HOUSE OF COMMONS

Defence Committee

Oral evidence: Defence in the Grey Zone, HC 405

Tuesday 21 January 2025

Ordered by the House of Commons to be published on 21 January 2025.

Watch the meeting

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

Questions 1-52

Witnesses

I: Dr Margriet Drent, Policy Adviser at the Counter Hybrid Unit at Ministry of Defence (The Netherlands).

II: Sir Alex Younger KCMG, Former Chief at Secret Intelligence Service (MI6)

Examination of witness

Witnesses: Dr Drent.

Chair: Welcome to Dr Margriet Drent, the policy adviser at the Counter Hybrid Unit of the Ministry of Defence in the Netherlands. Thank you for appearing before the Defence Committee. Without further ado, I ask my colleague Calvin Bailey to come in.

Q1 **Mr Bailey:** Good morning, Dr Drent. You are here to talk about the grey zone. It is probably worth situating that, because there is no agreed definition for what grey zone operations are, and that is sometimes called hybrid warfare. We have been considering grey zone operations as hostile activity intended to erode a state's ability to function effectively. We are looking at the four levers of power: diplomatic, informational, military and economic. We consider it a spectrum. With that situating of where we are, I shall start by asking, what is the contribution of our armed forces to countering hybrid operations?

Dr Drent: Thank you very much for the invitation. I am honoured to be here to give evidence. The question about the armed forces is very relevant. In the Netherlands, we use a broader definition of hybrid conflict, but let us not go into the definitions, because we do not want to open that can of worms. It is obvious; when you see it, you know what it is. For the armed forces, it has been—in the Netherlands, at least—quite evident for a number of years that we have been dealing with a different type of conflict. I am with the Counter Hybrid Unit of the Ministry of Defence in the Netherlands, which was created in 2018 for the purpose of making sure that the armed forces in the Netherlands were ready and able to respond to this new threat.

We were a frontrunner in the Netherlands as the Ministry of Defence, and it remained that way for a while. One of the first roles that the armed forces have had in the Netherlands is making sure that awareness of the new conflict situation within the other ministries in the country became evident. We also started very early with doing conceptual research about what exactly it is, what we are dealing with, what our vulnerabilities are, and what the contribution of the armed forces could be.

It became clear from the start that a strong deterrent is absolutely important—that is the conventional deterrent. Strength of the armed forces is important to deter our adversaries from escalating their hybrid activities. The deterrent should be strong enough to ensure that the threshold for armed conflict is not reached.

The responses of the armed forces to hybrid threats are also very important because they are on the higher spectrum of the escalation ladder. You rightly pointed out the multidimensional aspects of hybrid threats, but the answers should also be multidimensional. We use the DIME-FIL abbreviation, which is broader than the DIME one you used; it

adds financial, intelligence and legal. Internationally, it is becoming more and more accepted that there are up to 13 affected areas or sectors, so culture, society, information, environment and so on are also included. It is a broad spectrum.

The armed forces also have a large role in making sure that the country is resilient, so they have a protection and stabilisation function. They play an important role in making sure that deterrence by denial is in order, so that adversaries do not have the ability to strike us effectively, and, if they do, we bounce back as soon as possible. We are building on that aspect in the Netherlands at the moment, because for years it has been neglected.

Q2 **Mr Bailey:** I want to draw on a couple of things there. You spoke about the different types of deterrence. One type is the action response, known as the punishment method, but there is also the denial of action, which you elaborated on. Could you expand on that further, and give us some indication of the types of higher-response options that defence, particularly our defence, should be focusing on in that second type of deterrence?

Dr Drent: Deterrence by punishment, as we call it?

Mr Bailey: Denial—the high-signalling stuff.

Dr Drent: Okay, yes. We are increasingly focusing on the protection of the homeland. The Netherlands has a clear task in NATO to make sure that host nation support is taken care of, and that we secure our ports and points of entry for NATO troops if needed. We are making sure that the armed forces can function in a hybrid crisis. It does not have to be an armed conflict; there are many kinds of destabilisation in a society where the armed forces might need to take up their role in protecting civilians or critical infrastructure.

That also means that the armed forces need society to help them for certain functions. We need to make sure that we plan for that, and that it is possible at the moment crisis strikes. The armed forces are very much looking into how we can make sure that the homeland is secure even if there is a simultaneous conflict on the eastern flanks of NATO, for instance, because we need a resilient and strong country to make sure that our armed forces can do their jobs. That is something that we have been starting to work on much more in recent years.

Q3 **Mr Bailey:** I want to draw on some of those things. On national resilience, there are things such as healthcare and the ability to supplement the normal healthcare system with capabilities that you could perhaps offer to NATO. Are they things that you are looking at?

Dr Drent: Yes. Healthcare is something that you really need from civil society. If there is any lesson from the cold war, it is that we need to look at that—what did the armed forces have in place in case of conflict? Civil society has to be asked to help with hospitals, but also food supplies and transport. I think the Netherlands is quite comparable with the UK in that it is very much a privatised country where all kinds of functions are in

private hands. In times of crisis, you need to come to an agreement on when and how those facilities can come to the aid of the armed forces.

That works vice versa as well, of course: first responders are people from the armed forces making sure that the water supply is repaired in an emergency, and all these kinds of specialised things. Cyber-security is also provided a lot by the armed forces. There is a vice-versa relationship between civil society and the armed forces for the homeland.

Q4 **Mr Bailey:** I was going to ask you to pull on the other areas that we should be considering, such as the medical space. It is necessary for some deterrence to be high signalling, so that just having it is a statement of intent. Are there areas that we should focus on within our defence make-up—for example, forces that we can project rapidly, or the size and shape of our maritime forces?

Dr Drent: I suppose I would call that the response side, not so much the resilience side. To communicate and signal about your strength is part of deterrence, and the conventional build-up of your forces is important in that. That might also invite more hybrid activity—that is the paradox of it—because it is a weaker party's choice of instrument. You also need to be resilient. As armed forces, we are very much targeted in subsea areas, as you well know. The North Sea, the Baltic Sea and so on are very much the target of all kinds of activity. Projecting vigilance, projecting that we are surveying it and that they will be caught if they perpetrate there, is very important. Signalling your strength and signalling that you know what is going on and what they are doing—naming and shaming—is important.

Q5 **Mr Bailey:** I think it is quite critical that a lot of the things that you were saying about national resilience are not normally defined as military activities, but they still act to defend and deter. Do you think it would be valid to offer those things as part of our NATO contribution? For example, were we to offer medical capacity or maritime capacity that was not necessarily of a military nature, but that provided resilience, would it be reasonable to consider that as part of our 2.5% or 3%?

Dr Drent: Resilience baselines have always been there from NATO. Countries are expected to protect themselves against crisis and war, and that has not been counted towards the NATO contribution. I can imagine that in new situations, providing specialised services such as medical services not only for UK areas, but more broadly for NATO itself, could be a valid contribution.

Chair: To take the theme of hybrid operations further, I call Ian Roome.

Q6 **Ian Roome:** Dr Drent, I understand that you have had extensive dealings with the UK armed forces in the past, and I would like you to comment from a personal perspective on aspects of the UK MoD's approach to undertaking and combating hybrid threats. What is your experience of the United Kingdom armed forces' approach to operating in a hybrid environment and countering those threats?

Dr Drent: As a civil servant of the Netherlands, I find it difficult to comment on that specifically. From my personal experience, I know that

my country appreciates the UK very much, and we look at it for inspiration. The first encounter that I had five years ago, when I started this job, with research on what hybrid threats are and what the grey zone is, was of British origin. It was an MCDC project in the context of NATO where the first steps were conceptually taken on what we are dealing with, how deterrence can play a role in that, what that should look like and what the role of the armed forces should be in that. Conceptually, the UK has contributed extensively.

