International Relations and Defence Committee

Corrected oral evidence: The Arctic

Wednesday 5 July 2023

10.30 am

Watch the meeting

Members present: Lord Ashton of Hyde (The Chair); Lord Anderson of Swansea; Lord Campbell of Pittenweem; Baroness Coussins; Baroness Morris of Bolton; Lord Soames of Fletching; Lord Stirrup; Baroness Sugg; Lord Teverson; Lord Wood of Anfield.

Evidence Session No. 10 Heard in Public Questions 113 – 120

Witnesses

I: Dr Sidharth Kaushal, Research Fellow, Sea Power - Military Sciences, Royal United Services Institute; Dr Lee Willett, Independent Writer and Analyst.

Examination of witnesses

Dr Sidharth Kaushal and Dr Lee Willett.

Q113 **The Chair:** Good morning and thank you very much for coming. It is very kind of you to spare some time and we appreciate you coming to talk to us, Dr Kaushal and Dr Willett. This is the 10th public evidence session for our inquiry on the Arctic and we are going to focus today on the threat to undersea cables and critical infrastructure in the Arctic and the High North; if you want to stray a bit further south, please feel free.

This is a public session; it is streamed live on the Parliament website. A transcript will be taken and we will send you a copy so that you can check it is all correct. Can I remind all Members of the committee that if they have any interests pertinent to the inquiry to declare them? I ask the witnesses, when they answer their first question, to give a very brief introduction of their background; that would be very helpful.

There has been a lot of increased public discussion about the risk to undersea cables and other infrastructure. People mostly talk about cables, but there is obviously lots more besides. How serious do you think the threat of sabotage is by Russia—and by other countries, come to that? When Lord Peach, now a Member of this House, was Chief of the Defence Staff, he said that it represents "a new risk to our … way of life". Do you agree? Lastly, what are the consequences of that threat?

Dr Sidharth Kaushal: Thank you very much for your question and for the kind invitation to speak to you. By way of an introduction, I am the research fellow for sea power and the military sciences team at RUSI.

On the question of how serious the risk to undersea infrastructure is, I would say it is real but also a risk that should be contextualised. On the one hand, we should remember, particularly when we are talking about undersea cables—which was, of course, the subject of many discussions, including Lord Peach's comments—there is a significant amount of redundancy, particularly when one looks at transatlantic cable networks. A hostile actor would have to sever a lot of cables to have a meaningful effect.

It is also worth mentioning that, at the depths where damage to a cable would make rapid repair either difficult or impossible, there are relatively few assets that can target them. That being said, adversaries such as Russia have worked assiduously at developing some of these capabilities; for example, deep-diving special purpose submarines which are held under the aegis of the main directorate of deep-sea research, a specialised body which, though it controls submarines, sits independently of the Russian Navy under the direct control of the Russian Ministry of Defence.

It should be noted that, despite the redundancies I have mentioned, even partial damage to cable networks can be highly consequential. For example, studies that looked at disasters in cable networks that emerged as a result of natural calamities—earthquakes off Taiwan, for example—

gave us a rough sense of what a partial disruption to a cable network might cost in economic functionality. Roughly 60% of that country's internet traffic was shut down as the result of an earthquake back in 2006 which damaged some critical cables. It has been estimated that a significant disruption to a developed nation's internet services would cost roughly £23 million per day per 10 million citizens of its population, so this is not necessarily inconsequential.

There is also a specific risk to undersea cables that are used specifically for military operations, and here there is far less redundancy because we are talking about a relatively small number of secure cables; again, using natural disasters as a proxy for what the impact of adversary action might be. We might think of a 2007 event in which a cable used by the US DoD was disrupted, again, for natural reasons; this had the effect of shutting down all American unmanned aerial vehicle operations over Iraq for a rather extended period. So there is also a very specific military risk, in addition to civilian infrastructure.

To go back to something I said earlier, there are a relatively limited number of assets that can actually target these cables at depth, even under the aegis of Russia's GUGI.[1] For reasons that I am happy to go through as the discussion develops, the GUGI may be facing its own strains as an organisation, given the many tasks it has to perform and the relatively limited number of highly specialised capabilities at its disposal, which might have the effect of somewhat mitigating the risk it poses to cables, especially if this is combined with appropriate countermeasures.

Thinking of other infrastructure, for example things like pipelines, which run through shallower waters, there may be a much broader number of assets that can target them in areas such as the North Sea. That might be an emergent vector of attack against critical undersea infrastructure, and a way in which opponents try to compensate for the fact that targeting cables, while still useful and something they are likely to do, may, for a variety of reasons, become more organisationally difficult because of the highly specialised assets one needs to do it.

Dr Lee Willett: Good morning, thank you very much for having me. I am delighted to be here. I am an independent writer; I write for myself on various topics, primarily naval and maritime. I have been doing that for about seven or eight years, in which time I picked up on the issue of the seabed cable threat as far back as when Lord Peach first mentioned it at the RUSI CDS lecture, I think it was. Prior to working for myself, I was at Janes for four years and, prior to that, at RUSI for 13 years. I know a couple of the Members fairly well from back in that time, so I am glad to be here to discuss a really interesting and very important and timely issue.

My personal view is that this is a clear and present danger and risk, especially in the context of what is happening in the wider Euro-Atlantic

[1] Russia's Main Directorate of Deep-Sea Research

theatre and specifically with regards to Ukraine. We can get on to this in more detail in due course, but if you look at the way that Russia has conducted itself in its activities in Ukraine, it has very clearly gone after areas of economic infrastructure, whether they be on land or wherever; it is an important part of their strategy.

