are seeing an increase in sub-threshold activity, which can have an influence on both the UK and our allies. Some of that is using technologies that already exist, such as drones. The MOD operates a good counter-UAS capability, but drones are dual-use activity, and the developments, as we are seeing in Ukraine, provide more opportunities for those. I would just be cautious about placing too much into the public domain, because what we do not want to do is to set out, "Here is the list of threats that we face", which malign actors could then use as a to-do list, but some of those are already in the public domain.

Q68 Fred Thomas: I will mention one that is in the public domain. The *i Paper* published a story online earlier this year about having been able to geolocate, they say, individuals who, they say, were Russian proxies and who, they say, they were able to track from some farming activity in Europe, and who travelled to the UK and, apparently, happened to be located very near the UK air bases where drones were flown that stopped some of the UK activity from those UK air bases. That is already in the public domain. Are you able to comment on what the Government position is on whether we are at an increased level of threat from that disruptive, very low-level and very easy-to-achieve activity?



Luke Pollard: As a matter of default, we would not comment on operational activities or intelligence matters, so I would not be able to comment on that specific example. If we were to point to activities that are in the public domain in relation to a similar type of cohort, we know that there have been Russian-backed activities in the United Kingdom in relation to both the escalation of criminal activities but also the effect on infrastructure that could come from those.

That is in the public domain, but that is a really good example, for instance, of where there is a temptation to say, "Because it is a Russian activity, it must be the Ministry of Defence that responds to it". In many cases, that is a National Crime Agency response, which would be led by the Home Office and, in particular Dan Jarvis, the Security Minister, and the Home Secretary. How we approach those particular problems gives a good approach to, "It needs to be in a cross-Government way", but I might ask colleague to add to that.

Q69 **Chair:** Minister, as you said earlier, you wanted the air commodore and the director general to come in with examples to answer Mr Thomas' questions. Air commodore, director general, do you have anything to add to this?

Paul Wyatt: I was going to go to the same place that the Minister did, which is that there are a number of examples of Russian-linked criminality, particularly arson attacks. We can pick one example. In March 2024, charges were brought against criminal actors with an acknowledged linkage to a Russia connection against a warehouse that was connected to a Ukrainian interest and ownership. That is quite a good example of the kinds of things that we are seeing. That proliferation of the use of criminal contacts to generate more threats is absolutely the kind of change that we are seeing.

Air Commodore Bressani: From my perspective, it was quite well put in a previous session, where a witness described to you that, essentially, the threat surfaces are both increasing in size but also in the amount of surfaces that are out there. The threat can come from almost anywhere and through any domain. This has been recognised by military doctrine for quite a number of years, and everything that we plan comes from something that you may be familiar with, which is the integrated operating concept that was published a few years ago.

Essentially, we deem all sub-threshold activity to either protect, engage or constrain—protect our homeland, ourselves and our allies, engage with our allies and friends abroad, and constrain adversaries where needed. All of our activity is planned and, hopefully, executed along those lines in a sub-threshold manner.

Q70 **Fred Thomas:** Minister, you described the UK needing to show credibility and needing a stronger response to show that. You also spoke about how grey zone or hybrid warfare is all sub-threshold—that is, the threshold of war. People also talk about "pre-war". It is all about deterrence. It is all



about a push and pull of deterring war. A large part of deterrence is making sure that your adversary does not want to do something. As they stand at the moment, are our wider armed forces strong enough to deter a peer adversary?

Luke Pollard: Yes, but we want to do more. Deterrence by denial, which is what you are getting at, is about making sure that we have the capabilities, the credibility and the intent to, basically, deter any action before it takes place. That is part of a broad range of tools that the Ministry of Defence and, indeed all of Government, would have in the grey zone space. That would enable us to pick and choose from a much broader toolbox in any particular situation.

Q71 **Fred Thomas:** There is a move to spend 2.5% of GDP on defence in over two years' time. People such as Neil Kinnock, a former leader of the Labour Party, and several former Defence Secretaries say that that is nowhere near enough to credibly deter a peer adversary such as Russia. That is the game that we are in now. Is 2.5% in over two years' time anywhere near enough of an increase to deter Russia?

Luke Pollard: That is precisely the reason why we have set out a clear policy to move to 3% in the next Parliament. What we need to demonstrate with 2.5% is a journey to reform our armed forces, so that that money is spent better than it has been in the past. That deep defence reform that we need to take place is not only in procurement processes, in trusting our people more, in renewing the contract to a nation and those who serve, and in genuinely valuing service more, but is also about making sure that we can, on behalf of the British people, be a credible spender of more defence money, which means, in my mind, directing more of that money at UK firms, especially SMEs, where we know that defence can be an engine for growth.

When it comes to that credibility of deterrence, we do not fight alone. We fight as part of a broader collection of nations, and what you will be seeing from the SDR and the announcements since we came into office is that NATO-first approach and that clear focus that, when it comes to deterrence, and to the interoperability and, increasingly, interchangeability of the kit and equipment, and the fighting forces that we have to respond to or deter any challenge, we need to increase our lethality of that. We do that by investing more in our people and in our equipment, and by working together more. That creates a greater deterrence in a conventional sense, as well as sub-threshold deterrence measures.

Taken together, we need to spend money better. We are seeing an unprecedented rise in defence spending, and the biggest since the cold war. It is now the Ministry of Defence's job to spend that well and to clearly demonstrate that, in spending it well, we can not only have a greater military deterrent effect but also be an engine for growth across the country. The Secretary of State's intention is to do both of those.



Q72 Emma Lewell: Minister, you will be aware that, last year, the previous iteration of this Committee did a report called "Ready for War?", which highlighted that we are significantly lacking in kit and personnel. That was only around 12 months ago. At the time, we also said that you cannot just keep saying, "We will rely on our allies". What we have seen recently is allies' priorities changing. What they want to do in defence sometimes changes. What is different now than when we did that report?

Luke Pollard: It is a very good report that the Committee did.

Emma Lewell: I agree.

Luke Pollard: It was a really useful one in highlighting the state of our forces at any given moment. As a Minister, if we ask our forces to do something, can they do it? Yes. Can they provide credible deterrence? Yes. Do we want them to do more, potentially, and provide greater deterrence? Yes, certainly. To do that, we have to address some of the failings and the gaps that were found in your report, but also in the day-to-day understanding of where we are.

Some of those gaps have been created by the very genuine and the right thing to do of gifting equipment from our inventory to our friends in Ukraine. We need to make sure that we are replacing that inventory, which I do not think was done at the pace that it was required to be done under the last Government. With the strategic defence review, looking at the capabilities that we need, is it a simple one-in, one-out approach? It probably is not. It is about looking at how we adapt our capabilities to meet those challenges and to learn the lessons of Ukraine.

That means that, when it comes to the shape of the forces that we are seeking to create, that will be informed by the SDR's approach, as well as by the daily practice that we are seeing in Ukraine, because that is a war being fought by a peer adversary. We can see the way that Russia fights and operates, and that gives us more information to be able to design a credible deterrent force against those, but that does involve working with our allies.

Q73 Emma Lewell: What I was driving at is that, in that report, we found that we are not ready for an enduring war. What has changed between that report and now? Would we now be ready for one?

Luke Pollard: We are making changes to the system of procurement. We are trying to remove the barriers and the obstacles, so that we can refill our stockpiles. We increased defence spending in the Budget last year by £2.9 billion, with an increased budget of 2.5% from April. That provides the resources to create the renewal of our forces, and is why one of the first actions that not just the MOD but the Government took was to commission the SDR to understand what shape our forces need to be structured in to get there.

There has been quite a lot of change in terms of fixing the foundations. I would also argue that one of the fundamental failings of much of the



HOUSE OF COMMONS

defence debate that I have seen when I was in opposition was an over-focus on kit and an under-focus on the people who serve.

Q74 Emma Lewell: To be clear, our report covered both. We found that we were not ready for an enduring war. Are we yet, or is there still work in progress? That is what I am trying to get from you.

Luke Pollard: We are still making changes. There is still work to do. We have to refill our stockpiles. We have to reform defence procurement. We have to value our people more. We have to fix a broken recruitment and retention system. Against all of those, we are making progress. The SDR will really help as a catalyst to show the future shape of our force that we wish to move towards.

Q75 Emma Lewell: We are not ready yet, are we, Minister?