I also very much appreciate the UK's support for the European Centre of Excellence for Countering Hybrid Threats in Helsinki, which is an important European and international hub for devising counter-hybrid policies. There is also the intelligence strength that you have—the Five Eyes and the way that you think about intelligence, such as using disclosures as a means of deterrence—which is appreciated.

Certainly, we have also been working together in the Joint Expeditionary Force. The Netherlands has been a member of that for a long time and very much appreciates that the UK has had the foresight to look at the Joint Expeditionary Force as a military co-operation that could focus on countering hybrid threats or operating in the grey zone. It has extensively done that through exercises and, in 2023, by surveying the North Sea with JEF partners. It also took new initiatives to make sure that surveillance of the North and Baltic Seas was taken care of. Taking those initiatives and showing that kind of leadership, and being complementary to NATO in a smaller setting of military co-operation, is very much appreciated.

Q7 **Ian Roome:** Would you agree that the quality of the UK intelligence services is looked on favourably by our NATO allies?

Dr Drent: Yes, it is. It is something that I am not privy to myself, of course, but I know from open sources that the link to the United States, and to extensive intelligence facilities and abilities, is clear from the intelligence image that you present and have—and that you are sometimes willing to share with your European partners.

Chair: Dr Drent, you mentioned that you were inspired by some of the work that you have experienced from the UK and in JEF. Some of us have also been very impressed by the approach taken by the Netherlands, which is why we want to delve further into the contribution of defence to building a whole-nation approach to countering hybrid threats. I call Lincoln Jopp.

Q8 **Lincoln Jopp:** It strikes me that we would all love the certainty of being in a condition of absolute peace or absolute war, because then things would be clear. The trouble is that we are not, at any one time, and that—to me—is the grey zone. At one end, that is actually just life; it is sub-state or inter-state competition, which sometimes moves into conflict. The great thing about being in a state of absolute war is that you can generate a unity of effort among your nation, whereas that is much more difficult in the grey zone. What has been your experience of attempting to cohere a national approach in Government and a national approach including the

polity?

Dr Drent: That is one of the biggest questions in how to make sure that you are effective against these threats that can afflict your society. They are very innovative and are changing all the time. We are dealing with a learning opponent that strikes at us at our most vulnerable. In 2018, when the Netherlands' Counter Hybrid Unit was formed within the Ministry of Defence, there certainly was not a widespread awareness that we were dealing with this type of conflict. I cannot attribute it at all to the Counter Hybrid Unit, because I think it was mostly due to the strengthened hybrid activity of our opponents that that awareness has now grown and policies have now taken root.

From 2020, we already started building our whole-of-Government instruments to make sure that we have an instrument where all Ministries come together on a regular basis, with information from all sources—the Ministry of Agriculture, the Ministry of Social Affairs, the Ministry of Defence and everybody at the table—to make sure that all information about an opponent comes together. Another group then decides on the advice on what to do about whatever we see happening. That then continues to a governance structure where, eventually, of course, Ministers can decide on what to do.

So I think that having information provision from all sides of Government, and bringing that together and connecting the dots to see the hybrid campaign for what it is, is very important. It is probably easier for a smaller country to do something like that. You have to overcome a lot of obstacles, not least of course the exchange of classified information, or the cultural differences between the traditional security Departments and the Departments that have no idea what you are talking about in the first instance. That has gradually changed, and I must say that I think that the Ministry of Defence has been instrumental in that.

We always said during those years that we were leading from behind because, as the Ministry of Defence, you cannot take the forefront in this. You do not want to make it too much of a "Defence issue", because it is more than that; it is a larger security threat for the whole of society. You therefore need to feed other Ministries and entice them, and make sure that the right Ministries take the lead, which they did in the Netherlands.

We are not there yet, because we are also dealing with covert issues, which sometimes bypass this and end up with different working groups and so on. You are also absolutely right that we are not there yet with the whole-of-Government approach that we are setting up and running with. We also need to look at involving private parties, from businesses to civilians, knowledge institutions and so on. You really need to go to a whole-of-society approach, which is an even bigger step. But because of the hybrid threats that we now read about and see on the news and in the media every day, we sometimes feel that civil society is knocking at our door and saying, "What can we do, and how are we going to organise it?" That is something that we are trying to do now, but it is a really big task.

There is also a different mindset that we need to get into as a country. In Europe, we have been in a very comfortable nook for a long time, and are now confronted with a whole different reality. So we have taken in the Secretary-General of NATO's speech, which was very well publicised in the Netherlands, that war is coming. In our communication, we need to be careful not to scare people, but we also need to get them in the right mindset to be prepared and not to be naive about what can come towards them and what they need to do when the crisis is there.

Q9 **Lincoln Jopp:** Because "The war is coming" seems like a very binary, on/off, "peace or war" sort of language. It almost does not hit the mark when it comes to this constant state of conflict narrative. We were talking earlier about deterrence and subsea infrastructure. It would seem slightly de trop, if someone pulls up a cable with an anchor, to drop a bomb on them—it is called a grey zone for a reason. Rather than saying to people, "There's a war coming", we might—to take the example of social media—say, "You are subject daily to disinformation and misinformation." Getting your public to respond in such a way that they become a much more questioning audience of every piece of information they are given is a whole-nation effort and a vast challenge, isn't it?

Dr Drent: You need to do both. You are absolutely right; you talked about a spectrum. We feel indeed that we are in what we call the orange state, going towards the red state of conflict. We are on the spectrum, where it is not peace but it is not war. That is something that we need to prepare our public for, as well as for when it escalates and inadvertently moves on to an open armed conflict.

As for what we do at the moment, we have written a policy that we sent to Parliament in December about resilience against armed conflict and hybrid threats—both of them, the whole spectrum of conflict. As an asterisk, we say, "A natural disaster also requires something of you." We have packaged that together, because the whole mindset needs to be changed, and you need to find the right prompter for that for your audience—the larger public.

You are absolutely right. We feel that every individual has a role in this, is using social media and can be influenced, and needs to be literate in social media and to be aware of what the threats are. The cognitive conflict that is going on is a very large part of the grey zone or hybrid conflict. That is very difficult to address but very important to keep in mind.

It is so different for various parts of Europe, I suppose. If you are in the Baltics or eastern Europe, the threats and influencing are quite clear, but it seems far away here in the UK and the Netherlands. It is difficult to make clear to the larger public what is going on. We try to do that. Disclosures by the intelligence services are more frequent. Public reports from the intelligence services about the situation are more frequent. We send our generals and Ministers to talk shows on television, to make sure that they articulate what exactly is going on. That is the whole spectrum, from influencing to the possibility that it escalates into war.

Lincoln Jopp: Our Secretary of State for Defence is one of the most classic talk show guests I can imagine. With that, I will hand you back to the Chair.

Q10 **Chair:** The 2024 Defence White Paper noted that the Netherlands and its neighbours are very prone to the strategic rivalry and the war in Europe through hybrid attacks. In particular, Chinese and Russian espionage was mentioned. What is the Dutch MoD doing to counter that?

Dr Drent: We are certainly not alone in that. Our Ministry of the Interior has intelligence services, but the Ministry of Defence also has an intelligence service. They are increasingly working very well together, and have been enlarged and receive more money. Knowing what is going on and uncovering espionage are very important. We are particularly, in the Netherlands, dealing with cyber-attacks, cyber-espionage and cyber-theft of technology and knowledge—infiltration into our knowledge institutions and theft of expertise and knowledge on technology. That is something that we are very aware is happening.

It is also in our open reports from our intelligence services and in our White Paper. What we have done is legislated for a new law on espionage, which has broadened what falls under the heading of espionage. We have introduced a new law on screening of investments and mergers in specific areas of the economy. We have beefed up our cyber-defences and also the cyber-abilities of our intelligence services.