One point that is worth bearing in mind with regards to the threat is the UK's particular situation. We have a geostrategic vulnerability as an island that not many others do. One could perhaps postulate that an adversary could seek to isolate an island to make a point to others of the capabilities that they can bring to bear in this. I wonder if that makes the cables risk in particular quite acute for the UK as a country, as opposed to many other NATO states, for example.

There are a number of perspectives to see this from, which we will get into as we work through this, but I will highlight and concentrate on one. When you think of the risk to critical undersea infrastructure, you have to try and balance how you assess this and whether you are coming at it from a peacetime or a wartime mentality. While NATO assets below the surface may be on more of a wartime footing than its other assets, NATO is not at war and neither is the UK. One potential adversary is clearly on a war footing and, depending on which side of that fence you are on, that can change how you might think about doing something. For example, do we have a concern today about a risk in a certain situation? We might then look at how we build deterrence against that threat over a number of days, weeks, months or longer. Adversaries at war may have a concern and try to decide to do something about it on that day. They are coming at it from a very different perspective; that is important to bear in mind when you think about this issue.

I would make three other points on the perspective of how to deal with the threat. Can you think about whether you can deter by being defensive in your capability to do this? Do you need to be more offensive? Do your capabilities need to be more overt or covert in how you do it?

The Second Sea Lord made a point recently on overt deterrence. Talking at a recent conference about the procurement of "Proteus"[2], he said, "The UK is being really clear that we're procuring a vessel that is capable of protecting our sovereign CUI"—critical underwater infrastructure. That was quite a deterrent message in itself; the Second Sea Lord saying, "We have a ship that is coming to do something about protecting this here and now". You have to look at things like the way in which you can do sensing underwater and how you might be able to use that from a technology point of view—that is, passive versus active sensing. There are a number of ways to think about the problem, from the strategic all the way down to the tactical and technological level.

[2] *Proteus* is the UK's first Multi-Role Ocean Surveillance (MROS) ship, purchased in January 2023 and scheduled to enter service later in 2023.

Is the UK prepared for this? Militarily, it is certainly very focused on it; in terms of the civilian focus, maybe not so much. This is about more than just the Nord Stream situation. Over recent years there has been a string of incidents, in none of which is there any firm public proof of who did what. There were the cable issues off Lofoten and Svalbard in Norway, there was the fishing vessel issue with cables off Shetland, and then there was the Nord Stream incident. Depending on what you think about who was responsible and how and why, you could maybe start to put together a bit of a pattern, all of which is very important. All those incidents are in the geographical area that we are talking about.

Is this a new threat? No; it is a long-standing risk but it is becoming an evident threat right now, perhaps because some adversaries are in a position where they can now do something about it. Consequently, the really important thing for me in terms of the threat and response is the deterrent element. Whether you are talking about the UK or NATO or others, it is about being able to have a deterrent impact today, because the threat is today. Assuming you believe the theories—NATO, for example, put the Nord Stream attack down to sabotage—the deterrence element in all this is very important.

The Chair: Lord Anderson, do you want to follow up?

Lord Anderson Of Swansea: Apart from the physical destruction of cables, presumably listening devices could be attached to cables which may be fairly difficult to detect.

Dr Sidharth Kaushal: That is certainly a possibility, though tapping cables, particularly at extreme depths, is in some ways a much more technologically sophisticated and complex task than actually severing them, which requires a complex platform but is quite a simple task; penetrating their sheathes and installing a device. These things are certainly within the realm of technological possibility, but surveillance tends to occur at or near cable landing sites, precisely because of the difficulty of gathering data underwater at extreme depths.

That is not to say, however, that this cannot happen. There is good historical precedent for what you have described. Operation Ivy Bells comes to mind as a particularly prominent historical example, where the US Navy tapped a series of Soviet naval cables underwater using special purpose submarines and gathered a great deal of data on the activities of the Soviet Pacific fleet, so it is certainly within the realm of possibility. The only caveat I would add is that of the things an opponent could try to do, it is on the more complex side. That might be a limiting factor.

The Chair: It also cuts both ways; we do it too.

Dr Sidharth Kaushal: Absolutely, and we have in the past.

Dr Lee Willett: Taking Dr Kaushal's previous point about the numbers of cables and the redundancy in capability, NATO pointed out in a briefing that there are 400 cables, of which it sees 200 as critical and worth

focusing on. Therefore, the range has already come down, but that is still a lot of cables and a lot of distance that those cables cover. Your question raises the interesting point that there are ways in which you can go down and look at who is doing what to your cable, of course. You can send down ROVs[3] and have a look, but that is rather reactive. If you go down and find that somebody has done something down there, then by that point the damage has already been done.

Part of the capability challenge for me going forward is figuring out how you can develop a deterrence posture to deter people from wanting to do that in the first place, but that is by definition the nature of the problem. In such environments, at such depth and over such vast geographic expanse, it is difficult to generate such extensive coverage from a surveillance and sensing point of view.

Q114 **Lord Stirrup:** Good morning, gentlemen and thank you very much for your evidence. We have already moved into several other areas of questioning, including the one I want to focus on, which is Russia.

First, the 2021 defence Command Paper said that Russia was developing "deep-sea capabilities" that could threaten undersea infrastructure, and we do not expect the forthcoming defence Command Paper refresh to say any different. Dr Kaushal, you have already talked about some of the capabilities that Russia has been developing, but could you just give us some evidence on what they do? We have said that listening is rather difficult, but you said cutting them is easy. What do they actually do down there? What sort of capabilities have they developed? How would they be applied in practice?

