



HOUSE OF COMMONS

Defence Committee

Oral evidence: Defence in the Grey Zone, HC 50

Tuesday 14 May 2024

Ordered by the House of Commons to be published on 14 May 2024.

[Watch the meeting](#)

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

Questions 57-84

Witness

I: Mr Jānis Garisons, former State Secretary, Latvian Ministry of Defence.



Examination of Witness

Witness: Mr Jānis Garisons.

Chair: It is a pleasure to welcome you all to the third session of the Committee's investigation of defence in the grey zone, looking at comprehensive national defence and at Latvia as a particular case study. It is a pleasure to have Mr Garisons with us today. Jānis, would you mind introducing yourself for the benefit of the Committee and those watching?

Mr Garisons: Good morning, everybody. I am Jānis Garisons. I was for almost nine years the State Secretary—in the British system, the permanent secretary—at our Ministry of Defence. During my term, we started comprehensive defence, introduced it and set the scene for many of the pieces that now lie as a foundation for comprehensive defence.

Chair: It is a pleasure to have you with us today. Thank you for joining us. Derek, you are going to kick us off.

Q57 **Derek Twigg:** Good morning. Can you explain what is meant by the concept of comprehensive national defence and how it evolved from total national defence?

Mr Garisons: We had realised already, sometime around 2008, when Russia started their first war in Georgia, that this different malign influence had started against our society. At that time of course, the main signs were recorded in the information space. There were a lot of Russian channels appearing and a lot of fake news, and we started developing some resistance to deal with that issue. The question was how to reduce the impact of Russian information warfare, or even sometimes psychological warfare, on our society.

I am a graduate of the US Army War College and studied Sun Tzu. As you know, Sun Tzu said basically that the highest achievement is to win the war without the fight, and I think that the aim of everything that we are seeing when it comes to the grey zone—sometimes we call that hybrid—is to win without a fight. It is about your society's mind—the fight for people's minds—and then of course your ability to resist different harms, so I think it is to be viewed as a more general and theoretical issue.

The grey zone threat is just one part of general strategy. It is sometimes a mistake to separate the grey zone from military conflict, because even in terms of the so-called Gerasimov doctrine, everything that happens before is meant to reduce the ability to resist, or meant to conquer your society's mind, probably in the hope of not getting into fighting. Therefore we realised, sometime around 2015, that we had to change from the previous concept, that the armed forces would be fighting and society would simply await the outcome of battle. That was the wrong assumption, which probably emerged from the period of the peace dividend of the 1990s and 2000s. Therefore we developed the comprehensive concept of total defence 2.0, as it was during the Cold War, which then evolved.



HOUSE OF COMMONS

I would say there are two main goals in comprehensive defence. One is to strengthen resilience, by which I mean strengthening the resilience of society—the resilience of minds, psychological resilience—to different outside operations or malign operations. Another important goal is to change the calculus that if there is a war, society has to be assisted by the armed forces.

Previously it was believed that, even in times of war, the armed forces would deliver many services or assistance to civilian parts of society, which actually is not true; they will not, or at least we will not have sufficient manpower for that, so that second most important goal is how to teach society to survive during the war. That includes all critical services, because it will be very difficult if people do not get most critical services, starting with water, food and banks—the financial system—and so on. You can win militarily, but once people realise that they don't have access to their money in banks, there might be a big problem for society or for the country.

The concept as it developed centred around those two main goals. One is resilience, and I am talking about resilience because we are a frontline state and we see that impact on our society almost daily. Once we are not able to respond properly to some kinds of Russian action, there are fears in society, and we have to deal with those fears, which you can do only through resilience and through talking to your people. The other aim is, as I said, to teach and establish a system for the rest of society and civilian organisations like the private companies, banks, non-governmental organisations and the Church—establish what their tasks are during the war.

There is always a question whether you have to go to that extreme of war. I have to admit that when we started this project, if I may call it so, there was a very hesitant reaction from the public, because you have to start talking about war, which is not initially a very convenient subject. But then, when the Russians took more actions, society requested more and more, and after full-scale war in 2022, people actually demanded that we talk to them. Therefore, to respond to your question, that is how I see and how we dealt with all those issues.