These are all things that the Ministry of Defence is very involved in. That sounds a bit counterintuitive, because they seem to be all economic issues, or a lot of economic issues, but we have a very vested, immediate interest in our economy producing the best and most innovative technology for our armed forces, obviously, and in it not falling into the hands of our adversaries, such that we are encountering those technologies in the field. We have a very vested interest in making sure that these policies are tight and well kept, so we have been active in trying to do that.

On knowledge at our universities and our knowledge institutions, a screening law has been introduced and is making sure that specific areas of expertise for PhD and master's students are not open to unscreened persons. We cannot discriminate, so it is persons in general and there is a list of criteria. That is what we are working on to make sure that those persons cannot enter those sensitive studies or areas of research.

Q11 **Chair:** I appreciate that the whole-nation approach that the Netherlands has taken is very different from, for example, what is happening in the Nordics and the Baltic region, with their total defence strategy. I appreciate also that whether we are talking about the UK or the Netherlands, we do not share a border with one of our adversaries. But the nature of the grey zone means that physical borders, in essence, become irrelevant. So what do you think the UK and the Netherlands can learn from what is happening in the Nordics and Baltics?

Dr Drent: We can learn a lot from them. We have visited Finland, Sweden, Norway and the Baltics quite a bit; actually, we just had a ministerial delegation in the Netherlands. We are trying to learn from their example because they have the experience. They know what the threat is; they have dealt with it for a long time. They are clear-eyed about what the intentions are, in relation to a number of adversaries and not only Russia. So that is something that we certainly take to heart.

It is also something that our Parliament has asked us to do—to involve the experience of these countries in devising our resilience and counter-hybrid responses. That is certainly what we are trying to do. The UK is also mentioned by our Parliament as a country that we can learn from. I have been on delegations to the UK in the past to make sure that we speak with the Ministry of Defence and Department for foreign affairs, in this case.

Q12 **Chair:** Lastly from me for now, it is often said that legal and regulatory barriers are what cause a serious impediment to military readiness or societal resilience. What has been done in the Netherlands to overcome that? I ask because the Committee was advised that a lot has been done, especially in the legal arena. Will you please elaborate on that?

Dr Drent: We are working on a law on military readiness, which is going to be implemented as soon as possible in the coming months.

Chair: The armed forces readiness Act?

Dr Drent: Yes, I suppose that is the translation. Because of the legal situation that we are in now, where we are not at peace and not at war, for the armed forces to be ready for these types of conflicts, they need to have opportunities to exercise—in the cognitive and information spheres too. That is something that we are working on. It has not gone through Parliament yet, so I cannot say too much about it, but the idea is to give more leeway and more urgency to the readiness of the armed forces.

You are perhaps also referring to beefing up the numbers of our troops—our military core, but also the reserve forces, which we have tried to build. We have created opportunities for young people to serve for a year at the Ministry, and a lot of them stay either in the Ministry or the armed forces. One of the biggest problems that we have is understaffing. The Netherlands has increased its defence budget quite considerably, but one of the biggest shortages that we have is personnel—enough people in the military and at the Ministry to ensure that the manifold plans to react against the threats that we feel are there can be executed. That is one of the problems.

Chair: Moving on from the whole-nation approach, we now want to look into opportunities for our armed forces to counter hybrid threats. I call Mike Martin.

Q13 **Mike Martin:** We are grateful to you, Dr Drent, for coming to the Committee. I want to explore an idea with you. I was struck by your comments about how your brought different bits of Government together to talk and share, and to maybe decide on some action. It is very

familiar—it made me think of all those meetings I sat in before I became a Member of Parliament where you are trying to get different bits of Government to talk together. There are drawbacks to that approach, and you touched on some of those.

The idea I want to explore—this is country non-specific; we are just talking about an idea—is setting up a clandestine political warfare service with the job of dealing with grey zone threats. Perhaps lots of different Government Departments—we went through DIMEFIL, so defence, intelligence and so on—might second people to that agency. But it is an established agency that maybe works at the Cabinet Office or at No. 10, and it has its own executive powers to operate in that space. What do you think of that as an idea?

Dr Drent: Bold, that's for sure. As a civil servant, I would be worried about the legal and ethical aspects of it. I do understand where it comes from. What we try to do in the Netherlands is strengthen resilience—making sure we are better defended—but at the same time ensure that we are not just sitting ducks and are not only absorbing those threats but are able to respond to them. We call it deterrence by punishment; we draw lines and say, "This is as far as you can go. Now we will retaliate in some way."

As we are a liberal democracy, that is all within the boundaries of international law, obviously. That is a complication, because our opponents do not always adhere to the same rules as we do. Still, I believe that we have to show that there is acceptable state behaviour to which all countries need to adhere. We must set that example and not cross those lines, because then the norms will blur and our opponents will feel even more free to do what they want. This is not Dutch policy or whatever. It is something that I think you should be very careful about.

At the same time, I feel that there are lines that can be crossed that really need a strong response. Where those strong responses are devised is up to every country, I suppose. There is a nationwide response mechanism in the Netherlands where all Departments come together and discuss what our response could be. We also try to make sure that we think ahead: what could be the response that we get from our measures? Do we have a response to that? Because a tit-for-tat situation can be created; that is something that you have to take into account as well. That is a third-order effect that can be in store for us. That is my answer, if that is helpful for you.

Q14 **Mike Martin:** Of course we have to act within legal and ethical boundaries with countries governed by the rule of law. I was suggesting it merely as a way of perhaps co-ordinating better and putting one group of people in charge. When lots of departments come together, the decision that is made is often the lowest common denominator.

I guess that leads me on to my second question. Russia, for instance, is carrying out a programme of political warfare. That includes assassination in the United Kingdom. We had the poisonings with chemical weapons, nerve agents. That is a line that we would never cross.

We have other examples where, for instance, the Americans, in response to Russian activity in America, have switched off the power in Moscow very briefly and delivered at the same time a message saying, "You have crossed the line. Here is our response." You might consider switching off the lights in Moscow as illegal. It is a grey space, so we are in the grey zone. My question is: let us assume we do have an agency that is tasked with being the sole operator in that grey space. We have the military doing deterrence. They need to do that for conventional reasons, which is also useful in the grey zone. We have a whole of Government approach to societal resilience, but we have a separate agency that is in that space. To what degree do you think that western countries need to conduct political warfare in the sense of not just receiving and countering the threats, but actively shaping and driving that landscape? In war you want to be making the decisions, not responding to someone else's.

Dr Drent: First I would like to comment on your first question. You need a separate agency or, as we have, a separate instrument, that advises Ministers, because eventually we are talking about large countries. It is nuclear powers that we are dealing with mostly, so it needs to be a ministerial decision. That is obvious. But it can also have a lot of consequences, so it needs to be weighed by a ministerial commission.

It is interesting. If you turn this around, our opponents would say we are already doing that, because we are expanding NATO, we have devised sanctions, and we are making their life difficult in all kinds of boycotts. What does not cross that legal ethical line is difficult. As liberal democracies, we have also always supported democratic voices in various countries in the neighbourhood of Russia and so on. That can also be construed as political warfare by the other side, so you always have to mirror or look into the eyes of the beholder to see what is regarded as political warfare. We have to be careful with that. Again, while we want to take the moral high ground in this, I would advise at least doing that.

As I said, there are lines that cannot be crossed. There is the right to self-defence in international law, so there are measures—you mentioned some—that can be regarded as being within international law.

Mike Martin: As counter-measures.

Dr Drent: As counter-measures. That is a possibility. I sometimes compare the situation of hybrid warfare to a frog that is boiled in water: at some point, the water is so hot that you are gone, but you don't notice it. We see a gradual increase in sabotage and in the savagery of the activities—you mentioned the assassinations. We have to have a discussion on where to draw the line and what that means for us.