Secondly, can we move the focus a little back to the Arctic? We have talked about cables in general, but we have had evidence from other witnesses stating that there will be a lot of nations trying to put down undersea infrastructure in the Arctic because it offers a great many advantages. Presumably, as that infrastructure is mostly going to be new, it will not be as redundant as, say, transatlantic infrastructures which have been there for a long time. Would it perhaps be rather more vulnerable?

Thirdly, we have also had evidence showing that even in an era of global warming, operating in the Arctic is not nearly as easy as a lot of people might think it would be. But presumably, if you are operating undersea, it probably does not matter whether you are in the Atlantic or the Arctic, does it? Is the environment any more demanding in the Arctic for undersea operations? Perhaps you could start with those.

Dr Lee Willett: There are a couple of points about the capabilities and what they could actually do. If you look at the case of the Lofoten cable off the Norwegian north-west peninsula, about two or three years ago, there was a chunk of cable removed; according to the media reports, the section removed was about 4 kilometres long.[4] The cable is potentially as

[3] An ROV is a remotely operated vehicle

[4] During the oral evidence, Dr Willett mis-spoke and referred to the removed section

thick as your forearm, but that is still a lot of cable and a lot of weight that was removed, including being pulled away from the fixing points, and a chunk of it was found somewhere else.

Lord Stirrup: Was this done by a deep-sea diving vessel of some kind?

Dr Lee Willett: This was done by something. According to the reports, which included coverage of what the Norwegian Government said about it, a large chunk of cable—up to 4 kilometres—was physically ripped out and moved quite a way. That is an example of the kind of challenge and capabilities that somebody could have, if that is what did it.

From my perspective, the important point to make at a slightly higher level is that a country like Russia has a wide range of capabilities that could be involved in this kind of thing, and that is part of the problem. It has anything from a brand-new submarine that can go down to great depths and deploy mini submarines—some of which are nuclear-powered—to a whole fleet of surface ships that include intelligence vessels, surveillance ships or commercial ships. Even vessels such as fishing trawlers could be involved. There is a whole spread of systems where you could put a robotic vehicle on board and if you can do that and put it over the side, you can contribute to the threat.

Part of the problem is looking at a vast range of capabilities and figuring out which is the biggest threat. Certainly, particular Russian ships pop up all the time in this—the "Yantar", the "Admiral Vladimirskiy" and others—and those always seem to be around doing stuff. In fact, there is a report in the press this week of a Russian vessel being off the coast of Holland for about a week or so.

The Chair: Are they around in the Arctic?

Dr Lee Willett: I could not tell you without having a closer look; Dr Kaushal might be able to come back to you on that one. The issue for me, in terms of what you can see from a surface ship perspective, is that there is a pattern in the Russian activity, in that there will be a group of ships remaining in a certain place for a period of time, as was seen off the west coast of Ireland about a month or so ago.

As regards your question about the Norwegian side, your point about the new infrastructure going down there is most important because there are not many cables that transit that region. One of the key issues will be the concern about critical undersea infrastructure that relates to resources—the oil and gas pipelines coming south from there.

Regarding your point about the operating environment up there and how difficult it is, from a defensive point of view in terms of trying to deter threats to anyone seeking to challenge or disrupt CUI up there, there is a lot of work going into the impact of climate change and how it changes the fundamentals of things like anti-submarine warfare. You have melting

---

being 11 kms long. The transcript has been corrected to reflect the correct length.

freshwater mixing with the seawater and changing the densities and thus the acoustic layers underwater, so it means the experience you had of operating in the Arctic in the Cold War and what you understood about the environment is now different. At a time when you have to maybe start looking around in your submarine underneath the Arctic ice to see who is there doing what, the way in which you did it has to be relearned all over again.

Dr Sidharth Kaushal: I will pick up on capabilities first to extend on what Dr Willett said. It is useful to bifurcate the Russian capabilities into the two organisational frameworks within which they sit.

The first set of capabilities are a highly exquisite suite of things such as deep-diving mini submarines, things like the "Losharik" and the X-ray submarines that are purpose built to operate at extreme depths. They are titanium-hulled and typically launched from larger mothership vessels such as the "Belgorod", a stretched Oscar-class submarine, which acts as a host both for these deep-diving mini subs and, potentially, a range of unmanned assets. These assets are typically equipped with manipulators and are rated to operate at particularly extreme depths. They sit organisationally within the main directorate of deep-sea research and their personnel, who are fed into the directorate through the Russian Navy, are also a particularly special breed of person.

To be qualified, one has to have served five years as a submariner, following which one goes through a course that was designed on the basis of Soviet cosmonaut training and enters the 29th submarine division, which is the feeder division for this organisation. There are relatively few people and assets within this organisation that can do what is required but they are highly specialised; these are the capabilities the Russians would use to go after the hardest targets, particularly those that require the ability to operate at extreme depths.

As Dr Willett said, there is also another suite of capabilities which actually sits under Russian naval intelligence. It answers in turn to the fifth directorate of the GRU, Russia's military intelligence, and its director is typically deputy director of the GRU. Historically, during both the Soviet era and the contemporary era, Russian naval intelligence obviously provided operational intelligence with its own surface vessel; that includes the Akademic-class "Admiral Vladimirsky", which is not a GUGI asset but rather a Russian naval intelligence asset. But it has also maintained relationships with civilian actors as well as manning auxiliary vessels.

One could not necessarily damage infrastructure at very critical depths with these capabilities but what one could use them to do, as Dr Lee said, is surveil and potentially impact infrastructure in shallower waters, for example, areas of the North Sea or coastal areas or EEZs where the process is less technologically sophisticated.