Chair: Thank you. You have covered a lot of ground. Sarah, you want to talk about some of the practicalities underlying that.

Q58 **Sarah Atherton:** Jānis, in practical terms, what does the plan look like on the ground? In particular, which Departments take responsibility for which area of the plan?

Mr Garisons: I in the end, it covers almost everything, but at the beginning, when we started, the first area was the information space. First of all, we tried to establish a system where we could observe and recognise the hostile actions taken in our information space. We could then react to those hostile actions—either psychological operations or information operations. It took quite a lot to start co-ordinating. It started at the Ministry of Defence, but it grew into the full Government's strategic



communication policy, which now plays an important role in reaching people.

Then there is one block of issues related to critical infrastructure. We changed the previous notion of critical infrastructure because we realised that infrastructure alone does not play in all the occasions we are looking for. We therefore introduced the notion of critical services. For example, you probably need not the bank itself—the critical infrastructure—but the service provided by the bank and how the bank allows us to basically access the data. We also looked at possible options for if the country is cut off from, let us say, the outside internet, or if the supply of electricity is damaged. That was an area where the Central bank took quite an active role in developing a system, a plan for how to access data, which should be stored in the country. We also developed an internal internet exchange, which will provide us with the option to have internal internet. Even if outside communication is lost, we will be able to have at least some basic services to provide the internet.

Q59 Sarah Atherton: You have spoken a lot about psychological defence. Which Department took responsibility for that and what did it do?

Mr Garisons: In our case, that was the Ministry of Defence. We realised that people expected explanations from the Ministry of Defence. We are a frontline state. We have to give those explanations to people. There is a need for proactive communication, and you can counter hostile actions if you have previously been communicating proactively.

We organised a lot of seminars for different groups of society, like teachers or regional leaders, or the Church. We realised that the biggest problems are lack of confidence and lack of knowledge, and lack of knowledge and communication from the Government's side creates a lack of confidence. Once you start communicating and explaining to different groups in society, that generates confidence.

Q60 Sarah Atherton: So the plan relies on trust and co-operative relationships with society and community groups.

Mr Garisons: Yes. Exactly.

Q61 Sarah Atherton: How did you get that whole-society buy-in from extremist organisations who perhaps do not share the Government's beliefs of where the country should be going?

Mr Garisons: We invited the majority of organisations, but it was done on a voluntary basis; nobody had an obligation to do anything on that. A lot of organisations were willing to co-operate, such as the Church. They were very active in engaging and understanding, because they are all in such critical situations.

We also realised in 2016 that we needed to have some kind of united educational base for society. At that time, Parliament unanimously voted on the introduction of a defence curriculum in schools. At that point, we—the Ministry of Defence—were not happy, because it meant we had to provide teachers for every school. There was the period of introducing the



HOUSE OF COMMONS

system, but this year, from September, will be the first year when it will be mandatory for all schools to have this curriculum. There is basic military training, some elements of critical thinking, some cyber knowledge and things like that.

Q62 **Sarah Atherton:** One last question: how did you manage extremist organisations within Latvia who themselves could have been seen as a grey zone threat?

Mr Garisons: That situation is probably a little bit different in Latvia than in the United Kingdom. We have mainly Russia-oriented groups—we had them, but after the war started Parliament amended a law to prohibit those who support the war in Ukraine and who glorify Russian actions in Ukraine. Organisations who did that were prohibited after that, because hatred and propaganda of war are prohibited.

Chair: I think Jesse and Emma want to come in. Jesse, would you like to come in first?

Q63 **Jesse Norman:** Thank you very much, Chair. Thank you, Mr Garisons. You are giving extremely interesting testimony. Could you talk a bit more about the internal internet? Is that a kind of virtual private network for Latvia as a country, in effect?