Luke Pollard: We still have more work to do.

Q76 Derek Twigg: Does the MOD know what resources it has allocated to counter hybrid threats? Does it have any idea of what resources it has allocated, whether they are enough, and what the gaps are?

Luke Pollard: What do you mean by “hybrid threats” there? Effectively, anything below active kinetic activity could be covered by the definition of “hybrid threats”, and so we can point to nearly all of our budget being in that direction. If there are particular hybrid threats that we are looking at, the approach that I expect will be coming out of the SDR, and certainly one that the Secretary of State and I have spoken about a number of times since July last year, is that we need to invest particularly in increased homeland defence, which includes cable infrastructure. It includes cyber and digital protections, not just for the defence systems, but for the wider industry.

Some of that is an MOD responsibility, but some is also the responsibility of other Departments that we rely on to go and deliver greater effect. I would certainly want to see greater investment in some of those capabilities, but, as a broad bit, hybrid threats—or, as we regard them, state threats—are such a broad part of our budget and the response across Government. Would I like more money there? Yes. We are getting more money to be able to support that. On an individual line basis, we would need to look at the particular threat, the particular response, and the MOD role in countering that response to be able to give you a full answer.

Q77 Derek Twigg: Going back to your terminology in terms of state threats in the last five or 10 years, how have those become more of a difficulty in terms of resources that you have to counter state threats, and defence’s contribution to that? I get that it is a Government-wide approach, but I am just trying to get some sort of handle on, basically, where you are at in terms of being able to provide the resources that the situation is now demanding. You talked before about surfacing a submarine, and having the RAF involved and so on, which is fine, but, just as a matter of



HOUSE OF COMMONS

interest, how many operations have you been involved in in the last 12 months?

Luke Pollard: As a former Minister, you will know that I will not be able to give an answer to that last question.

Q78 **Derek Twigg:** I am not asking for the detail of what the operations were. I am asking how many operations you have been involved in.

Luke Pollard: I would not be able to give an answer on that one, because it would depend on what we mean by "operations".

Q79 **Derek Twigg:** You are not surfacing a submarine every day, are you? That is one thing out of the way. You may be, for all I know, but I guess you are probably not.

Luke Pollard: We try to keep the submarines out of sight, as a general rule.

Paul Wyatt: Costing against threats is incredibly difficult. It is something that we have tried endlessly, frankly, as a Government.

Derek Twigg: Yes, but you do not have the money.

Paul Wyatt: In some ways, focusing on costing against the capabilities that we need is a way that we can get after this in a way that has a bit more bite and grip to it. From a CT perspective, for example, our quick reaction aircraft are available to support air threats, but they are not there just for CT. They are there for state threats and they are there for the integrity of UK airspace, so costing against threats becomes incredibly complicated, and ends up with quite a lot of subjective judgment.

What we can absolutely do, though, is look at what capabilities we are offering to defence and to other Government Departments. Quite a good example are our counter-improvised explosive device and counter-explosive ordnance disposal capabilities. Those are available to deal with unexploded ordnance from previous wars. They are available to deal with IEDs that have a malign actor behind them, or a terrorist attack.

It is quite hard to attribute what threat they are really against, but we absolutely can understand what the Government want of us, which is coverage outside the M25, and the costs associated with that, so we tend to take an approach based on capability rather than threat.

Q80 **Derek Twigg:** One of the things that we are trying to get at is how much this area is now taking up in terms of the impact that it is having on defence's ability to provide resources, people and equipment. That is part of the reason for this inquiry. What I think you are saying is that you do not have really a handle on it, because it is all spread out all over the place and no one really knows. Is that what you are saying?

Paul Wyatt: It is our job to employ the force against a range of requirements. What we are saying is that we have a toolset that we use



against a range of threats, and they are not quite so niche or tailored to allow you to say, "That is for this".

Luke Pollard: What I would say, though, in respect of an answer is that there have been some very clear changes. For instance, the move of the British Army from being an expeditionary force fighting in Afghanistan and Iraq to now being much more orientated against a state threat—Russia—does change the force posture. It changes what kit and equipment we need in relation to that.

There are also newer technologies that we would need to develop, which would be different from what we perhaps had five years ago. If you look at drones and counter-drones, for instance, as a technology, that would certainly be a change from where we were in previous defence reviews. Certainly, if you look at the role of, say, misinformation—its pervasive nature in some contexts, and the malign actors behind it—that is a cross-Government response, but, clearly, MOD has a role within it.

Cyber would be another one where you would expect to see a greater investment required to meet the challenges, but also to reflect the fact that our people are in much greater demand as an industry, because the skills that our people have do not exist separately from the wider economy. Certainly, in terms of the high-end cyber skills that we train our people in, people can learn an awful lot in the private sector to deliver that. That has changed how we structure, for instance, some of those cyber responses to deal with the fact that the economic situation for our people has changed, as has the threat. Therefore, we need to restructure.

Because hybrid is such a large amount of Government activity, it is hard to answer particularly, but there are certain common themes where you can see a requirement for defence to invest more. My expectation would be that, when Lord Robertson reports, there would be areas where he would be making recommendations for additional investment to meet the iteration of threats that we are facing today.

Q81 **Derek Twigg:** That is even though we do not know what the investment is currently.

Luke Pollard: We know what our budget is currently.

Derek Twigg: Yes, we know that.

Luke Pollard: A Typhoon can be a response to a hybrid threat as well as a conventional threat. What underlines the difficulty of how this area is approached in public debate and your inquiry is the fact that you can count them separately. We could draw lines across it. That is an unhelpful approach to how we look at the capabilities that defence has. There are certainly more capabilities that we want to invest in to meet the threats that we are facing. The increased defence budget allows us to look at what those capabilities are once the SDR reports.



HOUSE OF COMMONS

Q82 Derek Twigg: You have described the aggressive action from a Russian ship. Are we too soft? Are we not being proactive enough in taking more action against adversaries than we do? We are always reactive rather than being more proactive. Could we be more on the front foot?

Luke Pollard: You have seen from this Government examples of where we are being more proactive.

Q83 Derek Twigg: Give us some, apart from the one that you have just outlined.

Luke Pollard: Yantar is a really good example of that.

Q84 Derek Twigg: We have that one, but what about others where you are being proactive?

Luke Pollard: I would also point to the broader area of UK leadership when it comes to Ukraine, because quite a lot of our counter-Russia activity has a Ukrainian flavour to it in terms of our support for Ukraine. This year, we are spending £4.5 billion, which is more than before, on our support for Ukraine. That is not just in ammunition such as 155 mm shells and other forms of equipment and ammunition. It is in the wider support packages that we provide to our friends there.

That is a stepping-up of UK leadership in terms of what we have seen over the past month in particular, alongside our French allies, in bringing together a coalition of the willing. The bringing together of that coalition has, you could argue, both a deterrent effect and a conventional force effect potentially in the future. There are absolutely areas where we want to step up.

Q85 Derek Twigg: I understand. Basically, if we found that an adversary had cut one of our undersea cables, would we go and do the same thing to them?

Luke Pollard: It is not always an eye-for-an eye approach.

Q86 Derek Twigg: Is it an option that the Government might consider?

Luke Pollard: In the event of any actions being taken against UK infrastructure, we would look at all the options that are available to us. One of the differences between the UK responding to a hybrid threat such as a cable cut and an adversary doing it is that we draw on different strengths than they do. Alliances are a key part of our response. The response does not necessarily have to be military. It could be diplomatic.

Q87 Derek Twigg: So we allow them to take out our communications but we would not take theirs out.

Luke Pollard: We would keep all options on the table in relation to how that works, but it does not necessarily mean that it is an eye for an eye. Certainly, there is a benefit in not being our adversaries in terms of the approach, but one of the strengths that the UK has in deterring some of these activities is that we are part of a strong alliance. We have exquisite



capabilities that we can use. The response that we would use may not be in the same domain as the initial activity—for example, public messaging, calling it out, and that affirmation of responsibility. We should not underestimate just what a powerful tool that is in our armoury. You would look at a broad range of options for any of those.

Q88 Mike Martin: I was struck, Minister, when you said that there has been a shift from an expeditionary military to one that is much more focused on Russia, European defence and all of that. As you know, we are still debating whether to send the carrier strike group to the far east. We hear interesting comments about the Red sea, which is where the risk is in that.