I would note that sabotage is not the GUGI's only function; it has a range of other tasks, including laying Russia's undersea sensor networks to

protect its own SSBNs[5], the Harmony network, which is a rough analogue to the American IUSS[6] network. It also has responsibility for surveillance around Russian waters. Finally, it has recently taken on responsibility for testing the Poseidon nuclear torpedo which will be mounted on the "Belgorod", one of its submarines.

That is actually an enormous organisational strain on a body that cannot hire very many people just by virtue of what it requires them to be capable of doing because, in particular, testing of this nuclear capability has required assets such as the "Belgorod" to be devoted to testing the torpedo rather than active duty. It also means that when mated with the Poseidon, potentially the "Belgorod" will sit under the Russian Pacific fleet rather than the GUGI, which will have lost partial control over critical assets and people. When one combines that with other incidents we have seen in previous years—the fire aboard the "Losharik" in 2019, which killed a number of Russia's hydronauts—and some organisational difficulties, it is possible that the very exquisite undersea component of Russia's capacity for sabotage is coming under real organisational strain.

The decision to shift to surface vessels such as the "Yantar" is interesting in this light. On the one hand, it is equipped with a very exquisite sensor suite and has the capacity to launch a number of remotely-operated vehicles, as we know, but what the "Yantar" does not have, which submarines do, is the element of deniability. If it is seen loitering as a well-known asset around infrastructure that is eventually damaged, everybody knows who did it, so it is actually a very curious capability investment choice. One way it might be interpreted is that, as an organisation, the GUGI has certain standing tasks, which it simply cannot meet with an overstrained force of submariners, and has opted for second-best solutions to meet some of its standing obligations.

This takes us to the second point; we might see much more of an emphasis as a consequence on shallow-water sabotage, going after easier targets that may be easier to repair but also easier to disrupt at scale and require less specialised vessels to do so, partially as a consequence of this organisational strain on the most exquisite capabilities in the Russian force structure, particularly the GUGI.

Moving on to the subject of the High North, I would largely echo what Dr Lee said. I do not have much to add except that, in addition to the fragility of new infrastructure as discussed, one might also consider the fact that it will likely converge on landing sites at a few key points, for example Svalbard, which could be an additional point of consideration.

Q115 **Baroness Coussins:** You have both referred to some reports of disruptive activity, but I assume that public information must be limited and, in any case, attribution can sometimes be notoriously difficult. I wonder if you could say a little more about your assessment of the significance of Russian efforts to survey, disrupt or hack undersea cables

[5] Nuclear-powered ballistic missile submarines
[6] Integrated Undersea Surveillance System

and, from their point of view, how effective and successful any such activity has been. Is anyone else engaged in similar activity, China for example? Finally, what is your assessment of whether there is a realistic threat from non-state actors in this activity?

Dr Lee Willett: If I may jump first on that last point, in 2013, I believe it was, the Egyptian Navy arrested three divers operating from a fishing vessel off Alexandria who were diving down to supposedly cut one of the cables that was running into that city. If you look at a map of where the cables come ashore, Alexandria is quite a hub. There was a reported case in the mainstream media that three divers operating off a fishing vessel went down to have a go at a cable there; it is not known who they were or what the reason was. Going to your point about the range of actors that could try to do this, there has been very early evidence. That was one of the earliest examples in recent memory of somebody trying to do this. In answer to the question, yes, the threat is potentially all-encompassing, going from a state actor to a non-state actor.

In terms of the messaging, just a quick point from my perspective; Lord Peach's statement in 2017 was quite striking because it was the first time that the cables issue had been mentioned publicly, although it would have been known for a long time as a potential issue. Along with other undersea warfare aspects, that was the thing in the room that no one talked about; everyone knows about it in various issues of national interest and other things, but it just was not spoken about. We have seen a steady increase in senior UK, US and other military officers making fairly public statements about it since then. The importance of that is the messaging at a political level that this is a significant issue; it has been an issue for a long time, but now the actual threat is coming to pass.

As regards the significance of the Russian efforts, balancing the point that Dr Kaushal made about redundancy against the point we both made about the difficulty of doing this, it seems to me that there is a significant Russian focus on it. The Norwegian Chief of the Navy said at a conference recently, effectively, that you can look at the problems the Russian armed forces have been having in Ukraine and park those, but the Norwegian view is that the Russians have been investing more heavily in their navy—and there is no suggestion that that navy would have a similar operational problem. Their perspective would be that Russia is prioritising naval activity like this.[7]

I think you could say that Russia is focused on it; the fact that western navies are now rushing to deal with it, for example with the UK bringing a ship into service in six months, is a sign that there is a real concern about a potential problem that must be addressed and dealt with. The example of the conflict in Ukraine showing that Russia is prepared to target civilian infrastructure suggests that there is not really a threat that is off the table, so the concern amongst western powers has been that this is a real threat.

[7] This speech, by Rear Admiral Rune Andersen, was given at the RUSI seapower conference in London in April 2023.

We both mentioned the ship "Yantar", for example; when you deploy "Yantar" or another ship and sit it in a certain location for a certain time, you can just send a message to NATO, the UK or whoever that you have the capacity to do this. From the Russian point of view, if you talk about the threat being made up of four components—the capability, its credibility, communicating that capability and then showing intent to use it—you can make the case that Russia ticks all four of those boxes.