Mr Garisons: We can say, yes, to some extent it is a private network, but it is owned by the Government. You can use all the infrastructure that you have, but the idea is that you have an internal exchanger. So internal internet traffic is not going directly from me as a user, for example, to an outside source, but going through an internal exchanger. If your perimeter is broken or isolated you can use the external exchanger, but it is a requirement for critical service providers to be linked to the internal exchanger.

Q64 **Jesse Norman:** Right, so you have to be an identified Latvian resident or citizen to be able to participate.

Mr Garisons: Yes.

Q65 **Jesse Norman:** Would that imply that you can't participate if you are a Latvian overseas?

Mr Garisons: There is no need if you are overseas, because you most likely will not be able to access it.

Q66 **Jesse Norman:** You talked about teaching society to survive in a war, which I thought is a very helpful thing. Obviously for reasons of geography and history, there is a seriousness about what you are facing vis-à-vis Russia, which is not directly at the forefront of people's minds in this country, but perhaps should be. There is a public debate about what that means in Latvia, from what you have said. How would you compare the kinds of preparations that you have made with what you see in the UK? What things should we be doing if we are going to take the threat from Russia with the same kind of seriousness as you have?



Mr Garisons: Of course, I think everything depends on threat perception, and that is greatly different in different countries. Once you have threat perception, as in our case, the public require action and a lot of explanation. On numerous occasions, the public say that they don't know where the bomb shelters are and things like that. That is what they are asking us now.

In our experience, there are a lot of issues when it comes to information warfare, because there is a lot of malign influence going on through different media or fake news. That would be one thing, and the UK can probably take a lead on some of those issues. I am a historian by education, and I studied what was done with the media and broadcasting in the cold war. I was 16 when I was listening to Voice of America and the BBC. We could get it in the '80s.

Another thing is critical infrastructure and critical services. We understand that you have to protect them. Even if it is a private company but it provides a critical service or produces critical goods, you have to ensure that it is not taken over by hostile companies—your enemies. Therefore, we introduced a system where critical services, critical infrastructure and critical companies are reviewed, and they can be prevented from selling their shares to hostile countries. The same goes for critical infrastructure properties in order to avoid, for example, somebody from a hostile country buying the land just next to where we have developed a military base. We also introduced a clause that requires the Ministry of Defence's consent when the owner tries to sell a property that it is in the protected area of a base.

Q67 **Mrs Lewell-Buck:** Morning. We know how difficult it can be to co-ordinate different Government Departments, let alone bring in the private sector and then bring the public with you. What was the most challenging aspect of the development of your comprehensive national defence, and what challenges remain?

Mr Garisons: I would say the most challenging was the beginning. It was challenging to understand each other, so that we on the military and defence side conveyed the right requirements to the civilian side. I think our misperception was that everybody understands what it means to operate in times of war, but that was not the case.

Therefore, we developed one possible scenario and declassified that scenario. Then we provided this scenario and all our assistance to different groups, including private companies, and we facilitated different gamings. Through those gamings, they started to understand what it means to have continuity of work, continuity of services and things like that. Otherwise, they had an issue of even understanding the core of that and what we required from them.

Since that, more and more companies started to approach us. Once that ice was broken, if I can put it that way, they started to actively develop their own agenda, and it was more easy. For example, the financial system and banks are now developing the system where they would



HOUSE OF COMMONS

provide the payment card services, even if there was no internet connection, and things like that. But that can be a problem not only for war; it can also be a problem in any other scenario where you do not have electricity or something happens with the internet.

Q68 John Spellar: Clearly, a lot of what you are undertaking has been shaped by geography and history—your geographical proximity to Russia and of course your being part of the Soviet Union—and therefore that creates a greater perception in society of threat and also necessary action. I am still trying to get a grip of where the centre of gravity is. Where is the real driving force across society? Where does that lie within the system? Is there a national security council that drives that?

Mr Garisons: Actually, it is the Ministry of Defence. You have to co-ordinate all those actions and bring them together. We have had different exercises in the last 10 years, including the Government's exercises. The Ministry of the Interior plays the leading role in civil defence, but it is only co-ordinating things like the health system and, for example, the conflicting road use for military and civilian purposes. The Ministry of Defence would then take the leading role in co-ordinating and making sure the system actually works.