I would like to focus on something else, which is the opportunity cost of doing that. If we send that carrier strike group with all of the other assets—naval, air, and all the rest of it—it is a huge force package. What is the opportunity cost in the Euro-Atlantic security area? What is not being done here in our region because of that deployment?

Luke Pollard: Deploying the carrier to the Indo-Pacific directly supports our ability to protect the NATO area of operations in the future, because the key military purpose as to why we are deploying HMS Prince of Wales is for it to achieve its full operating capability, operating alongside other carriers of our allies that are in the Indo-Pacific. That is the key military reason why the carrier is being deployed.

In terms of the ability of that carrier to project power at any point on its deployment, one of the advantages of maritime power is the ability to move them around. At all times in any deployment, whether for the carrier strike group or for a single ship deployment, we retain the ability to move and deploy them in different manners. Those options that are provided by a fifth-generation carrier with fifth-generation fighters are quite considerable. It does not preclude options, but, at the end of its deployment, we will be able to dedicate a fully tested and operational carrier to SACEUR for its activities in the NATO area of operations from next year.

Q89 Mike Martin: What is the risk that the carrier strike group passes through the Red sea, does its deployment, and then the United States tries to extort money from us to provide the necessary protection to get the carrier back through the Red sea?

Luke Pollard: We have a very strong and deep naval relationship with the US.

Mike Martin: You saw the comments last night from very senior American politicians, including the Vice-President, about exactly this, and about getting the Europeans to pay for American security protection in the Red sea, which is the key choke point our carrier has to pass through. Is there a danger that our carrier will get stuck the other side of the Red sea and not be able to get back through that key choke point because the US withdraws its security guarantee?



Chair: We are seriously veering off topic. I do not want to get into the carrier strike and so on, and I do want to bring it back into focus. You have made your views known on this particular issue. Unless there is something else that you want to add, I want to move back to deterrence.

Q90 **Emma Lewell:** Just following on from my colleague Derek's questions, what we know is that, in the last six weeks, Russian ships have been in UK waters three times. Is our approach of deterrence working there or not?

Luke Pollard: It is in relation to what activities we are undertaking alongside those ships. To answer your question fully, we have to look at why there are Russian ships there. In many cases, they are there because they are moving equipment out of their Mediterranean ports in relation to Syria. Is this an escalation in Russian military activity deliberately designed to influence the United Kingdom? It probably is not. It is movement of their goods and equipment out of Syria.

Because there is a presence of a Russian vessel near our shores, what we have seen is a strong response not just from the Royal Navy, but from the Air Force as well, in being able to track and follow those ships, and to give the Russians no scope for doing anything other than transit through our waters. It is worth remembering that, as a naval power, we obey the international law of the sea, or UNCLOS, which allows nations to transit through international waters and our own waters.

Let us be under no doubt: the reason that we keep on-standby ships available to shadow Russian vessels through our waters is to be absolutely clear to those Russians that they have no ability to veer off to do any activities that we would not be able to spot and deter.

What we have seen in recent transits in particular is not just the Type 23 frigate HMS Iron Duke, for instance, shadowing some of those Russian vessels, but greater and more impactful presence of some of the P-8 maritime patrol aircraft, showing a greater presence against those ships and a clearer public communication message from the Ministry of Defence that, every time a ship has gone by, we have been identifying it and reassuring the British public that we are shadowing it and thanking those forces that are doing it. That is different from where we were perhaps a few years ago for similar Russian operations.

Q91 **Emma Lewell:** In what other ways can defence use deterrence to counter hybrid threats? That is one example. What other ways are there?

Luke Pollard: It depends on what you mean by "hybrid threats". Again, I am sorry to take you back to this broad thing, but, if you were to look at, say, the Russian shadow fleet, that is a good example of how an HMG-wide approach, including Ministry of Defence analysis with our intelligence partners, can identify which ships are in the Russian shadow fleet, because it is not always easy to tell from the first point of call, to publicly call them out, to then sanction their activities, and to prevent their access to certain ports or to certain international activities.



That is directly deterring Russian aggression, because it is directly affecting the revenues that the Putin Administration receives from the illegal sale of oil on the international markets, for instance. If you look at that as an example, increased activity against the shadow fleet has a direct effect and provides support for our friends in Ukraine by choking off some of the revenue that the Russians would receive from that activity.

That is not necessarily a conventional deterrence, but it is an example of how across HMT—FCDO, MOD and our intelligence partners—we would be able to bring together that analysis to have an effect that we are looking for.

Q92 **Emma Lewell:** Just to expand it a little bit, the territory that Russia seized with its bite-and-hold operations in Georgia, Moldova and Ukraine has so far proved impossible to recover. Should the UK enhance our deterrence by denial by forward-deploying more military capabilities to deter Russia from crossing the threshold from hybrid into armed conflict?

Luke Pollard: I might bring Paul in here, because it is an area that he spends a lot of time working in. If you look at the forward land presence that we have already in Estonia, for instance, as a NATO partner, and with NATO partners operating across the Baltic states, with Finland and Sweden also now being part of NATO, the new regional plan that covers that part of the world, hubbed out of Norfolk, allows us to have not just a UK presence in Estonia but a greater integration with the presence of our allies in Latvia, Lithuania, Finland and Sweden, and across the High North.

There is a real benefit to our forward land presence in Estonia, not just for the Estonians, but for the UK's security as well. That is probably a really good example of conventional deterrence that also allows a forward presence for the UK to conduct information discussions and to show our support for our NATO allies, because the visible support of that presence makes such a big difference in terms of reassurance for our allies in that area. Certainly, having the Prince of Wales—the person rather than the carrier this time—visit Estonia only last week is a really strong sign of our commitment to that Baltic states security but also that of the wider region.

Paul Wyatt: The Minister is absolutely right. This is something that we do not do unilaterally. We do it very much multilaterally in the context of NATO planning and a combined multilateral NATO endeavour. We have French forces alongside us in Estonia. We have other major NATO nations in the Baltic. From our perspective, as the Minister said, we have a NATO-first approach. It is about understanding what the demand is from NATO and from SACEUR, and how we play into that in terms of their plans for adequately securing the NATO area.

The other thing that we do now, and expect to continue doing, is the air policing role that we conduct in the Baltic and indeed in Romania. It is not



just a land forces deployment that we play into this space, but also security of the airspace. The straight answer is that it is something that, of course, we would consider, but, in a multilateral context, the force lay-down is very much a matter for NATO and for the NATO commanders, and we support that.

Q93 Alex Baker: You have already touched on this, but I would really like to focus on cyber-space, if you do not mind, which is increasingly a part of hybrid operations that we have been talking about. What role can defence play in deterring and countering cyber-attacks?

Luke Pollard: It can play an increasingly critical one. If we take a step back, the UK is under continuous cyber-attack from malign actors worldwide. Defence has a role in particular in terms of deterring and supporting certain systems that are critical to UK security. We operate in conjunction with the National Cyber Security Centre. That is a brilliant resource, and a model that has been copied worldwide, in terms of how we work alongside industry, the private sector and, increasingly, the third sector, due to a lot of attacks on charities that we are seeing, to make sure that we can increase our cyber-resilience.

Going back to the question from Fred in relation to deterrence by denial, because we are a country with high levels of cyber-resilience and of cyber-expertise, it makes us a less favourable target for some nations to come after, but we should be in no doubt that the level of cyber-threats that we face as a country, both on defence networks and in the wider civilian population, are considerable.

That is why some of the developments that we have made in recent years are so important. The standing up of the National Cyber Force is a good example of how, given that it is not owned just by the Ministry of Defence, we can now create cross-Government expertise that builds on the very best of our colleagues over in GCHQ and the wider security apparatus to look at defensive cyber as well as the ability for us to conduct offensive cyber, should we need to.

Q94 Alex Baker: You are confident right now that we have the right people and the right skills to be able to counter the threats that we face.

Luke Pollard: We need more people and more skills. It is for that reason that we launched the direct entry cyber pathway only a few months ago, because we know that some of the skills that we need in cyber are, by their very nature, different from some of the warfighting skills that we might need on the frontline. We changed, for instance, some of the medical and physical requirements, which would be different for someone entering the cyber force on the direct entry pathway rather than, say, a usual entry into the Army, Navy or Air Force. This was deliberate, because we want to attract different people with different skills into that area.