We are working on this in the EU and in NATO, and I hope that it will be done collectively, because we are strongest if we respond collectively; it has a large communication and signalling effect. It signals strength and unity, and that is one of the biggest communication assets of the West. We have partners within NATO, but also beyond—the Indo-Pacific, for instance, can be regarded as partners in that sense.

Q15 **Derek Twigg:** You referred to drawing the line. Do you feel that we are really being too slow in deciding where that line should be drawn and being too nice, given the threats that we face from some pretty difficult and ruthless actors?

Dr Drent: That is not up to me.

Derek Twigg: I know, but I am just asking.

Dr Drent: I used to be a think-tanker—back then, I would have answered quite differently. I have always advised against too strict line-drawing in hybrid threats, because our opponents will make use of that. They will then go just below that line and ensure that we are not triggered into taking harsher measures. You have to consider that. It is really a very complicated game of manoeuvre, more or less, where you have to be ambiguous about your lines. That is what I feel, at least.

Q16 **Derek Twigg:** You are right that we do not want to publish what our line is, because that would obviously give it away, but as you said, there has to be ministerial write-off or higher input. We seem not to be getting to grips with this as quickly as we should be in terms of what we are prepared to do.

Dr Drent: I suppose it is also the nature of the threat. I mentioned the boiling frog. It is difficult to respond to a ship that is looking into all kinds of infrastructure on the sea but says, "I have a right to be here. These are the open seas. If you enter me here, I will do the same to you when you are in our waters." I absolutely agree that it is very difficult to respond. It is very incremental, but what is responsible statecraft? Can we define that? Can we hold them to account on doing that? We need multiple entries for doing that in the UN, in NATO and so on, in all kinds of fora. At some point our national security and interests are damaged so much that we need to do something. We are doing something, of course. We are making it more difficult. We are making sure that we have the information, and that we see what is happening. We are doing all kinds of things diplomatically. We are speaking to them. We have 15 sanctions packages.

In the EU now we also have a hybrid threat package of sanctions, even for Russian activists in Africa, for instance. We are doing something. However, we still see—at least this is what you can see from open sources—a perceived increase in their hybrid activities. So it is a very good question and it is a very difficult one.

Q17 **Mr Bailey:** We have been talking about the whole-nation approach and the need to scale up rapidly, or to give the perception that there are persistent responses and capabilities in order to deny or prevent hybrid operations. Key to that are reservists. They are central to giving an impression of size and of persistence. Could you offer views on our reserve forces and what they should look like? Perhaps some of our old concepts are wrong and instead of considering reservists part-time, the work they do should be considered extra time? Should there be more of a continuum for reservists' capabilities, therefore making it something in which more

people can engage?

Dr Drent: Yes; you have described that very well. That is something we are looking into. We are talking to employers of those people who are interested in having a reservist function, to enable them to take more hours within the armed forces and within their specialised tasks. We are working on a necessary modernisation of the reservist legal framework.

In the Netherlands, by the way, it is both men and women that are on call. We have suspended conscription. It is discussed in the media—should we lift the suspension, making sure we do have the numbers by calling up our generation of 18-year-olds, men and women? The problem is that the absorption capacity of the professional force to ensure that reservists are doing their jobs, are assisting where they are needed, and to advise and train reservists, is now lacking. We have growing pains. I suppose that is something that sounds familiar. We want to grow, but it can be difficult if you do not have the personnel to realise that growth.

What we are also contemplating in a new law is a survey—this is already done in Sweden—to hear people out and to see to what extent they can be interested in a "serve year", as we call them. We then try to retain them for the armed forces and in that sense grow our numbers. We are talking about almost 10,000 extra people that we need.

Q18 **Mr Bailey:** Do you think a change of approach could perhaps help in some of our critical skills gaps? Should we be investing in our military's ability to scale up certain key capability areas, rather than pushing that investment forward into some of the pointier areas of defence?

Dr Drent: Either/or, do you mean?

Mr Bailey: Yes. It was maybe 15 or 20 years ago, when Lincoln was serving, that we would have had colleges that did this for us, and that was considered a national endeavour, growing key skills and so on. Those things went with the "Options for Change" review in the UK, and therefore we do not have anywhere that we could point to that would grow key national skills and capabilities. Is that something that we should be considering again?

Dr Drent: You need to get them from somewhere. You need to look at what the most efficient and effective way is, that suits the culture of the country. I am not an expert on reserve forces, but what I understand is that we are looking to the private sector mostly to militarise in times of need, and to exercise with them, so that we can make use of them when it is necessary. I am talking about hospitals, but also logistics, train stations, and cyber reserves—all kinds of skills that you can imagine we will need. There is also protection of critical infrastructure, and drones—how to legally engage them in protection of the homeland is a concern. A whole different mindset has to evolve. Another challenge is how you get the numbers quickly in a tight labour market, with a small generation of the age that you need.

Q19 **Mr Bailey:** You have mentioned hospitals a number of times. Do you

retain your military hospitals?

Dr Drent: That is a good question. There is a military hospital, but a number of hospitals have dedicated military wings when there is a conflict. They are converted at that moment.

Mr Bailey: So that is capacity over and above the national normal usage.

Dr Drent: Military usage, yes. We need to boost the numbers, considering that we are possibly dealing with a number of wounded.

Q20 **Mr Bailey:** You spoke earlier about resilience against conflict, about hybrid threat, and natural disasters as well. Before I let you go, do you want to offer anything about the Netherlands' cyber-security strategy and how that has taken a broader approach on utilising capabilities that were within the whole of society—particularly cyber specialists—to grow national resilience?

Dr Drent: I apologise that I am not a cyber specialist, though we work very closely together. They have developed all kinds of plans and cyber is very much at the forefront of our thoughts, but I would not want to comment on it in detail.

Mr Bailey: Thank you.

Chair: Thank you very much, Dr Drent, for giving evidence to the Committee. I am sure that it will prove invaluable within our "Defence in the Grey Zone" inquiry. That concludes this panel of the evidence session. Thank you.

Examination of witness

Witness: Sir Alex Younger.

Chair: Thank you, Sir Alex Younger, for agreeing to appear in our evidence session on defence in the grey zone. Sir Alex Younger is the former chief of the Secret Intelligence Service from between 2014 and 2020.

Q21 **Derek Twigg:** You probably will not be surprised by this question. What is the nature of the hybrid threats to the UK and its allies and partners?

Sir Alex Younger: There are lots of different definitions of the hybrid threat. You certainly know it when you see it, but it is essentially the process of concerting all lines of national power against specific national security objectives, regardless of whether there is a state of peace or war. It is ascribed to our authoritarian adversaries, principally. But in layman's terms, this is about our boundaries and our values being used against us by an adversary.

Q22 **Derek Twigg:** Can you give specific examples of the nature of the threats?

Sir Alex Younger: It is not new; it is a long-lasting phenomenon. It is everything that stays below the threshold of war. That can be anything

from disinformation to sabotage to cyber, or economic coercion—whatever it might be. Indeed, there will be new techniques on offer. But the key point is that they offer the adversary the opportunity to achieve its security objectives in a way that is short of armed conflict. So, the sort of Sun Tzu style—to win a war without fighting.

Q23 **Derek Twigg:** Has the nature of that changed in recent years, and is there anything that specifically gives you cause for concern?

Sir Alex Younger: Yes and no. As I say, this has always been a threat: propaganda, subversion and sabotage have been a feature of inter-state conflict for ever. But I think it is also fair to say that our attack surface has increased. The ways in which you can manipulate or undermine a sophisticated, advanced democratic economy have grown, and that is a problem. I think it is largely about the degree of interconnectivity that exists now in the world. The paradox we face is that at the same time as the world is polarising ideologically and moving apart, it is becoming more and more connected. That connectivity provides vectors for attack, be it disinformation, be it cyber, or be it operationalising disaffected individuals to carry out acts of sabotage. All those things have arguably got easier.