We took the Finnish example. They have this total defence council chaired by Ministers and also an executive of permanent secretaries. In that framework, we deal with all those different issues and whatever comes up. Also, there are different committees where, let's say, the Ministry of Transport is responsible for railway services and transport. But that is still co-ordinated by the Ministry of Defence.

Q69 John Spellar: That is very helpful. A lot of that is about almost physical planning. You also referred to the Voice of America and the BBC, and all that structure during the cold war and even going back to the second world war, when we had the Political Warfare Executive and similar actions from the United States operating right across the spectrum and a wide range of society. Do you have any capacity in that regard? What is the extent to which it ranges much wider than normal civil service specialists in bringing in journalists and people with political understanding? You will understand much better than us that in dealing with what is basically still a Leninist mentality, the political struggle is enormously important in that context.

Mr Garisons: I think it probably looks more difficult than it is in reality. When we started this comprehensive defence, my intention was to avoid as much of that paperwork as possible, because sometimes the European Commission produces a lot of papers, with one paper replaced by another review, and we do not get to the practical terms. Actually, it does not require so many resources. On the Ministry of Defence side, it is more about the ability to formulate requirements and whether they are needed for different organisations and to facilitate that process through gaming and engagement. It does not require a lot of money or human resources.

Q70 John Spellar: My final question: how do the traditional military react to



HOUSE OF COMMONS

this expansion and change of role from what, in many cases, they would regard as proper soldiering?

Mr Garisons: I think initially there was a bit of confusion on the side of militaries, but then we expanded military exercises and expanded outside the areas of traditional training ranges. For more than five years, a lot of military exercises have been going on in the real environment and real geography, outside training areas, and they started to understand that they need to communicate specifically. For example, a lot of interaction is needed with the municipalities, because in our case the municipalities will be in charge of things like providing critical services, water, food and evacuation, if it is needed.

We also understood that there is a completely different meaning of civil-military co-operation, or CIMIC, as it was previously used in Afghanistan or Iraq. Basically, as local commanders you have to talk to people. Even if the operation goes on, you have to talk to people, municipalities and those in charge. Now, since we took the decision to go back to conscription, that will of course change the calculus, because more and more youngsters will go not only through that defence curriculum in schools, but through conscription.

Q71 **Mr Jones:** Can I pick up on the role of reservists in grey zone activity? What are their roles in delivering the overall strategy? We usually see reservists as members of the armed forces who do "military activity". Are reservists used in your system across industry and across the piece?

Mr Garisons: As we reinstated conscription, the reserve system is actually now under construction. There will be more and more reserve units. In our case, it is the National guard that is a voluntary force; it is territorially based and it has more of the military than are in the professional or conscript armies right now. There is a system where we allow those local battalions to be engaged in providing support to local municipalities without higher approval; if it is 50 soldiers, the municipality can get that support immediately, and there is no need to request permission.

Q72 **Mr Jones:** Is that broader than just defence? For example, would it be for civil emergencies and things like that?

Mr Garisons: Yes. We also understood that there might be the problem of providing the manpower for the protection of critical infrastructure. We therefore also introduced that big, critical companies can establish national guard units. When they finish basic training, they would be assigned to have the specific task of protecting that infrastructure.

Q73 **Mr Jones:** So in that case, for example, a large power station or telecoms company could have its own unit.

Mr Garisons: Yes. Actually, the first unit was for the Ministry of Defence; I was in that unit myself. The weapons were also stored in the Ministry, and the point was to have a very quick reaction if needed. The second unit was established in the biggest telephone communications company.



HOUSE OF COMMONS

Q74 **Gavin Robinson:** Good morning. What other good practice examples of total and comprehensive national defence have you witnessed in other countries?