One of the other areas that makes not only cyber but also, for example, 77th Brigade in the Army different in this respect is that we need to look again at the mix of regulars and reserve. In a traditional military lay-down, you would expect nearly everyone to be a regular, with top-ups of reserves on a rotational basis, or as operational needs require.

That is different in cyber, because we know that the high levels of wages that I mentioned earlier mean that our people are in heavy demand in industry. What we can offer in the Ministry of Defence, especially in some of our forward-facing cyber units, is a sense of purpose, mission and contribution that is different to the level of pay that someone can receive. That is why, increasingly, we are seeing more reservists in those units—indeed 77th Brigade is two-thirds reservists—which is a very different personnel mix than you would see in a conventional military unit in any one of our single services.

It is that type of adapting our systems that we are going to need to do to make sure that we keep our people, but also allow them to have careers that do not produce a cliff edge. For far too many of our people across defence, but especially in areas of incredible high demand for their skills, it is very binary: you are in the military or you are not. We need to move to a greater continuum of service, which does mean adapting some of the legislation—and you might see that in the Armed Forces Bill next year—where we are removing some of the cliff edge moments, which will enable people to transition from serving in uniform to serving the nation in the private sector, in what might be very similar roles, especially because cyber is supported by many private sector partners.

The model of allowing the transition back and forth between regular reservists and the different types of reservists is incredibly effective in getting the people we need and retaining them over the course of their careers, while still enabling them to gain new skills and experiences outside military service and bringing that benefit to our armed forces. If we exist on a very simple cliff edge, whereby you are serving or you are not, we will lose those people and that expertise, and our country will not be as safe as a result. That is why that new model is so important, and why we are adopting it at pace.

Q95 Alex Baker: That sounds like a really sensible approach in terms of where we are at now, but this is a fast-changing environment. Having worked in the private sector, I know how important that skills pipeline is and how you do that planning. You have very eloquently talked about how this is a cross-Government approach and that it is not just the MOD. How are you approaching that skills planning piece and making sure that we have the pipeline of talent to face whatever is coming at us in the next decade?

Luke Pollard: There is no doubt in my mind that the MOD needs to do more to recruit and retain people. In many cases, that is about making people aware of the incredible opportunities that a career in service and the armed forces provides, and we have not told that story well enough.



We also need to work with our cross-Government colleagues, and especially the Department for Education and its equivalents elsewhere around the United Kingdom, to encourage people to be aware, from an earlier basis, of the opportunities and the skills requirements. How do we get more people excited about maths, science and engineering, which are precisely the bedrock skills that will be required? It is amazing how many young people are now involved with coding, which is a direct skills development that we could really benefit from in terms of cyber and some of the other advanced technologies that we need. It is a whole-of-Government effort, but defence is certainly doing more, and will need to continue to do so.

Q96 Mr Bailey: I am interested in the integrity of our Article 5 response. Sir Alex Younger, a former head of the SIS, told this Committee of the “grandmother’s footsteps nature of the hybrid threat, which is all about slowly increasing harassment or subversion and normalising a new situation”, which could result in the blurring of previously robust red lines around security. My personal analogy would be that used by the scientific adviser providing advice to Minister Hacker and the Russian approach to using salami-slicing techniques to slowly gain ground.

In that regard, I could not resist writing down a series of escalations and wondering where our Article 5 response would be. Spy ship off our coast—do we push the button? Cutting subsurface cables—do we push the button? Drones at a US air force base—do we push the button? Attributable violent attacks on mosques and Muslims—do we push the button? Fostering antisemitic behaviour—do we push the button? Damaging our critical national infrastructure—do we push the button?

To take you back to the original question, how can defence counter threats to ensure the resilience and integrity of our Article 5 commitments? Does our defence policy adequately address this?

Luke Pollard: It is always good to get a “Yes, Minister” reference into a question, so well done on that. I have not experienced many “Yes, Minister” moments as a Minister yet, but I am sure that there will be plenty more in store for me.

What I would say is that our commitment to NATO is unshakable. It is important to understand that the Article 5 moment, certainly in conventional terms, is not necessarily triggered by, say, a Russian tank coming across the border. It is triggered by a decision of the North Atlantic Council that that represents an Article 5 moment. From 2016, NATO has decided that a hybrid threat, or a cyber-threat in particular, could be considered an Article 5 moment if it meets a certain level of severity.

The challenge around that is that all Article 5 moments are context-specific and would need to be decided upon at a political level, on the recommendation of where NATO would be. It is absolutely vital that we maintain that Article 5 unity among our allies that an attack on one is



HOUSE OF COMMONS

attack on all, but it is also true that, increasingly, NATO allies need to look at hybrid threats and their reaction to them as part of collective defence. Effectively, being resilient against a hybrid threat needs to be viewed as part of your Article 3 commitment on ensuring that you, as a nation, maintain the adequate defences, so that you can contribute to the security of the overall alliance.

Although the definitions and terminology will vary across the alliance as to what we mean by hybrid and cyber threats, we are seeing a commonality of approach and increasing co-operation. On cyber in particular, we are fortunate, as a nation, that we have some of the very best cyber-operators, both defensive and offensive, in the alliance, but we also have deep partnerships with our allies, especially those on the eastern flank for whom hybrid threats are a much more common everyday occurrence, because of the proximity of Russia, which allows them to have greater freedom and a greater range of options available to them than further into the alliance, as we are in the UK.

In terms of the challenge about what represents an Article 5 moment, can a hybrid threat be there? Yes, certainly. It is about severity. I would also stress that I cannot imagine a scenario where a conventional Article 5 moment is not accompanied by sub-threshold state threats and, immediately before that, actively deploying them alongside, in parallel, any Article 5 conventional moment, as we might traditionally have considered it.

In that respect, our deterrence needs to be both a conventional one, but also one that meets an understanding of where they come from. A challenge in that, for all NATO members, but for the United Kingdom in particular, is identifying what those are. You can identify the steps on that process, which goes precisely to the point of your challenge around at what point you would do what.

If you cannot identify and, importantly, attribute them—and the attribution is a really important capability that we have shown that we want to do—you might not be able to see the path that may take you there and would allow us to put in measures to deter that. It is certainly in our interest to deter aggression rather than to necessarily have to defeat it, but to be able to identify and attribute it is an important part in the steps towards that genuine deterrence that we need.

Q97 Mr Bailey: Before I allow the DG to add any comments, we are trying to gather evidence, and I am trying to take you on a path so that we can inform our report, rather than just clips for social media. It is quite important that we go on that journey, and I will come on to attribution separately, because that is the second half of my question. The important thing that I would ask us to perhaps take away is your acknowledgement that an Article 5 response is primarily a political response.

Paul Wyatt: It is a political decision. The response itself can take any number of means, and may well be very military. The Minister has



covered it, but it is probably worth just coming back to definitions, which we talked a bit about earlier. The nature of hybrid, grey zone or whatever you want to call it is an adversary seeking to do us harm, generate coercive effect, and generate advantage in a manner that they judge is below the Article 5 threshold, essentially. That is one way in which we could describe what you are talking about.

That makes answering this question a bit difficult, because you will understand that we do not want to give the adversary too many hints as to how far they can go. It is absolutely the case, as the Minister has highlighted, that there are examples of attacks that would have been considered hybrid and non-warlike in the past, such as cyber, where NATO has been very clear that it considers that that kind of attack, at a scale, would merit consideration as an Article 5 response, and we have been very clear on that.

The other thing that I would observe is that, curiously, perhaps, the only time that Article 5 has been invoked was in the context of what, in some ways, could be described as a hybrid event. It was a terrorist attack, but one with a connection to a degree of state sponsorship. Our subsequent military campaign in Afghanistan was directly as a result of that attack, and in the context of NATO invoking Article 5, so this is not an outlandish proposition. We have, in recent observed history, used Article 5 to address a hybrid event.

Air Commodore Bressani: From my perspective, to answer your question, "How can defence counter that threat?" it all comes back to the deterrence message and the traditional four Cs of credibility, capability, comprehension and communications. Defence has recognised that there is a fifth C there, which is competition, and that is pretty much everything that we have spoken about this morning in terms of being ready and able to compete across all domains whenever the need arises.