Dr Sidharth Kaushal: In terms of Russia's intent, it has been clear that Russia sees the ability to inflict what it describes as dose damage as a means of what it would call war containment on its periphery—ensuring that a local war with a neighbouring country does not involve a larger regional coalition—and one of their primary means of doing so is signalling the ability to target critical national infrastructure. That applies to how they think about using missiles, but also, as Dr Willett said, the ability to target critical undersea infrastructure, and to signal that they can do so, is a major part of their approach to inflicting that calibrated damage on civilian lifestyles that it effectively entails.

I would subdivide the Russian threat by depth, because there are different threat types at different depth levels, each of which has a different set of mitigations. At extreme depth, the special purpose assets we have discussed pose a pretty significant challenge to NATO deterrence. Interestingly, that is particularly true in peacetime rather than wartime because, in wartime, tracking something like the "Belgorod", a converted Oscar-class, is not a simple ASW task. But NATO navies have for a long time planned for tracking Russian submarines, and, frankly, the same suite of capabilities that we would use against any other type of submarine applies against it.

In peacetime, rules and permissions are somewhat more complex. If an adversary submarine is conducting activity of a non-lethal variety around critical infrastructure, that is a slightly more complex challenge to deter. The tools of deterrence are much more constrained by policy restrictions, amongst other things, as indeed are the tools of attribution, because the maritime assets that could attribute, for example, damage to a Russian special-purpose submarine might well be of a highly classified variety. This means that getting information into the public sphere, which might then allow some of the other punitive tools of statecraft sanctions, for example, to be used as part of the deterrent, would be a more complex task; there is a gap in the information system.

That being said, the mitigation of the threat to really deep-sea infrastructure, which is very difficult to repair, lies in some of those organisational weaknesses that I mentioned the Russians are facing: the strains on their hydronaut force, the organisational strains inflicted on the GUGI, the number of tasks the Russian Government have made it do, and the fact that they are having to rely more and more on surface vessels, which are much more deniable. That might be a partial mitigation, which could be viewed as a basis for longer-term policy when it comes to the deep-water threat. In shallower waters, there are a range

of assets that could target things like pipelines, in particular; potentially cables as well, but things such as pipelines are particularly at risk.

If the Russians are relying on auxiliary vessels and targeting infrastructure that lies within national exclusive economic zones, there are legal grounds for restricting the freedom of action of ostensibly civilian vessels under UNCLOS if, for example, there is a suspicion that they are conducting research relevant to economic activity within a nation's EEZ. That might be one way in which nations might restrict the activities of unbadged or clandestine auxiliary vessels, effectively using that status against them.

When it comes to naval vessels, things like the Akademic "Vladimirsky", fewer options exist to do this because they have the freedom to operate in a nation's EEZ under UNCLOS, so long as their passage is innocent. Equally, these assets are more visible and their activity around infrastructure is easier to detect, publicise, and, on that basis, create an evidence base for whatever punitive action a Government might choose to take. It is kind of a federated threat and for each component of that federated threat there are mitigations, but they require very specific tools.

To the second question about China, there is some evidence that China sees severing undersea cables as potentially useful in a conflict. We have seen potentially the PLA severing cables using trawlers off Taiwan's Quemoy and Matsu Islands, though of course China would deny that this is the case. So there is some evidence that, as an actor, China sees this as useful.

However, it does not appear to have built the same very specialised suite of deep-diving capabilities that Russia has; indeed, much of China's approach to undersea infrastructure, and gaining in particular some of the informational advantages that were mentioned earlier, have come rather through the avenue of investment. Chinese state-owned companies are trying to build themselves a larger and larger stake in the globe's undersea internet pathways and pipelines by laying more and more of that critical infrastructure, which is another indirect way to conduct things like surveillance without recourse to those sorts of special-purpose assets. It would appear that the Chinese approach is quite different from the Russian one.

On the point about non-state actors, I would not have much to add to what Dr Lee said. The Egyptian example is a particularly good one of how, particularly in shallower waters and near landing sites, even non-state actors can definitely pose a threat.

Lord Teverson: I have a couple of points of clarification which require only short answers**.** Baroness Coussins asked about surveying. Presumably, it is completely public knowledge where all these cables, interconnectors and pipelines, actually are, if only to make sure that other quite innocent actors do not damage them; I just want to see if that is actually the case. Which ones are purely defence related? I

understand all the sensors to try to determine what submarines are going through whatever gaps in the North Atlantic or whatever, but what are specific defence assets underwater, and do nations know exactly where those are as well? Please give brief answers.

Dr Sidharth Kaushal: As you said, there is quite a lot of data in the public space on the civilian infrastructure. When it comes to defence use, as you said, things such as the datalinks that allow information from undersea hydrophones to be transmitted to command centres, but also many of the datalinks that enable transatlantic communications, which are quite critical for NATO, would be examples of the sort of undersea infrastructure that are very defence-specific. The locations of those cables are not public, but it is the sort of thing that I imagine adversaries have made quite a lot of effort to surveil over the years.

The Chair: Are you saying that our Government know where every single cable in the world is?

Dr Sidharth Kaushal: I am saying that in the public sphere, the vast majority of civilian cables are known to most people; as to defence-related ones, I would not know what our Government's state of knowledge is, though I would expect quite a lot of effort was invested into that sort of thing.

Dr Lee Willett: As Dr Kaushal has started to clarify, there are different kinds of cables. Cables gets used as a generic term, but there are very different ones; on the military side, you have the surveillance-related cables and also military communications, but on the commercial side, you will have power cables, data cables and others.