Q24 **Lincoln Jopp:** You have a range of adversaries out there, and you have seen them develop these new techniques onto the surfaces that you refer to. There's nothing new under the sun but national character. To what extent does that inform the way in which they develop their own offensive capability?

Sir Alex Younger: It is more a question of the political character, because I think this is our values being used against us. One of the manifestations of our values is a set of laws and boundaries. We in western liberal democracies, for instance, organise around the principle that war is different from peace. It is permissible for Governments to do things in war time that would not be permissible in peacetime. We also organise our response around whether it is domestic or international. We have a Home Office and a Foreign Office. The legal capabilities or permissions that exist for services like mine are different in the domestic space as to the foreign space. These are all there for a reason. They are part of the checks and balances of our governing system.

If you are from a political dispensation that does not do that stuff, does not have any political accountability and can move at the speed of the autocratic whim, as opposed to the democratic will, you will have some potential advantages here. You can get inside our decision cycle and cross boundaries. You can do stuff that has the effect of war, but does not cross our threshold, in the knowledge that we will be constrained in our response.

You can also explore asymmetric vulnerabilities such as the requirement to have some common version of the facts, which we, as democracies, need to function. This is not a problem if you are a non-accountable autocrat. That is a key point that I wanted to make. It represents an asymmetric vulnerability. There are things that you need to run a liberal democracy

that are intrinsically vulnerable, and those things do not, by and large, obtain amongst the people who want to do this stuff to us.

Q25 **Lincoln Jopp:** That is very much looking at it from our point of view, and how we protect against said attacks, but I want to invite you to explore the nature of the threat. You have described it as autocratic, as if that covers the spectrum, but is there a nuance within that in terms of our adversaries' national approach to the way in which they develop the capabilities?

Sir Alex Younger: Yes. We face threats in this space from a limited and recognisable number of actors. Up there in lights, obviously, are Russia, North Korea, Iran and, to some extent, China. Their national situations absolutely dictate where they are going to take this. Looking at Russia, the asymmetry in the relationship with Russia is, of course, all about capabilities and systems, but it is fundamentally about the fact that they think they are at war with us and we do not think we are at war with them. Putin is seized of the idea of horizontal escalation, which he believes is a reciprocal response to what we are doing in Ukraine. It is completely false and erroneous, but that is how he looks at it, so that dictates what they do. They are now actively using capabilities just below the threshold of war to undermine our capacity to resist their agenda.

Looking at China, it is a completely different situation. They do not conceive of themselves as being at war with us, and Chinese aims are, in fact, very different. They are essentially that China should rise and be allowed to pursue its own interests unfettered. Although this has global ramifications because of China's size, it is fundamentally a domestic-oriented agenda. You can see the full quality of Chinese hybrid capabilities in the campaign against Taiwan. The whole thing is there: if you want a textbook on subversion, cyber and political harassment, it is all there, but it is not the same story as Russia. I do not think we see signs of them behaving like that.

Q26 **Lincoln Jopp:** In our last session, we were discussing how we loved the clarity of the ideas of perfect peace and perfect war, because then our rules kick in and we know where we stand, but this "grey zone" that we are talking about really just represents life. The gap on the spectrum between competition and conflict is another grey area. Given that, presumably our approach is to understand the nature of the conflict we are in—which I remember someone saying is the first rule of any Government—am I right in thinking that we lost a bit of pace when it came to Russia? Did we take our eye off the ball for about 10 years when we closed down all those bits of the military that were counting explosive-reactive armour plates on T-35s and all our linguistic capabilities. Did we swing our binoculars away too long and too far?

Sir Alex Younger: Certainly on that point, I think that the rise of terrorism is a national priority. Just mathematically, it diluted the capacity we had as a country to face these state threats. You could argue that it went too far—it depends on your view of terrorism, really. But it is undeniable that the culture and capabilities that existed during the cold

war, the national understanding, the culture of security within the Government and our physical, protective capabilities were all far in advance of what we have now. We disarmed in lots of ways, and this was one of them.

When you talk about us taking our eye off the ball, I think that is also a reference to the "grandmother's footsteps" nature of the hybrid threat, which is all about slowly increasing harassment or subversion and normalising a new situation. When you look at disinformation campaigns, they are all about normalising chaos and distrust, and then moving on to the next point.

One of the really pernicious and difficult things about hybrid threats, as you said, is that they are not binary—they slowly increase. It is hard: democracies do not really have the capacity to draw a line at some point to just say "No", so this Russian stuff did creep up on us. You look at that with hindsight—the behaviour of Russia assassinating citizens on our soil and the way in which we fundamentally saw that as a criminal issue, as indeed to some extent it was—but it took us a lot longer, arguably until the Ukraine invasion, to understand that this was of a piece with a structurally aggressive Russian approach to asserting what it sees as its interest in Europe.

It is hard for democracy to get ahead of that. I saw the same thing with counter-terrorism. It took the horrors of 2001 to produce that step shift—God forbid that we have to do that with the hybrid threat, but we need a similar process where we get real about this and organise to effect it.

Q27 **Lincoln Jopp:** We are going to come to the nation's response in a minute, but I want to explore the nature of the threat. You said something about culture—I cannot remember the word you chose—but when it was the cold war and treated as a war of national survival, do you think we were better at keeping secrets than we are now?

Sir Alex Younger: I think it was easier to keep secrets. We were not in a hyperconnected world. There was a security culture in Government which has to some extent been undermined, including by the advent of technology, but also by a generation of a world that was essentially—or at least apparently—free of those considerations. Then there is the need to invest properly in those capabilities. It is a more challenging environment than it was before.

Q28 **Lincoln Jopp:** But is the genie out of the bottle? Can we only go in one direction for a liberal democracy, or can we re-instil that security culture?

Sir Alex Younger: Absolutely. I do not see why that is not entirely possible. Frankly, you only have to go to different countries in Europe to see different cultures in operation. I know that the centrality of resilience and security is normally in direct proportion to proximity to Russia. If you go to Finland, for instance, you will find a resilient culture that fully understands the value of all those things—the value of information, for instance—in a way that we can learn from. I do not think that is wholly

surprising; we have had 30 years without having to think about that very hard. But can we get it back? Yes, absolutely.

Q29 **Chair:** Sir Alex, you served as the Chief at the Secret Intelligence Service, and I thank you very much for your service to the nation. One of your counterparts, the head of Germany's domestic intelligence service, remarked in 2022 that "Russia is the storm, China is climate change." With regards to defence in the grey zone and hybrid threats, how far would you agree with that statement?

Sir Alex Younger: He is essentially right that China is the pacing issue—the chronic issue. We face a massive societal question that will hugely affect the choices and lives of my children: can an autocratic regime get rich? Can it rise to be the peer adversary of the United States? We need to be honest that we are therefore in a systematic competition.

Russia is much different, much more acute, and much closer in. I slightly struggle with the climate analogy because, if this is a storm, it is a storm that has been going on for a very long time and it will go on as long as Vladimir Putin is alive. There is a risk of being dismissive of it, in those terms.

Q30 **Chair:** Agreed. The National Cyber Security Centre's 2024 annual review made for some very alarming and concerning reading. For example, the number of attacks reported to the National Cyber Security Centre rose by 60% in the last two years—if we compare the 2022 figures with the 2024 figures—to 1,957 attacks reported. Likewise, the number of highly significant and significant incidents per year rose by 50% in the last couple of years and now stands at 89. Whether it was for the number of incidents handled, or for data exfiltration, all the parameters were going up. Do you think that we are doing enough? Are we matching up to the challenge, or is the UK found wanting here?