Does that mean that we can see every threat that is coming all of the time and that none will get through? That is unrealistic, but we need to be as well prepared as we can be. Of course, all of this needs to be underpinned by understanding and our intelligence picture, but, as long as we can do that to the best of our ability, that will put us in the best place to make sure that we are that credible deterrence.

Q98 Mr Bailey: To follow on from where you took us, Minister Pollard, the second part of my question that we would like some understanding of is on the things that you consider you would respond to, although we understand that we would not necessarily want to publish those. It is just important for us to have a semblance of an idea of what they would look like. We also want to understand what the attribution mechanisms to prevent escalating tensions are, so that we can maintain the integrity of an Article 5 response.

To come back to a point that you made, Director, which was about doing us harm, the head of MI5 warned in October last year that Russian



HOUSE OF COMMONS

intelligence had been on a mission to generate sustained mayhem on British and European streets, and I would describe that as harm. Within my constituency, *The Guardian* put out a very well-sourced article about a network of Telegram channels, not with US personnel in them but with Russian links, encouraging UK residents to commit violent attacks on mosques and Muslims, and offering cryptocurrency in return. In 2024, we saw the attribution of Russian FSB agents to the antisemitic graffiti campaign that was seen across France. In March 2025, Russia was accused of starting the IKEA store fires in Lithuania.

To come back to the harm and the need for attribution, how can we improve our attribution mechanisms, for instance, in order to counter these escalating tensions?

Luke Pollard: The first thing that I would say is that we have a lot of examples in recent history of a very effective attribution system working. If you roll back to the Defence Intelligence briefings that were made public in the run-up to Russia's illegal invasion of Ukraine, they were deliberately designed to counter the Russian narrative that they were not planning to invade Ukraine, with the very clear evidence of the build-up of Russian forces and the very clear intelligence of the conversations.

The ability to attribute, declassify and communicate that intelligence, thus becoming just information, is a really clear example of how using the assessment tools that we have across Government, including our intelligence partners, owned by Government Departments and the Defence Intelligence part of the MOD, we are able to call that out. Across recent years, we have had, in the cyber domain, for instance, the attribution of Chinese state-backed hacking and a cyber-attack on the Electoral Commission to undermine our electoral integrity. We have seen activities that we can, with our allies, attribute to Russian actors taking action against our allies, especially those in eastern Europe.

The system that we have of attribution works very well. The big difference between intelligence thinking, "We think it's them. We have the evidence. We know it's them", and then the decision to say, "With that, we are going to put it in the public domain and clearly attribute it to them", is a confidence piece about building the credibility of our intelligence systems, as well as directly countering the misinformation and the malign activities of our adversaries. We have that system.

Increasingly, one of the bits that I would like to see more of in the hybrid space and in the nexus of cyber-intelligence and some of the sub-threshold activities that may be further away from the conventional end of that spectrum, given that it is a continuum that we are looking at here, is the greater joining up of our systems across Government. We have good operations that already join us up.

To the point that I made earlier to Mike, the Cabinet Office and some of the functions that sit in the convening part of the centre of Government are really good at bringing together intelligence across Government to be



able to have a full picture. The intelligence from one part of our system may not provide the full picture, and that collaboration that our people do on an increasing basis in an integrated manner is so important to providing the foundational information that we need to make an attribution.

That is working, but we would like to do that more, and we would like to integrate especially some of these services across Government in an increasing way. That is behind the broad approach that you are seeing across Government at the moment in terms of how we bring together our capabilities to deliver effect, with attribution being one of those.

Paul Wyatt: As the Minister said, there is the integration of our assessment activities. The Chair of the Joint Intelligence Committee and the Joint Intelligence Organisation is sat at the top of an assessment community, which includes the intelligence agencies and Defence Intelligence. Bringing all of that together to provide the best possible picture is a really key part of the way in which we address these issues and allow other agencies, such as the police, the National Crime Agency and others, to harden the environment. It is that kind of information that allows that hardening, as well as communications with allies.

On some of the threats that you have outlined, in particular those that were outlined by the DG of MI5, you will not be surprised to hear that we talk a lot with our allies around what we and they are seeing, so that we can mutually harden each other's endeavours. From a narrow defence perspective, Defence Intelligence are right at the forefront of that and provide a really important contribution to the wider assessment efforts that we can really understand and enact.

Q99 **Mr Bailey:** I am glad, director general, that you pulled on those remarks. The examples that I have given you are of our head of our intelligence services narrating what is happening to us in a way that we can attribute ourselves, perhaps not directly, but in a hybrid method. I note that there have been some very powerful reports from the State Department about the Kremlin's use of antisemitic propaganda. There was a very in-depth report that it released last year. Is this perhaps something that our intelligence agencies or broader Government need to do to address, tackle, identify and counter in terms of things such as the very obvious use of Telegram in the violent attacks that we saw on Muslims, our Islamic communities and mosques earlier in the year?

Luke Pollard: The work that the Home Office has conducted with its own strategic security review delivers much of the intent that you are after in that respect. One of the challenges that we will have once the SSR and the SDR report is how we can create a more integrated model with a greater clarity and fidelity on the threats that we are facing. It is certainly true that, across the security apparatus of Government, there will be some that will focus on domestic threats and others on international ones.



Let us also be clear that, in many cases, we are seeing state-based activity engage a network, which includes both international and domestic activity. The idea that you can easily stovepipe it, as we might have wanted to in the past, in our description of our activities is much harder now, because of the complexity of the activities, but also the geographical reach of them. We are seeing, for instance, malign activities around North Korea engaging in different types of hybrid activities than perhaps the Russians do.

Our approach needs to be alive to the broad range of threats that we have, and sometimes how those threats interplay together, as well as our ability to call them out in terms of the hateful misinformation that may exist online, and understand where it is coming from and how you address that in terms of a UK context as well as in terms of interference with an election overseas, for instance. We need to work with our partners to be able to challenge some of that, but the ability for us to collect that data, and to work with our allies to interpret and analyse it properly, is a real strength that the United Kingdom has, and is certainly something that our allies really benefit from and have a respect for the UK's role in.

Chair: Thank you very much, Minister. I just want to move the conversation from defence's role in deterrence to issues around a whole-of-Government approach.

Q100 **Lincoln Jopp:** I am tempted to say, "Thank you, Mr Hacker", but I will not. We visited the National Cyber Force and Strategic Command. At one stage, there was the phrase "Whitehall customer group". This question is about our own grey zone within Whitehall. If bad guys attack NHS IT systems, that is the defensive play part of the national cyber strategy. Can you just talk us through a bit of the governance around the offensive reaction?

To come back to Derek's point about, "Do we go and clip their cable?" without going too far into the out-of-bounds box, it is not a Department of Health function to want to go downrange and do bad things to the King's enemies, but it is in ours. Does that mean that defence plays more of a role in that customer group when it comes to offensive?

Luke Pollard: The work of the National Cyber Force is incredible. By its very nature, NCF is cross-Government anyway, because of the sponsorship by a number of Government Departments. It is worth saying that, before you get to any point of looking at what the offensive cyber action is, there would be the understanding of what has happened, and then the attribution to an actor. That may not necessarily be the immediate actor that took the offensive cyber action against us, but who commissioned and paid for it, and the whole system that may come from it.

What we do with that information does not necessarily always mean a tit-for-tat approach. One of the strengths that the UK has is that we have a



HOUSE OF COMMONS

range of measures within our toolbox that allows us to calibrate what the right response is, both on a deterrence point and a restoring order point in terms of where we get to. In the example that you use, I might ask Matt to give the approach of what would happen in that scenario.

It is important for us to realise that we are not our adversaries, so our approach to how we deal with those would be different from how they would calculate an approach towards the UK in the first place. That does not mean that that approach is any less strong or determined, but just that it may take different forms than the initial attack on our systems.

Air Commodore Bressani: All I would add to what the Minister said is that, of course, the reaction does not always need to be in the same domain either. Just because it is a cyber-attack, it does not necessarily mean that a cyber-reaction needs to take place. As the Minister has already said, we will take all of that information and work out the best reaction to it.

Going back to your specific question about the Whitehall customer group, though, within the cyber domain, that is, essentially, a prioritisation group. All Government Departments can put in what their cyber priorities may be, and the correct level of Government can decide where the resource of the National Cyber Force can be aligned to over the course of a set period. It may sound like quite a transactional group, but it is a prioritisation mechanism to give the National Cyber Force its priorities from a cross-Government position.