As regards the mapping or the public knowledge, there are lots and lots of open-source information sites you can find that say roughly which cables run from where to where; these cables are laid by large commercial companies that have a website that says, "This is the map of our cables," so you can find those maps fairly easily. I would suggest the maps are not particularly precise because it is a long way between here and Australia, and having a cable that runs all that way does not tell you precisely where it is in the vastness of the ocean, but there are maps that can tell you roughly what sort of cables run through UK or northern European waters. This is quite interesting, or maybe concerning: if you were to look at a map of the cables and a map of other critical undersea infrastructure, could you identify certain areas in UK waters or elsewhere where there seem to be either critical nodes—connecting points—or a critical mass of various infrastructure running through it that present perhaps more particular vulnerability than others?

This connects back to Baroness Coussins' previous question about China. Talking about the kinds of cables, there are NATO officials who have made the point that China's approach to this is very different in that it is looking to put in place infrastructure from a critical undersea perspective and a more defensive point of view, because it is looking after its own security. It has had its own problem because it has the US Navy on its

doorstep, and I am sure it would like to know what US Navy submarines are doing, so maybe it is putting down infrastructure to listen for that kind of threat, as opposed to trying to interdict anything that anybody else is doing. China's investment may be more on the specific point of laying sensing capability to understand what the US Navy is doing.

The Chair: Lady Sugg, part of your question has been answered, but did you want to follow up?

Q116 **Baroness Sugg:** Yes. You talked about deterrence and mitigation in general, but can you go into a bit more detail about what the UK and its allies can currently do, and what you think they might be able to do in the future, in trying to protect the subsea infrastructure, perhaps both on the shallow and the deep-water side?

Dr Lee Willett: A very interesting question. There is the issue now of deterring the clear and present threat and then building capacity to do that in the longer term. In the immediate term, the importance of collaboration at a multinational level is critical, and that is one thing that potential adversaries of the West do not have.

From a sub-surface deterrence point of view, you have the US Navy, the Royal Navy and the French Navy operating together in the North Atlantic. They are probably three of the most capable submarine navies in the world. You have three navies with their collective submarine presence that can bring a deterrent and a sensing effect to deal with that issue. To what extent they share information on such critical issues is a really important point. One thing that needs to be considered going forward, when you have a clear and present threat like this, is whether that is going to encourage countries to get over some of the barriers to information sharing on critical things like underwater matters, which has always been a no-go for sharing information, or at least there were limits to it.

It is also important to think about collaboration with industry. Going back to briefings that I heard from the Norwegian Chief of Navy—it is worth making this point because the number is quite interesting—he was talking about the Nord Stream situation and what the Norwegians did in response. They picked up the phone to the commercial industry—the oil and gas sector, which in that part of the world is very significant—and asked, "What sort of numbers do you have in terms of remotely operated vehicles and others that could help with this?" and the answer was, "600". There is a very significant amount of capability in industry if you can seek to collaborate with it.[8]

This is where you look at the points of co-ordination between countries and between sectors. The NATO cell that has been established in Brussels is designed to lead that political and strategic level co-ordination; to encourage countries to talk, to encourage industry to get involved, and to

[8] This speech by Rear Admiral Rune Andersen was given at the 'First Sea Lord's Seapower Conference 2023', hosted by the RN in London in May 2023.

be a point of contact for industry. If a company is aware there might be a problem with one of its cables or pipelines, they would have an ROV that could go down there and do something about it and have a look, but they would not know where to go in terms of who to ask for help. NATO's Brussels cell is designed to be that starting point.

NATO is also in the process now of setting up what you might term an operational cell at Allied Maritime Command in Northwood in the UK, which is going to deal with the military operational side of that co-operation; the Brussels bit does the political level and the Northwood bit does the operational level, so that kind of progress is now coming together quite quickly.

Baroness Sugg: In your view, is NATO the best kind of facilitator?

Dr Lee Willett: Interestingly, NATO has the membership and the numbers. There are 31 members that can talk. It also has the established history of co-operating and the access to the bigger picture through broader maritime surveillance. It can be that hub, at the strategic and operational levels, to get people to start integrating.

Dr Sidharth Kaushal: I will build on a couple of Dr Willett's points. First, on the importance of public and private sector partnerships, I echo that wholeheartedly. Another example that comes to mind is the Italian Navy signing a contract with that country's largest internet provider to share data around the cables which it owns and operates; that is important both for building an information picture and having a link between what is publicly known and what can be gathered by classified sources. We saw this before Ukraine for the first time; the US Government could pre-bunk a lot of Russian claims without releasing its own classified sources by using commercial satellite imagery, so commercial imagery became the bridge between the bits of government that are ring-fenced, for good reasons, and the rest of the state.

We are in a similar dynamic here because a Royal Navy submarine that tracks something like the "Belgorod" in peacetime probably cannot sink it under peacetime rules of engagement. There may be other tools of deterrence—sanctions, for example, or various other constraints that could be placed on Russia—but an evidence base needs to be built for their use and the Navy cannot release its sources. But, for example, in the context of a public-private partnership that same data could be validated from a private sector source and therefore shared into the public sphere, much like commercial imagery. That could create a whole of government system for undersea monitoring, while sharing the data into the rest of government and using the rest of government's tools as part of the overall deterrent.

In terms of other areas where the risks can be mitigated, particularly when it comes to auxiliary vessels, there is a strong legal basis for mitigation. For example, the 1888 cable convention allows a vessel's captain to board and search any vessel on the high seas which it suspects of tampering with undersea cables; this is a right the US has exercised

before against Soviet vessels in the 1950s. In principle, a strong legal basis exists for interdiction against some of those more auxiliary, shallow-water oriented threats.