Mr Garisons: If you look at Europe and where we seek advice, the first model is Finland, because they kept their total defence system alive throughout the last decades. They have a fully working and comprehensive total defence system. Outside of Europe, it is Israel and Singapore. Those are the three countries that we have analysed and find the most useful.

Q75 **Gavin Robinson:** Nationally, do you have arrangements with Finland, Israel and Singapore? Do you have accords? Do you have formal arrangements where you draw on one another's experience, or is it more ad hoc and informal?

Mr Garisons: No, we don't have formal arrangements, but we did a lot of consultations with all of them around establishing different elements in total and comprehensive defence.

Q76 **Richard Drax:** Good morning. Are there any aspects of comprehensive national defence that might be appropriate for enhancing the resilience of the United Kingdom, and does that strategy have weaknesses? I read in my notes that the main goal of comprehensive national defence is to prepare the Latvian population to do four things: defend the country; facilitate efficient crisis management at a national level; support the critical functions of the state; and ensure continuity of Government, which involves both military capabilities and the sustainability of society. Looking at us, do you think we are in that position, or do we have a lot to learn?

Mr Garisons: I think you have great experience from the Second World War and the Cold War. Sometimes we simply forget about those things, about what we have had already. I probably was not so fortunate; I had Soviet experience in my childhood.

I think that part of this is those issues that I have already mentioned: information security and information warfare. We have also established a cyber national guard unit, which invites IT experts from the private sector to join the unit. It is like a Reserve force for times of crisis, because it is very clear that we will not be able to provide all full-time soldiers or full-time experts to combat major cyber-incidents. Therefore we have developed that cyber unit, which is actually a mutual effort. It is more like a public-private partnership. Those IT experts gain knowledge and experience and we provide for them training that you cannot get in the civilian sector. They have trained already for some military operations, but they can of course use those skills in civilian life as well.

Q77 **Richard Drax:** From your knowledge of the United Kingdom, can you comment on this issue? You are talking about a sort of militarisation of your country so that civilians and others are brought into it and children are educated about the threats. That does not happen here to that degree, but we are farther away from the main threat, which in your case



HOUSE OF COMMONS

is Russia. In your view, from your experience of this country, are there many things that could enhance our defence better?

Mr Garisons: The one issue that I think is important in the current environment is that at least a few values of the society have to be shared by everybody or at least the majority of society. That is also the meaning of the education system changes and many other things, because if you expect your people to be ready to sacrifice for the country, they have to share something in common. I think that probably you can better answer that question yourselves: what are the values in common in your society?

Q78 **Richard Drax:** Does the strategy have any weaknesses?

Mr Garisons: Well, of course, there are the human weaknesses. I always think that much depends on the human factor, because the Government's ability—

Q79 **Richard Drax:** Sorry to interrupt you. The question is whether the country gets behind the idea. Is that what you are saying?

Mr Garisons: No, I was talking more about decision makers. As you know, we had a bad historical experience in 1940, when we had an army of 130,000 and there were many other quite capable militaries, but on a political level it was decided not to fight the Russians. That left quite a significant trauma, in our perception. Therefore, five years ago, the Parliament amended the National security law and now it says that basically units are obliged to fight—this is because of that psychological trauma—if there is a military aggression against the country. They have to fight, according to the approved plans. It might not be a centralised political decision to start resistance.

Q80 **Richard Drax:** Finally, is it leadership from the top—from business people and the politicians—that is needed to bring the nation to a point where they fully accept that there is a real threat, they are prepared for it and, in the event of something going wrong, they can all lend a hand to do something to combat the enemy, whoever that enemy is?

Mr Garisons: Yes, exactly. In both peacetime and wartime, you have to have leadership who people believe in and who can lead, because it is also most likely that there will be very difficult decisions to be taken.

Q81 **John Spellar:** To what extent are the Russians trying to undermine public confidence in the policy and the system? If so, how have they gone about it and how successful have they been?

Mr Garisons: Starting from the last part, I think they have not been successful for different reasons. The main reason is because we have been working quite hard on establishing a dialogue with society. That is very important. What they are doing is no surprise. There are information operations happening on a daily basis—psychological operations. To deal with that, we discovered that it is important to train journalists, because journalists have to recognise that there is a Russian influence operation going on.