Paul Wyatt: If I can just offer a couple of examples in that space, you will not be surprised to hear that we are a customer. Our Home Office colleagues are as well. As an example of operational activity that the NCF has talked about conducting, it has a responsibility, as part of the Ministry of Defence's command and control system, to deliver cyber effects in support of operations—some actively, but mostly in the contingent space, just as you would expect from the Navy, the Army and the Air Force. In the event of something occurring, we expect the response to be across all five domains. We ask the commander of the NCF to be ready to contribute cyber-effects in support of military activity.

In terms of things that we have talked about in the past as a Government, the Home Office has asked the NCF to help it in terms of child sexual exploitation and internet site takedown. There is a legitimate conversation about how much relative time they spend doing one or other of those two things, and other demands that come from other parts of Government.

Q101 **Lincoln Jopp:** I am glad that you said that last bit, because the way in which we have been talking up until now suggests that the hybrid activity stops when the war goes hot. It seems from the outside that, in a period of relatively low military activity for the last 10 years, defence has side-slipped into this. It is unerringly can-do, has some great people and has developed some capability. We are briefed that it is going to get bigger



and bigger. There is clearly a temptation, when you escalate up to conflict, that all your ploughshares get turned into swords again, because that is what you are really there for, but this is not like that, is it? The hybrid operations must run alongside the kinetic ones in any future conflict.

Luke Pollard: I agree. One of the bits that you will see more from this Government in terms of prioritisation is our approach on all-domain warfare as distinct from looking at a particular domain and the effects that can be achieved in it. If we want to have the kinetic effect on a target, whatever that may be, that will probably not be able to take place without all domains contributing something to the delivery of that kinetic effect. That will include space and cyber, as well as the capabilities of individual services as well as the joint environment to be able to deliver it.

An understanding about how we deliver effect now means that, by default, any offensive and, indeed, defensive action is integrated. It does cover all domains by default and, as part of that, we need to make sure that the systems that interplay between those domains can speak to each other and understand the prioritisation and their immediate involvement in delivering that effect. I talk quite vocally about my dislike of multi-domain integration as a concept, because it is a journey. All-domain warfare is a destination.

Q102 **Lincoln Jopp:** I am sure that that phrase meant a lot to you when it came out of your mouth, Minister, but I am a simple soldier.

Luke Pollard: I do not believe that for a moment. Multi-domain integration is about how you get the different domains working together. How do you integrate one domain with another for a particular thing? That is very much necessary and immediate, and a given for all our activities. We have gone from, "How do you integrate one domain with another?" both on a theoretical basis—"Should we? How do we do that? Do our systems work together? Do our terminologies work together? Does the digital backbone that sits behind it work together?"—to it now being all-domain by default for all UK military operations. That changes how we piece together our ability to conduct operations. It means that, for us to have effective operations, we need all parts of our military system understanding and co-operating together.

To Derek's question earlier, it also makes it harder for us to cost the individual effect, because you are now, effectively, drawing from across the entirety of the UK armed forces—and, indeed, sometimes our allies and partners—to be able to deliver that effect, rather than just saying, "A plane took off. It dropped this bomb. It flew back. It took X amount of fuel, X amount of wear and X amount of staff time in order to piece it together". Delivering that similar effect now will involve space, cyber and maritime forces, and joint command in doing so. It will involve all domains.



That does mean that how we structure and how we operate needs to change. It also means that how we respond to hybrid as well as conventional challenges needs to be reflective of the fact that we can now draw on the very best talent across all our armed forces as standard. That improves our lethality and our response time, but also means that we are not locking ourselves out of options that might otherwise be available just because we do not have one bit of the military with the connections to the other bits. That is increasingly why our joined-up commands—PJHQ at Northwood, for instance—play a critical role in choosing the best parts of all our military to deliver an effect, whatever that may be.

Q103 Michelle Scrogham: On the Committee's recent visit to Finland, we saw how their security committee and the MOD work and co-ordinate long-term across Government planning so that they can better prepare society to be able to counter hybrid threats. Is this something that the UK should be emulating?

Luke Pollard: I was in Finland the week after the Committee was there, meeting Ministers to talk about our mutual support for Ukraine. The context of Finland really has to be understood. Until it recently joined NATO, it was very proud of its independence. Because of its proximity to and experience of Russia, it has taken a very different approach to a whole-of-society approach. That proximity drives different behaviours, but also different assumptions from the public about what their responsibility is to national defence, what their obligations are, how they will be taught in schools, what their role is in terms of experience with the military and, in the event of conflict, what they do, which is different to how the UK has traditionally acted.

Certainly, there are things that we can learn, not just from Finland, Sweden and the Baltic states, but also from Norway as a longer-standing NATO member, for instance, about how we can create the links between society and be clear about what the threats are and what we need from people to be able to do it.

As an example, as we touched on earlier, our lay-down structure of reserves does not meet the moment right now. That is something that we are looking at as a Government to reflect in the event of us needing to draw on that wider pool of people who exist within society with military experience. How do you do that? Finland and our Baltic allies have a much clearer and more operationalised versions of those. Some of those are learning from the experiences of our allies. Others are getting our house in order in more difficult times. Reserves is a good example of that.

Finland, the Baltic states and Nordic colleagues have civ-mil options in terms of their industrial capabilities, but also their national infrastructure such as airports and maritime ports. That is different from how the UK has historically been structured in recent years. The challenge that we have to have is that it is not a model that you can just pick up and run



with, because the context is very different, but there are certainly lessons that we can learn.

My experience of the conversations that I was having on my recent visit to Finland precisely around this area was, "What conversations do we need to have with the British people in the first instance?" That is about clarity about the threat that we face and what we can do about it. A knee-jerk reaction would be unhelpful and also not necessary, but it is about a greater clarity about what the threat is, why we are investing in defence and, if we are investing in defence, how we do that.

I mentioned earlier an intent to spend more money with SMEs. That is not just a good growth reason because it creates jobs in our community, but is directly supporting a resilience option. One of the key bits around the Finnish model is a greater national resilience.

Q104 Michelle Scrogam: This is exactly where I am heading with this. It is more about the whole-of-Government approach and the resilience within our communities. In one of their evidence sessions, our predecessors were looking at the fact that 90% of what will be on the internet in 2027 will be fake or false. It is about the resilience in our society to be able to combat that, to understand it, and to be able to take it that apart and realise what is and is not fake. Have Government done enough on that, or is that something that we could learn from, again with a whole-of-society approach in terms of how we counter the hybrid threats?

Luke Pollard: I do not think that any Government worldwide has got this right yet. Certainly, if you look at the progress that was made with the last Government's Online Safety Act, notwithstanding the big holes that, as a party in opposition, we were highlighting, it did highlight that there is misinformation online. There is a responsibility on individuals to be able to call it out. There is something about how, as an individual, you identify misinformation, and how, in terms of participation in structures or workplaces, we prevent that information being shared more broadly.

Also, what is the responsibility of the platforms where the information is being shared? One of the roles that the UK has, as a nation that is proud of its democracy and of its adherence to international law, is how we make a case against misinformation that is true to those values. We are certainly seeing malign actors flood our social media with misinformation, sometimes deliberately targeting a community, a demographic or an event with a piece of sustained content. We are also seeing just a general fuzziness of the information picture.

There is a benefit for our adversaries in eroding trust and confidence—not necessarily saying, "Instead of having view A, move to view B", which may be in their interest, but just confusing the picture so that people cannot distinguish between the truth or credible information being shared by reputable sources, and disinformation and eroding confidence in the sources that will be providing credible information.



That fuzziness of that picture, and the 97% figure that you mentioned, is a real challenge that we need to address. Our role as defence is only one part of that bigger HMG approach. That does mean, for instance, greater responsibility of DSIT in that picture. Many people—including many parliamentarians, I suspect—will understand how critical their role is, as well as this. That is why that whole-of-Government approach is vital.

Q105 Michelle Scrogam: It did appear in Finland that it was a whole-of-Government approach with education and DSIT, and all of those joined up together. That is why I was asking whether this is something that we should be emulating. The threats that they face in Finland are somewhat different from what we face here, but their approach to it would seem very well-rounded.