Sir Alex Younger: I am a tech optimist. I think that these technologies have been enriching, the connectivity is extraordinary and the productivity enhancement is amazing. But there is a dark side and a tax that we have to pay, which is to invest in our digital resilience. Because this is an invisible threat, it is almost inevitable that we do not pay enough. We cannot see the problem. We cannot see the drip, drip loss of strategic advantage from the IP theft that takes place every day. Although the ransomware epidemic makes it clearer, we still do not understand the true consequences of a destructive cyber-attack, particularly a systematic one, so it is inevitable that there is a risk of complacency.

The UK—again, this is a corollary of a positive—is one of the most online, connected countries on the planet and that does us very well but, to your point, it means that we are particularly vulnerable. I think the National Cyber Security Centre is a great innovation—I remember when it was set up—and, in particular, the bold idea to, essentially, integrate the secret world with the open world. It has worked and it is now widely copied, but this is certainly something that the National Cyber Security Centre cannot do on its own. There needs to be a societal effort to improve standards of

digital security across the piece because, while we are as vulnerable as we are, we can have no hope of deterring hostile powers, like Russia, in cyber-space.

Q31 **Chair:** That's right. The National Cyber Security Centre rightly highlighted that the number of organisations whose information is being stolen, or against whom extortion is being used, has also risen significantly over the last couple of years.

The NCSC has done a lot to counter the digital attacks but there is also the physical infrastructure, including undersea cables and gas pipelines, as we have seen in eastern Europe. Our Joint Committee on the National Security Strategy is looking at undersea cables and will undertake an inquiry. In your view, are we doing enough to protect that physical infrastructure? An attack on it would have a debilitating effect on the nation, because banks would not be able to trade, military operations would slow down and things would come to a grinding halt. Do you think that we are paying enough attention to that physical infrastructure, and what can be done?

Sir Alex Younger: This is a societal choice. To be honest, the facts are now self-evident. The cables issue has been very much in the public eye because of what has apparently been going on in the Baltic. We have been warned. In practice, this is something that Russia, in particular, has been focused on for a long time. Indeed, the solution is pretty clear, which is the need to invest for resilience to ensure that we have a wide set of redundant systems that mean that we are not vulnerable to single catastrophic interventions. This is about much more than cables; it is about our supply chain generally.

To be clear, the societal choice is that, if we are in essence to internalise that risk into the economics, that will cost money. Britain is in a difficult fiscal situation. It is a really tough choice. It seems to me that that is an area where politicians, in particular, need to be very clear about the choices that exist. If they believe that they are justified, I think it will be important to incentivise the private sector to invest in resilience, with appropriate industrial policy, regulation or whatever it might be. But we cannot pretend that this comes without a cost; it emphatically does.

Chair: Ultimately, much of that infrastructure is in private firms. You mentioned choice, but in essence, do we have a choice? If we do not take action, it will be catastrophic and significantly impact our way of life.

Q32 **Lincoln Jopp:** I do not want to misquote you, but I just want make sure that I heard you correctly when you said that we had no hope of deterring a country such as Russia in cyber-space. Is that because of policy or capability?

Sir Alex Younger: Thank you for checking, because that is not what I wanted to say. It is important to be able to deter hostile adversaries, including when they employ cyber-means against us. That does not necessarily mean a reciprocal response—in other words, I do not think that we have to meet a cyber-attack with another cyber-attack—but we as

western countries should want to have our own set of capabilities, whether economic, legal or whatever, including cyber, to bring to bear to deter the worst excesses of our adversaries. We must do that. However, that is a completely pointless activity if, at the same time, our defences are let down. There is no point—I am not a great football fan, but I assume—in investing in the forwards, but sacking the goalkeeper. That will not end well.

Lincoln Jopp: Having been to Wolves versus Chelsea last night, I completely agree.

Chair: We will now move on to examining liberal democracies and hybrid threats.

Q33 **Michelle Scrogham:** Welcome, Sir Alex, and thanks for your time. When it comes to countering hybrid threats effectively, what is the balance between using the armed forces, intelligence agencies, and other public and private bodies?

Sir Alex Younger: That is a really good question, because to my mind, it is all about teamwork. We cannot emulate our authoritarian counterparts, which definitely get the decision advantage by the fact that there is one man—I use the term advisedly—in charge. He can concert capabilities across the spectrum of his country, say Russia, and he can do that regardless of whether a war is going on or not.

Those are things we cannot do, so we have to think about how we generate equivalent capabilities. Teamwork is at the heart of it. By and large, a thing that autocrats hate is our alliances and the quality of our teamwork; that is not something they can emulate. That is true internally, domestically, and internationally. Domestically, this is a real challenge that I want to put out: how does a democratically elected Government move at the speed of a hybrid adversary?

When I first became a leader in the national security space, David Cameron had just invented the National Security Council. I was a real fan, because anything that improved our capacity to concert our capabilities across the spectrum, regardless of institutional ownership, is good for us and bad for our adversaries. However clunky, I thought that it was a good step in the right direction.

To be honest, I do not think that the National Security Council survived in that form under subsequent Governments. I do not know how it is used now, but my strong hope is that it is a place where you can take decisions that transcend stovepipes and do that in a timeframe necessary to react to this stuff. So I am voting for anything here that improves the capacity of Government to react with agility, because this is a whole-of-Government threat, and it requires a whole-of-Government response.

Q34 **Michelle Scrogham:** You mentioned that the Netherlands' MoD have referred to themselves as leading from behind when it comes to these cyber threats. Is that something you would see as a benefit to us, and where do you assess the UK as sitting within that?

Sir Alex Younger: Just to broaden that out, we should define security as being about more than what the Ministry of Defence does. That is the reality of what we are dealing with. If you are going to effectively counter a full spectrum threat, you have to use your full spectrum capabilities—that includes the Department for Education, for instance, when you are dealing with subversion, and it absolutely includes the Treasury, and so on. The first point is not to be too hidebound by how you define security. The membership of the National Security Council should accurately reflect that.

I worry a lot about the fact that we effectively have a ministry for war and a ministry for peace in the MoD and the Foreign, Commonwealth and Development Office. I think we recently lapsed into a very uncomfortable paradigm where the MoD did hard power and the FCDO did soft power, and that was nonsense. Everyone should do both, and it has to be integrated. This Government, certainly when in Opposition, talked a lot about the need to solve that and bring it together. If that is happening, that would be good, and I think the club should be broadened to include my former community, the UK intelligence community.

But the reality of what's healthy is that it is not so much about being behind or in front as it is about seeing that grouping, in particular, working as a team, and whether the Ministers involved understand that and whether the mechanisms exist for the decisions taken to be transmitted into facts changing on the ground. I worry that our systems and our laws do not enable that.

Q35 **Chair:** I want to delve into autocracies versus liberal democracies. It is often assumed that we as liberal democracies—with consensus, political debate, and an open and free press—are more vulnerable to hybrid threats. Do you think there is a perceived weakness and how can we counter it?

Sir Alex Younger: I think it is a weakness. The reality is that our attack surface is much broader. To be democracies, we make our decisions in the open, and we admit a very wide range of influences on those decisions, most of which are ripe for manipulation by a malign adversary. In the information space, there is a profound asymmetry. We need a set of common facts to run a democracy but autocrats do not—and worse, facts, AKA the truth, are a threat to autocracies. They do not have a disinformation problem by and large because the leader just says what the truth is. We are in a position where they have, on the face of it, a pretty cheap way of making life pretty expensive for us, and we need to organise against it.

But you must not fall into the autocrat fallacy. They do have these advantages, but please can we not conflate resilience and rigidity? What you see with the grand parade on the national day and the serried ranks of tanks is, to my mind, a sign of rigidity, not resilience. There is little flexibility. There is great brittleness in these regimes, and they have a different set of weaknesses.