There would be a strong basis for multilateral co-ordination in both co-ordination between enough actors—so that no one nation bears the extent of political risk for this; there will be some—and information sharing because, ultimately, we are looking at clandestine vessels. There are a number of tools emerging, for example in areas such as machine learning, which could allow irregular patterns of vessel activity to be used to sift the signal from the noise.

In terms of frameworks for this, I agree with Lee that NATO represents a particularly useful framework. Potentially, frameworks like the Joint Expeditionary Force, which are optimising for the sub-threshold space as an area of complementarity to NATO, could also in theory be viewed as a basis on which the UK, in particular, could engage European partners on the Northern Tier to provide a more persistent presence than NATO perhaps can, at all times and in all places.

Lord Soames Of Fletching: I think Lady Sugg has effectively shot my fox.

Baroness Sugg: I do apologise.

Q117 **Lord Soames Of Fletching:** But further to the points you were making about interfering with the subsea infrastructure, of the incidents of damage to that infrastructure in the last few years where attribution has been contested or denied, how much do you feel that there is the knowledge available, albeit maybe not in public? Is it clear who has been the major actor in dealing with this? Further to the points you made in response to Lady Sugg, what options are open to the United Kingdom and its allies to deal with these matters in the grey zone, short of war?

Dr Sidharth Kaushal: In terms of attribution, depth is the great differentiator because, at certain depths, only a handful of nations can realistically operate and then it is quite easy to narrow down intent. If something was sabotaged at extreme depths, it would be very easy to attribute it to a given actor. The question, of course, would be whether proof—to a standard of evidence that would be needed to use other policy instruments in a punitive way—could be delivered. Given the very classified nature of a lot of the tools that would be used to attribute, that might be the more difficult part, and maybe where commercial sources could offer partial mitigation.

The Chair: Just for clarification, when you are talking about the extreme depths, is that mainly data? Does that include electricity or oil and gas, or are oil and gas at shallower depths?

Dr Sidharth Kaushal: It is primarily data cables that we would be talking about.

The Chair: I am never quite clear why an enemy would necessarily want

to cut all the data cables because they use them as well, sometimes for offensive purposes. Is that true?

Dr Sidharth Kaushal: That is true in terms of cutting data cables. Certain cables are critical to financial flows, for example, between specific countries so, to a certain extent, an opponent could mitigate its own risk whilst maximising it for another set of nations.

Russia's foreign minister, Lavrov, once described it as a minority stakeholder in globalisation and probably now even less of a stakeholder; presumably it feels less and less reliant on those systems of dataflow which underpin a globalised economy. That might make it much more willing to engage in this activity on the grounds that its own economy is developing in a somewhat quasi-autarchic direction, being quasi-dependent on nations like China, ergo it bears less risk from these sorts of events.

The third rationale would be that in a context where Russia thought it was fighting from a position of conventional weakness, it might simply see increasing civilian pain as the one way to offset these weaknesses. Even if it did inflict a certain amount of economic blowback on itself via what it has done, that might be seen as preferable to conventional defeat. Those are some rationales that you might think of.

Dr Lee Willett: I will make three quick points. There have been some arguments made by NATO officials that Russia does not rely upon some kinds of critical undersea infrastructure to the same extent that the west does, because of the geophysical nature of the country. It does not need to send a cable or pipeline from the North Atlantic round through Suez, the Indian Ocean and wherever else, up to the Pacific to do whatever it needs to do there; it just goes straight across its own landmass. It is a continental power so it does not have the same kind of degree of reliance on that infrastructure that an island country like the UK might, for example, so there is that geophysical difference.

Lord Soames, with regard to your point about the attribution of information in the public domain, if you look at some of the media reporting regarding the Lofoten and Svalbard incidents off Norway, in particular, the Swedish reporting of the incursion into its waters in 2014[9], and the Nord Stream incident, the public reporting has been clear in a lot of cases, including quoting the police sources and investigative sources involved, as saying there was human involvement—there was external involvement, et cetera. They have been clear in saying that somebody has done something, without necessarily saying who. One can make a case that, in the nature of the politics of language, by saying, "Someone has done something", they are leaving it up to others in the public domain to work out who. I suspect that some evidence that is known at a classified level may provide a clearer answer.

[9] In October 2014, the Royal Swedish Navy surged assets in response to what it referred to as "foreign underwater activity" in Swedish territorial waters off Stockholm.

One point about cables and undersea infrastructure as a whole needs to be looked at, in terms of what you do about security. When you think about a cable that leaves the UK and goes ashore on the other side of the world, for example, it passes through many different legal jurisdictions, different countries and open ocean. What comes up, as it has in the wake of the Nord Stream incidents, is the need for permission to go into somebody else's waters and look at something. In the case of the post-Nord Stream response, what has been happening is that needs must: "Yes please, come in and check it, and we will worry about the legalities afterwards". There is the issue of who owns the cable—the commercial company or whatever—whose waters is it in, and can you come down and have a look at it, for whatever reason? Those kinds of legal issues still need to be borne in mind.

Q118 **Lord Anderson of Swansea:** Gentlemen, the salience of the underwater cables first came to public attention in the lecture to RUSI by Air Chief Marshal Lord Peach in 2017, since when there have been greater attempts at international co-operation. In January of this year, NATO and the EU established a joint task force on resilience and critical infrastructure protection. In February of this year, the NATO cell was established, which has already been mentioned.