Luke Pollard: Broadly, this Government want to see a whole-of-Government approach to our national security in all its facets, and a whole-of-society approach in how we deliver it. It is one of the reasons why, in making the case for increased defence spending, you will notice the Defence Secretary, the Prime Minister and me, in our media interventions, spending more time, in many cases, talking about procurement, industry and jobs than necessarily about which bits of kit or capability we are buying. We need to make the case that increased defence investment has a benefit that is not just in the abstract deterrence place and buying weapons systems, but about underpinning economic wellbeing for our entire nation.

When the Prime Minister speaks about national security being part of national renewal, that is absolutely about keeping us safe, but also about how people can feel part of that broader endeavour. If you were to take a hybrid threat that every single person in this country could do something about on cyber, and everyone updated their operating systems on their phones and laptops, this country would be enormously safer. That is not an MOD responsibility. We update our systems. In fact, we are very vicious about updating our systems, as I sometimes know when I try to turn on my phone. It is really important that we do that, and we take that seriously.

If everyone did that, it would reduce the opportunities for malign actors to be able to exploit systems, to be able to rip information from people, to be able to place things on people's phones, or to do whatever they may want to do. That is something that requires a whole-of-society approach, but it does mean that everyone needs to know why it is not just about getting the latest feature on your operating system when you do it. There is a security benefit for that individual, their data, their information and their finances. It also speaks to a small contribution that everyone can make to our wider national security picture.

Q106 Michelle Scrogam: What are Government hoping to achieve from their home defence programme?



Luke Pollard: We need to be safer. We need to create greater deterrence. We need to support our allies in doing so as well. Those objectives are entirely consistent with that NATO-first approach, which you have seen outlined since July last year, of us working to support our partners.

There are also a lot of people who are generally concerned about the world out there at the moment. One of the key jobs of the Ministry of Defence and of Government is to provide our people the confidence that we have good people, with the right equipment and the right approach, and the right friendships across our international space to keep ourselves safe, and to recognise that our security depends on the security of others as well.

That is a big mission. Certainly, I have been quite struck by just how many of our international friends are looking for British leadership, especially at this time. They are seeing it in what the Prime Minister is doing in relation to Ukraine, but they are also aware that, just as President Trump has correctly asked Europe to spend more on defence—something that, to be honest, America has been saying for a very long time—Europe needs to step up. We need to step up, and indeed we are with increased defence spending.

How we spend it and how we create a force across Europe that is more than the sum of its parts, where we are genuinely interoperable and interchangeable, and where our deterrence function is stronger and is underpinned by the popular support of each of the populations in every NATO member country, creates a much higher deterrence against Russian aggression than we can achieve if we just spend money and keep that defence spending within our own boundaries in terms of where we put our kit, equipment and people.

We have a big challenge to meet, but the approach that we are taking in having some of the early conversations about what a whole-of-society approach is will help us with that. I would much prefer a whole-of-society approach that shows a benefit for people engaging, serving in the armed forces and looking at their businesses' technology. There are loads of businesses out there that will not think of themselves as a defence company but could be making a substantial contribution to not just their bottom line by doing so, but to our national security. That is a broader conversation that we have to have.

Q107 **Lincoln Jopp:** Listening to you talk there, Minister, it strikes me that we have a bit of a problem in as much as our messaging is not quite as clear as it could be. You said that it would not be helpful to come in and tell the people that they are under threat, because that would be counterproductive. Equally, you want to take the public with you. You are clearly walking a very delicate line in terms of what you are saying about Russia. There are deliberate attacks on our information space to inject some doubt into people's minds as to whether they are a bad guy, and



the last 24 hours have not helped. I will just put it like that.

Without putting you on the horns of a dilemma or asking you to pick sides, would you like us, as a country or probably as a Government, to just dial up a little the threat perception in the minds of the people of Britain?

Luke Pollard: We are already doing that in being clear with the British public about what the threats are that we are facing, and to be able to marshal that in a clear way. That is why we commissioned the SDR. When the strategic defence review reports, it will set out a clear assessment of the threats that we are facing as a nation. That will contribute to that national debate as to why we, as a Government, are spending more on defence, the reason behind those decisions, and why we are doing it in a way that can benefit more people.

What we need to do is be very aware that, in all these debates, all parliamentarians, on a cross-party basis, are making the case that we live in more difficult times. They use different language and approaches, but there is cross-party agreement on that. What we have to do is find a way of taking the public on that journey with us, because there will be actors that are seeking to deliberately undermine confidence in the voices of myself as a Minister, the armed forces and our Ministry of Defence, just as much as they will of individual politicians who make that case as well, so we still have a lot of work to do there.

Q108 **Jesse Norman:** Mr Wyatt, this is the strategic defence review that we have under way at the moment and has just been filed. In the recent past, we have had strategic defence and security reviews. You are the director of security. Is there any difference between an SDSR and an SDR, or is it just that someone forgot the other words?

Paul Wyatt: Yes, there is a difference. The strategic defence and security reviews—and, indeed, the integrated review—were whole-of-Government endeavours focusing on aggregate national security. I was fortunate enough to be part of the defence team that did the SDSR in 2015.

The SDR that we are currently conducting is a defence-led activity and is looking particularly at defence capabilities and issues. It is doing so in the context of other reviews, such as the security review that is being led by the Home Office, and it will be brought together by the Government into a single and coherent picture, as the Minister described earlier.

Perhaps to slightly anticipate your question, “Why an SDR?”, I will offer a personal view. A series of SDSRs and integrated reviews did a very good job of addressing national security, but there is a particular issue around defence reviews, which are able to get more fundamentally at the full structure and posture of the armed forces in a way that we are perhaps tempted to gloss over or not get into quite such depth when we are thinking about national security.



The SDR conducted by the review team and led by Lord Robertson will have and has had the ability to get into some really deep conversations with our military capability people and the single-service chiefs to think fundamentally about the frame of the armed forces at a depth that we probably would not have been able to do if we had simply been doing a national security review.

Q109 **Jesse Norman:** That is very helpful. So we, as parliamentarians, should expect an SDR that is much more tightly focused on force structure, deployment and the kinds of deep issues that you have described, however much of that is put into the public domain or kept privately within Government.

Paul Wyatt: It absolutely allows us to have that deeper consideration.

Q110 **Jesse Norman:** What you are saying is that that is the point of it, in part. Given all of the concerns that we have heard expressed about the need for a whole-of-Government review, and all of the different issues about attacks on critical national infrastructure, which could be extended to lawfare, weaponising migrant flows and all those other things, why was it appropriate to ignore those things from within the wider defence context, which is what we are really considering?

Luke Pollard: That is probably one for me rather than the official, if I may. I do not think that we are undertaking that perspective as you present it. On the counter view, we are having a clear focus on our defence structure. It is beyond doubt that the war in Ukraine has changed the way that we think about conflict and the way that we would fight a conflict, based on the experiences that we are seeing, if only because our doctrine does not allow for the pervasive nature of drone warfare in the way that we are now seeing in Ukraine, so there does need to be a change in our broad approach.

The other difference between the SDR and previous iterations of defence reviews is that it is externally led. Having someone outside of the Government apparatus leading and following the path that they wish to go down, delivering against the terms of reference set by the Prime Minister, the Chancellor and the Defence Secretary, has been very helpful in shining a light on the bits of the military that sometimes the military might not always want a light shone on, especially when we are approaching it from a situation where, on a cross-party basis, there is an understanding that we have hollowed out and underfunded our military for quite some time.

What we ask our military to do and what they have the capabilities to do may be different from the public-facing perception. That is why that zero basing of defence with an SDR, and deep defence reform in parallel, is a very different context than we had in previous SDSRs.

Q111 **Jesse Norman:** So what it does mean within the context of this inquiry is that a more tightly focused SDR is going to be less engaged with and



competent to consider the defence aspects of hybrid warfare, because those aspects affect much wider bodies of interest and potential security threats across the whole of Government and society.

Luke Pollard: It is precisely why we are bringing together, as a Government, the SSR, the SDR, the various reviews—and there are additional ones across Government—into a single national security strategy. That is what I think is the basis of your question.