If you want to know what I think we should do to deal with the threat posed to us in the hybrid space by Russia, I would remind you that the language they respect is strength, not weakness. The way to deal with this problem is to ensure that Ukraine does not stop existing as a country. That is where this is being contested. If we flake on Ukraine, I can assure you our hybrid problem will not get better; it will get worse.

Q36 **Chair:** So in essence, the way to take on a bully is to face them down.

Sir Alex Younger: Ukraine is a sign of the failure of autocratic societies. It reveals the essentially corrupt nature of these regimes. It was a catastrophic mistake on Putin's part to get involved in this. If he is seen to be vindicated, I think our problem is going to be a lot more difficult, but the reverse is absolutely also the case.

Q37 **Mike Martin:** On the point about facing down a bully, in the hybrid space it often seems that we are responding to or "countering"—it is even in our language—the hybrid threat. To what degree do you think that we—the west, the UK—should be conducting political warfare? Russia is an opponent and they are assassinating people on our soil with nerve weapons, nerve agents. To what degree should we be leaning into that problem and switching off the lights in Moscow?

Sir Alex Younger: It will be clear that I bow to no one in my hostility to Vladimir Putin, but the maxim that we always had when I was in office was that we aim to beat the Russians, not be the Russians. I am not talking about artificially ruling out a proportionate and justified response to Russian aggression, but we need to understand that we are societally completely different and organised in a different way. We have a whole set of different advantages that we can bring to bear.

To put it bluntly, I do not think Putin is particularly susceptible to a lot of the techniques that we use on him, because he is not accountable to his own population. So the attitude is right. We should certainly be proactive and work assiduously to attach cost to what he is doing, but I think we should do it our way, and our way is defeating him in Ukraine.

Q38 **Mike Martin:** I totally agree about Ukraine. Rather than the methods, because we would never assassinate people in Moscow, for instance—as you know, in warfare, you want to get your enemy to respond to you rather than you responding to your enemy. You call it proactivity, but even using a different set of methods from those of Russia, is there a degree of proactivity we can use that will actually have them responding to us?

Sir Alex Younger: The principle of what you say is uncontestable. To the extent that we are reacting to this, we will always be in a weak position. We have a set of tools—economic alliance, cyber, whatever it might be. We need to think about using those to create the highest possible cost to these adventures, which is perhaps not as bloodcurdling as you want me to make it sound, but I think that is the sober reality. I do not think we as liberal democracies can organise in a different way.

Q39 **Chair:** To build further on that, I would posit that liberal democracies have

some inherent strengths, such as a robust civil society. We have a vibrant private sector that leads to technological sophistication, and our strong institutions. Do you think we have other strengths, given your experience within the intelligence services, and how can we better exploit those strengths to counter hybrid threats?

Sir Alex Younger: It would be irresponsible of me to speculate about anything that is operational, so I am not going to do that. It is important for us to recognise that as much of this is about us as it is about them. If you took, for instance, the well-grounded fears we all have that Russia is subverting, with its disinformation campaign, our political discourse, I would agree with that. But I absolutely do not think that that is our biggest problem.

In practice, Russia has been pretty frustrated by the resilience of our politics and has not found much by way of new divisions that it can create. It has had to settle for a second option, which is just to seek to amplify the discord and division that already exists, and you can see Russia doing that in cyberspace. That is why it does not support one side of the argument or the other; it just tries to muddy trust in our societies.

In our modern politics in western countries, there is a much bigger issue of polarisation. The role of tech inside that is an important factor. To be honest, I would worry about focusing on external factors, such as Russian aggression—pernicious and dangerous though it is—at the expense of some much more core issues about our integrity.

Chair: Agreed. Before I come back on to the vulnerabilities within autocracies, I want to bring in Calvin Bailey and Lincoln Jopp.

Q40 **Mr Bailey:** I just want to go back and explore your statement about Ukraine. Wars are won when it costs them too much—we hope to win that conflict when Ukraine makes it cost Russia too much—but you also lose wars when it costs you too much, and those costs are not just financial. It can be will. You have to build will, and drawing on some of your points effectively about the holy trinity—people, Government and the armed forces—we have to galvanise good will or create the understanding that the outcome is fundamental. What strikes me with your remarks about Ukraine is that if I took those out on to the street, they perhaps would not resonate adequately with our people. How do we create the good will necessary to fight a sustained conflict?

Sir Alex Younger: I think it is the cost thing. You have to go out and explain that the costs of giving in to Vladimir Putin in Ukraine far outweigh the alternative. I worry enormously that if we fail to invest now and pay that cost now, the cost to our society in future will be astronomic. We have to face this down at some stage. I would be talking to the public—it sounds distasteful, I suppose—about the fact that this is a bargain. We have an opportunity to demonstrate to Putin that he cannot act with impunity. If we do so, it will reduce the broader threats that our societies face. If we fail, the costs will be pretty well incalculable in terms of the demands on our economies and the extent to which our defence

capabilities will have to grow and, frankly, dominate our scheme of expenditure at a time when we face serious fiscal challenges. I appreciate that coming from me—you might think I am invested in a narrative of conflict—it could sound like a self-serving narrative, but it is important for the broad political spectrum just to make people understand what is at stake here. It is absolutely not a faraway land of which we know little. To be clear, by the way, I understand that in the end, there is diplomacy and there is a conversation, but I do not think that will produce the right answer, unless Putin is incentivised to make compromises, and that requires us to double-down on our effort.

Q41 **Mr Bailey:** With that being the case, let's assume a failure with Ukraine. What does the developing hybrid threat look like?

Sir Alex Younger: First of all, I think Putin will be emboldened. He will think that that his tactics, which have been very much about hybrid warfare, have been vindicated. He thinks that we are already much more active than we actually are. He is intent on horizontal escalation. In better news, his army has performed risibly. It is completely depleted and exhausted, and it will take a number of years to reconstitute. I do not think he will invade Poland, because I do not think the capabilities exist, at least for the next few years, but will we see ongoing momentum in the hybrid space? Absolutely. Moldova would be the obvious next choice, and that would further compromise Ukraine's position if Moldova's western orientation is effectively undermined. Then you will see the playbook of the weaponisation of Russian-speaking communities in the Baltic states. You will see an intensification of the disinformation campaign. You will see the political factions that Russia identifies as helpful rising in Europe and being supported in the covert space. We will see more subversion, including sabotage, and in that sense I think we are at the beginning of the story.

Q42 **Lincoln Jopp:** To follow on, I guess the other side of Calvin's coin is cost and cash. I do not want to probe around the operational out of bounds box, because this is pretty much an area of policy. We have taken the decision internationally to skim off the interest from the seized Russian assets. Does there come a time—have you done an assessment, even if it is just in your own head, of the effects of going for the actual money itself?

Sir Alex Younger: I worried about the international precedent that it set, but I now think there is a strong argument for doing just that.

Q43 **Michelle Scrogham:** What is your assessment of our vulnerability to electrical interference? We see an awful lot in the media, particularly in terms of media interference, who owns the media, who is lobbying and who is donating to political parties, with that kind of competition between them. What kind of threat do you see there?

Sir Alex Younger: It is going to get worse, most obviously because the capacity to create falsehoods has been massively uplifted by the advent of generative AI. That has offered the opportunity to produce disinformation at an industrial scale and at internet speed, in a way that must surely be

alarming. I also think that we are seeing worked examples of Russian-orchestrated disinformation campaigns altering election results. Georgia would be one possibility, and it is pretty startling what has been happening in Romania. It has been rather heartening to see the judiciary there take the stand that it has. I also return to what I was saying earlier. I actually do not believe—bear in mind, I am not in office now—that there has been, in this astonishing year of elections, an example of a major democracy's result being swung as a result of Russian disinformation. Their operations fall far short of what they would desire. I think they have actually found us to be rather more resilient than they would have expected. I think the vital ground of this conversation, as I have already said, is about much more than foreign interference.