I see that the NATO Centre "will facilitate engagement with industry and bring key military and civilian stakeholders together". What can you say about the extent of international co-operation thus far; EU-NATO, or NATO generally? To what extent is that co-operation constrained by commercial confidentiality?

The Chair: Perhaps you could bear in mind that we have about 10 minutes left.

Dr Sidharth Kaushal: In terms of co-operation at a NATO level, things such as generating a shared situational awareness has been an area in which the alliance has already had some pretty significant extant capabilities and has progressed quite a long way. To echo a point that Lee made a bit earlier, the real challenges lie with the issue of national jurisdictions. Nations are willing to share intelligence but shared surveillance across jurisdictions, as well as efforts at things like repair, are still constrained by legalities and questions surrounding whether permission can be secured from a host nation quickly enough. That, much more than the question of commercial limitations, is the major limiting factor.

We have seen individual NATO nations have relatively little difficulty in engaging the private sector when they have wanted to; Italy and Norway stand out as examples. The private sector is willing to engage here, partially because its own infrastructure would benefit from greater security; the major challenge to me seems to be more a question of transnational co-ordination.

Q119 **Baroness Morris of Bolton:** Given everything we have been discussing, laying cables on the ocean floor must be a very specialised area, so who

are the main players? As well as Governments engaging with the private sector, are they also keeping a close eye on the commercial sector to see who is doing what and where the cables are going?

Dr Lee Willett: I do not have them off the top of my head, but there are some very well-established and well-known companies that take the lead in cable laying and are the major players. I would be very happy to refer back to other notes I have and let you know.

There is also the issue to bear in mind of those involved in the oil and gas sector, which is a different set of companies altogether. Since this problem first emerged in public discussion post Lord Peach's comments, it is interesting that there has been quite a lot of engagement with the commercial sector to see what technological capabilities it has that potentially have a military crossover. The commercial sector, for example from the oil and gas point of view, has been doing things like deploying ROVs to great depths, looking at technologies—stuff like how you can maintain an ROV down there using some kind of recharging capability—and at the kinds of vehicles they have to see if they have relevance from a defence point of view.

Ultimately, remotely operated vehicles are going to be a key part of this. There has certainly been a lot of engagement and sharing of understanding between the defence and commercial sectors on the technologies to get down there in terms of ROVs. It is a lot because they are the ones with the state-of-the-art knowledge.

Dr Sidharth Kaushal: There has not been as much of an effort to monitor who is actually laying this infrastructure in the past, but that seems to be changing. I would point to a recent example of the US threatening some pretty crippling sanctions on a Chinese company that wanted to be part of a consortium laying a cable between Europe and Asia, and effectively forcing it out of that consortium. There seems to be a growing focus on which companies specifically are involved in creating this infrastructure and whether they come from potentially hostile states.

Q120 **Lord Teverson:** Are there any further recommendations that perhaps we have not covered here, just those for the Arctic and the High North? Are we also being quite naive here, in that one of the best deterrents is that we can do back to them what they might do to us? I suspect we are doing exactly the same, but I take your point completely, Dr Willett: the Russian Federation is far less vulnerable on commercial cables, but maybe not so much on some of the military infrastructure.

Dr Lee Willett: Without sounding too trite about this, since a lot of this cable stuff has been going on, I have moved back on to my desk a book from my bookshelf called *Blind Man's Bluff*, which is the story of Cold War underwater espionage, including how this was all done during the Cold War by everybody involved. There is a remarkable degree of similarity if you start flicking through some of the examples.

On your point about further recommendations, this is again quite a trite point to make in the context of defence spending when there are

capability choices to be made across the board, but if you want to have something that can give you a lot of sustained presence up in the High North and everything else, an obvious platform to do that with is a submarine. The UK's submarine numbers are fairly limited; seven is the stated force level.

It should be worth noting that Australia—a different part of the world, admittedly—has jumped its submarine numbers from six to 12, at least under its old programme. Given its new nuclear-powered submarine, the numbers have not been quite refined yet, but its plan was to double its numbers. There is discussion in Canada about a significant increase in its numbers and—it is a major navy that will be patrolling in the Arctic.

You can talk about networks of gliders and unmanned underwater vehicles that can get down and maintain constant eyes and ears below the water, but to have something that can go down there and then do something about it, a submarine is a candidate. We have only seven and they are all very busy.

Dr Sidharth Kaushal: I have not much to add, other than that Lee is absolutely right; the element of vulnerability, particularly of military cables, is something that the Russians probably share with us, and even on commercial cables. Taking Lee's point that they have a bit more transcontinental redundancy, they also rely on undersea cables, particularly along the polar route and through the Baltic Sea, for quite a lot of their transcontinental dataflows. I do not think we have invested in these, to the same degree at least, and the specialised assets for that particular function. But, certainly, the ability to tap and potentially damage infrastructure cuts both ways as far as deterrence goes.

On submarine numbers, I would agree completely with Lee in terms of them being the primary means of ensuring presence. There is probably another element to it which is, to the extent that our submarines are active in places such as the High North, the sorts of capabilities the Russians would use to tamper with infrastructure—because they are also dual surveillance assets, as I mentioned—would be tied down to more defensive tasks like monitoring our submarines. That is one way of effectively fixing a fairly limited amount of human and physical capital in tasks that we would prefer them to be doing relative to more offensive ones, but to do that one needs more submarines than we currently have.

The Chair: Any other points to raise? No. Thank you both very much indeed for your time and for coming today; it has been really interesting. I am not sure how much time we spent in the Arctic per se, but it is all obviously connected and has been very useful. As I said, we will send you a transcript and you can make sure that it has been taken down correctly. That is where we will finish.