HOUSE OF COMMONS

Of course, there is a lot of small details that you have to introduce, including those security requirements for members of your armed forces not to visit Russia and Belarus to avoid any kind of problems afterwards. It is not only your information security that can be explored or developed in information operations. We have seen those information operations where German generals are talking about Taurus missiles, and that was later on developed. We provided them basically—not what the Russians developed—with facts on one occasion. Therefore, we have to avoid that and train the journalists and public to understand where those operations are.

Q82 Mr Jones: Just picking up on John's point, the problem with misinformation at least over the internet is that it is very quick. It is not just the internet; it is social media and things like that. How do you react to that and try to counter that, because it has to be done very quickly, hasn't it? Is that done centrally, or is it just because you have fed it into the ecosystem?

Mr Garisons: I would say, and this is my personal opinion, that when I started in 2015, 80% of all daily communication was more like crisis communication, where we reacted to some kind of events or Russian operations—things like that. But that should be done anyway. You have to monitor your information space, including social media. You have to recognise it and then either explain to the public or react in different ways, but basically you have to explain it.

What is most important is to have proactive communication and to inform in advance on many things, because if our public are informed, they will not pick up some kind of strange article. When I finished, the situation was vice versa: 80% was proactive communication and then 20% was crisis communication. That is the most important tool to combat any malign information operations. Simply, it is about your people not reacting to those kind of articles. My most famous example is the US think-tank RAND, which developed research announcing that Russians would be in the capital Riga in 72 hours. Of course, that immediately has an enormous impact on a society, because people will say, "Well, everything is already gone." You have to deal with that by explaining the situation before. Once they believe that you have sufficient defences and things like that, such things will not go viral.

Q83 Mr Jones: So part of it is actually educating your public to become critical of the stuff that they are getting on the—

Mr Garisons: Educating and informing. They simply have to be informed.

Q84 Jesse Norman: You will remember that in that great attack column that was sent towards Kyiv by Russia at the beginning of the Ukraine war, many of those tanks had the dress uniforms of soldiers because they were expecting to be in the capital within a matter of hours, and how wrong did that prove? Your point about the danger of viral misinformation or taking something the wrong way is very well taken, as is your point about public leadership and communication. Now, in a relatively small



HOUSE OF COMMONS

state—

Mr Garisons: Very small.

Jesse Norman: Where people tend to know each other, or know someone who knows someone, there is a high level of social trust and social cohesion. Therefore, there are potentially forms of social pressure that can give feedback loops before some of these ideas get out of the loop. When you have a bigger country, with a much more diverse, vibrant and highly—frankly, in many respects, for the best historical reasons—challenging media environment, do you have any suggestions about how that kind of local connectivity and trust should be maintained?

We had a very interesting conversation yesterday with a NATO official who reminded us that, in a world of escalating AI, you are going to get to the point relatively soon where very little on its face will necessarily be believable. Almost anything could be a deepfake. He said, “Look, you better forget Zoom. Get used to spending a lot of time with people in the same room.” Does that strike a chord with you? You might want to talk a little about what the implication of that might be for a country like ours.

Mr Garisons: Of course, if you are a small country, it is easy. There is no issue on that. Still, I think it is about the basic of principle of having leaders—not only political leaders but the media—who are trusted and informed sufficiently. You have to have local municipality leaders who are actually informed and can address their constituencies and the people. You have to choose how you deliver your message. For example, 10 years ago, we started organising seminars for pupils in schools to talk about defences. We realised that basically the teachers were even more uninformed and vulnerable. We then thought, “Well, let’s talk to the teachers because then it is easy to discuss and convey a message to them, which they will then convey to the pupils.” Of course, that is more difficult in a bigger country, but I still think that is the way in which you deliver the message.

Chair: Thank you so much. That was a fascinating session. Thank you very much for coming and spending time with us today—it is very much appreciated, Mr Garisons.