Where does it get at it? It gets at it in terms of that broader national piece. What we need is a very clear understanding of what defence's role is. What is the structure that we need? The strategic defence review is, by its very nature, strategic. It will not be setting out the precise number of paper clips on any particular bit, or a precise number of things, but it will be setting out the broader strategic shape that we need to have for our forces. It will then be for the Ministry of Defence to align our forces against that vision that will be set out in the SDR.

In that respect, we will get a very clear focus on defence—the threats and the capabilities that we need. Just to reinforce this, none of our capabilities exist on their own. They exist as part of that wider HMG package of measures. If we are deploying any activity, it is part of that broader thing. Those broader non-MOD components are being looked at by different Departments, but being brought together in the national security review.

Q112 **Jesse Norman:** That is the point that I am making to you, rather than the point that you are making to me. They do run more widely. We recently heard that the final draft of the SDR has now been given to Government. Is that right?

Luke Pollard: Work is still ongoing with it. It would be for Lord Robertson to make announcements on the progress.

Q113 **Jesse Norman:** We do not know what the status of that is, or you are not prepared to say what the status of that is. We do not know that the final one has been delivered.

Luke Pollard: Work is still ongoing. The Prime Minister described it as work being advanced at this stage, but it is for Lord Robertson to make announcements on the progress of his review.

Q114 **Jesse Norman:** How much of an embarrassment or difficulty is created by the fact that all of the underpinning assumptions of European defence and security policy have been upended by recent events?

Luke Pollard: It reaffirms the reason why we are doing a defence review.

Q115 **Jesse Norman:** Except that the thing was going for eight or nine months before the events that upended it. How long is it going to be further prolonged for before we get the re-posturing that would inevitably be required by the changes that we have seen to US co-operation,



potentially, in a whole range of areas that I do not need to enumerate?

Luke Pollard: Some of the underlying assumptions are still broadly the same, though. We are still seeing Russian activity in Ukraine using different tactics and doctrines than we may have viewed in the past. We still have a situation where the US is a key partner for the United Kingdom and will remain so. We know that there are new capabilities that we need to develop. Indeed, there are old capabilities that we need to retire to free up the resources and the people to invest in those new capabilities. That is the challenge that we have.

I have no doubt that Lord Robertson is well aware of the events, and the access that he has, as a former secretary general of NATO, gives him an unparalleled insight to be able to create the report that is true to the threats we face as a nation. It certainly underpins the need for a NATO-first approach. It underpins the need for defence procurement reform. It underpins the need for us to realign our force structure and how we value our people.

Q116 **Jesse Norman:** My constituents in Herefordshire are not particularly confused about the importance of national security and defence, but that is not true about the whole country. You have rightly been saying that, as it were, the awareness and the clarity of communication needs to be increased. Given the complexities of non-attributed, for all kinds of reasons, hybrid warfare, how do you, as a Minister, or your colleagues plan to join the dots on what could be attacks on critical infrastructure or other forms of intervention in migrant crossings, lawfare, or a whole range of other social media contexts, so that people realise that what they are getting is part of a wider pattern and is not necessarily to be taken at face value?

Luke Pollard: It is quite a challenge, and one of the reasons why our adversaries undertake hybrid activities against us and our allies is because there is a difficulty in attribution. When that is accompanied by misinformation, as well as an effect, that is deliberately designed to confuse a population or to cast doubt on the underpinning assumptions.

You are right in the fact that this is a difficult space to operate in. How we respond to it is with clarity on where we can attribute activities, where we can call it out, and where we can be clear about the capabilities that we need, as well as the right conversation and debate to have, not just in the MOD but across Government, about the capabilities that we need. That is what the SDR is prompting, as well as the events that we are seeing on our TV screens, but we still need to make a clear case as to why defence investment, delivered in the way that we are proposing, will deliver the maximum benefit not just for our national security but for our economy and for our people.

We also need to relate that to individuals. A good example would be that Putin's invasion of Ukraine spiked energy prices worldwide. That directly contributes to higher energy bills at home. For any politician, not just a



HOUSE OF COMMONS

Minister, to be able to make the case of, "One of the reasons why we pay high gas and energy bills is because of Putin's illegal invasion", it reinforces that, "Our security is not just about what happens within our own country; it is about what happens further afield as well".

Q117 **Fred Thomas:** I have some quickfire questions, since we are about to end, with the assumed kind permission of the Minister, for the air commodore. You are the head of military strategic effects. If you could distil it into one sentence, what are military strategic effects?

Air Commodore Bressani: My department is responsible for the orchestration and cohering of all effects across all domains, whether that be hard kinetics, information operations or cyber.

Q118 **Fred Thomas:** How many people work for you directly?

Air Commodore Bressani: It varies on a regular basis, but circa 50.

Q119 **Fred Thomas:** How much of your work is contingent on the very long-standing and close joint intelligence sharing that we have with the USA?

Air Commodore Bressani: It is significant, as you would expect.

Q120 **Fred Thomas:** Give us a rough percentage, if you could.

Air Commodore Bressani: I could not put a figure on it.

Q121 **Fred Thomas:** Are you not able to give us a rough idea of how much of your work relies on intelligence sharing with the US?

Air Commodore Bressani: The intelligence that comes to me has been delivered by either the JIC or, specifically, Defence Intelligence.

Q122 **Fred Thomas:** So you do not know.

Air Commodore Bressani: I do not know. I would have to go back to Defence Intelligence and work out a percentage.

Q123 **Fred Thomas:** How much of the job of you and your 50 people would not be able to happen without our current relationship with the US on intelligence sharing?

Air Commodore Bressani: Again, that is really difficult to try to put some kind of metric on, because hitherto, despite current situations being played out in the media, at the working level within ourselves and the Department of Defence, I have not seen a single change.

Q124 **Derek Twigg:** In terms of the protection of undersea cables, you could say that RFA Proteus is more suited to a hybrid type of protection. Do you need more hybrid-related assets?

Luke Pollard: We do, and that was the original plan. RFA Proteus was supposed to be one of two ships when originally planned by the last Government. Certainly, we are seeing a huge interest in Proteus'



capability with our allies and the ability for us to look at what platforms we need to deliver it. The Norwegian model, where industry takes a much bigger role in the protection of critical undersea infrastructure that they are responsible for, is also something that we are looking at. Certainly, the work of Proteus, the RFA crew and the wider defence enterprise that use Proteus and similar capabilities is really quite exceptional, and we would be seeking to invest more in those.

Q125 Derek Twigg: Just to be clear, you would like more defence assets, but you are also expecting industry to do more.

Luke Pollard: When we are looking at a whole-of-society approach, there are some really good models. This is not about a greenfield site and creating a new concept, but about borrowing best practice. The Norwegians are exceptionally good at this, and there is a real opportunity, as we deepen our defence relationship with Norway, that it is not just about mil-to-mil engagement. There is a lot to learn from their offshore industries that could really benefit us.

Q126 Chair: Thank you very much. We are very grateful for the work of RFA Proteus, as well as her sister ship, RFA Stirling Castle. I would have wanted to ask some more detailed questions around that. Unfortunately, time has defeated us. In fact, I wanted to talk a bit more about the work around misinformation and disinformation, but we will, no doubt, be questioning Ministers further on those issues in our Joint Committee on the National Security Strategy.

I wanted also to place on record my gratitude to the National Cyber Security Centre, which the Committee recently visited. Its work is invaluable, especially given that the UK is the third most targeted nation on earth in terms of cyber-threats. That is why this inquiry is incredibly important, and I am very grateful to your good selves—and in particular yourself, Minister—for making yourself available today to give evidence.

Lastly, now that I have your attention, there are various operations happening that we cannot discuss in public within the House of Commons Defence Committee. I wanted to ask, on behalf of the Committee, if we could have your undertaking for classified or, in particular, secret briefings on, for example, Operation Kindred or Operation Hirst. Would you be willing to facilitate those, please?

Luke Pollard: I would be really happy to. We want to create a deeper relationship between Parliament and the MOD. With this group, without phones, I am absolutely happy having those conversations.

Chair: Thank you. There definitely will not be any phones. I am very grateful to your good self for giving that confirmation. As I said at the outset, that builds upon the Secretary of State's undertaking to have a very collaborative and very different approach with the Defence Committee.

Thank you very much, Minister, director general and air commodore, for your evidence today, which I know will inform the publication of our



HOUSE OF COMMONS

inquiry. With that, I bring this to an end.