Q44 **Ian Roome:** Sir Alex, I have been listening patiently to your answers. You obviously had a very good career, and thank you for your service to the country. With all your experience, from a personal perspective, what do you want to see from the next strategic defence review?

Sir Alex Younger: Organisationally, I want to see a huge premium on our capacity to work together across the spectrum in response to the threats that we see. There are institutional and legal measures that can be taken to improve that and that do not cost anything. Then, of course, a significant technological investment is required in connectivity and joint data to allow us to operate as one. That will already put us in a significantly improved position. The issue that will dog the SDR is the choice between the climate and the weather, or the storm and whatever it is. I think that we can blunt the immediacy of those choices if we work hard to integrate our capabilities. By the way, I am not saying, because I had this in the UK intelligence community, that the different bits of the machine should not have distinct cultures and distinct identities.

SIS will always be very different and have a distinct identity, but we are ultimately servants of the public, and we should bend our capabilities to the highest priority and do that in concert with other people. It sounds a bit nerdy and governmenty, but it would be a huge gain if we could bring that about. There has to be investment in resilience. And if I can do a shout-out for my community, we need to make sure that they have the tools and law and resources that they need to actively combat those threats below the threshold. In there is a set of things that would already make life more difficult.

I am conscious that alongside the conversation about the hybrid threat we also have a very real conversation about hard power and deterrence, and that makes this wicket. I understand defence colleagues when they talk about the need for us to be building capabilities that can defend this country in an extreme emergency. I am not belittling the choices that exist.

Q45 **Ian Roome:** One of the big areas facing defence at the moment is advancements in cyber, particularly in recruiting to the intelligence services professions. Do you have any thoughts on that?

Sir Alex Younger: If I could expand that, the things that will condition the choices available to my children relative to the choices that I have enjoyed are who owns the global commons of hardware and software—of the digital world. Who is running the digital world? Is it an autocratic regime like China, or is it open societies like ours? That is wide open, and I cannot overstate, at least in my head, the importance of the tech and innovation competition as a determinant of how this nets out.

You ask about the SDR, and of course investment in metal will be really important, but if you were to ask me the thing that will determine whether we have real security in this country in a generation's time, it will be whether we have maintained our technological edge over our potential autocratic adversaries. That is the big one. I will revert to that priority at every stage. That gives rise to a whole set of so whats, which also, conveniently, apply to our economy. Skills is a huge thing there, and it is imperative for Government to be able to attract those skills as well as anybody else. We should think about mechanisms to get people in the civilian world who have those skills operating in some capacity or another, perhaps more so than already happens.

We need to recognise that Government's cyber defences are never going to work without the necessary skills. More broadly, technologies such as AI are unlikely to be deployed in a way that really maximises the advantage to us in the defence space, unless we can get the people with the right skills. The market is not pushing us in that direction.

Q46 **Ian Roome:** I completely agree with you. We need to be a lot more focused and possibly change the cultural attitude in the MoD. We need to invest in recruiting cyber. Do you agree that we need to think out of the box to work out how we can recruit from civilian society? People do not need to be in uniform.

Sir Alex Younger: That is the advantage of the interface with the intelligence community; we are essentially civilian, and we have lots of skills in this space and different ways of understanding. Sometimes we can move more quickly. Defence have skills of their own. There is a strong argument for integration on all these capabilities.

Q47 **Lincoln Jopp:** On the whole-nation approach and the digital edge, if we were talking about teaching 12-year-olds how to disassemble an Armalite, we might end up in controversial conversations with the National Union of Teachers, but because we are talking about digitalising our youth, those skills can be generic. That suggests to me that a logical so-what from what you were saying is that the digital content of our educational syllabus should be increased and enhanced.

Sir Alex Younger: That is a no-brainer in any case, isn't it?

Q48 **Lincoln Jopp:** Funnily enough, in another part of this building a discussion is ongoing about whether we should ban people under 16, or 18, from having smartphones.

Sir Alex Younger: Yes, but that is a slightly different issue.

Q49 **Lincoln Jopp:** In some people's view it is as dangerous as teaching a 16-year-old to disassemble an Armalite.

Sir Alex Younger: Tech literacy is really important, but I would go further and talk about a capacity for critical thinking. How do you get and process information? What do you believe? How do you go about finding the other point of view? How do you stay out of an echo chamber? Those are all things that we should be talking to our kids about. They are things that we have talked to them about in the past. This is surfacing as yet another area of the identity politics debate, but it is much more fundamental than that. Teaching people to think for themselves is at the basis of our capacity to resist disinformation campaigns, and that starts in the classroom.

Q50 **Chair:** In open liberal democracies, it can often appear that autocracies are omnipotent, and that the strong man model is the one that should be employed. Indeed, David McFarland, in his written submission to our inquiry, noted that autocratic governments often have the advantage of longer timeframes and more consistent approaches to policy, and obviously they don't have to bother with the election cycles that many of us are vulnerable to. They can take a more long-term approach. Given your own experience in the intelligence agencies, how would you categorise vulnerabilities in autocracies, particularly with respect to hybrid threats?

Sir Alex Younger: That is a really important point. They can plan long-term, and that confers spectacular advantages in the tech competition. They are not inhibited, arguably, by laws or values, so they can manoeuvre. They don't do boundaries. But they are fundamentally fragile. The point about our democracy, imperfect though it is, is that it confers one golden property that does not exist on the other side of the fence, and that is a mechanism for the peaceful transfer of power. In some sense Putin is trapped by the logic of his own narrative. He can never leave. Xi Jinping, in going for his third term, also has disintermediated an entire generation of Chinese leaders and made the succession much more fraught. In those circumstances corruption and tension build up behind the scenes.

As we saw in Syria, things can change at short notice. The reason I was being so cautious when answering the questions about what we should be doing to our opponents is that this is a process that always comes from inside. It is about the people in those countries finally deciding that things should change. That is why I even hesitate to characterise it as a vulnerability when we are looking at how we respond or what vectors we use. It is important to understand, just from the psychology of this, that one must not conflate resilience with rigidity. They are different things.

Q51 **Chair:** Would you not agree that a lack of accountability and challenge can often incentivise loyalty over efficiency and lead to paranoia over effective planning?

Sir Alex Younger: That is all absolutely true, and it makes us feel good as democrats. My advice is not to make a plan on that basis. It is a pretty

febrile time in the western world, and I do not know how long country X or country Y will last. Even if I did, there are contradictions and tensions that I have described, so our strategy should not be based on all this going away because all those countries will fall apart. I know that that is not what you are saying, but it is incredibly important for us not to be complacent. The short-term advantages that you get from being an autocrat are quite considerable.

Q52 **Chair:** Would you agree also that the "zero sum game" approach employed by Putin in Russia in essence distorts the truth about the west and what is being done here, and therefore some of the hybrid threat activity is undertaken without knowing how liberal democracies function? There is a lack of knowledge in China and Russia, in particular.

Sir Alex Younger: As I have said already, the Russian attempts to manipulate our political systems have fallen far short of what they wanted to achieve because they do not really understand how we operate and because we are pretty resilient. Those are good things. They have optimised around a process of making everything worse in order to increase distrust between the Government and the governed and ultimately claim a moral equivalence between their system and our system, which is what Putin really wants to achieve. We need to be alive to that, but we should not blame it all on the Russians because that risks diluting our determination to deal with lots of really fundamental stuff in our own system.

Chair: Indeed, we have our own vulnerabilities in the system. Sir Alex, thank you very much for giving evidence to our Defence in the Grey Zone inquiry.