HOUSE OF COMMONS

Energy Security and Net Zero Committee

Oral evidence: Energy resilience, HC 171

Wednesday 3 June 2026

Ordered by the House of Commons to be published on 3 June 2026.

Watch the meeting

Members present: Bill Esterson (Chair); Ms Polly Billington; Sir Christopher Chope; Lizzi Collinge; Torcuil Crichton; Graeme Downie; Bradley Thomas; Claire Young.

Questions 137 - 206

Witnesses

I: Chloe Oakshett, Maritime Lawyer, Addleshaw Goddard LLP and Director, Scottish Maritime Cluster; Elisabeth Braw, Senior Fellow, Atlantic Council; and Graham Skinner, Health, Safety & Security Policy Manager, Offshore Energies UK (OEUK).

II: Deborah Petterson, Director of Resilience and Energy Management, NESO; and Stuart Okin, Director for Cyber Regulation and Emerging Technologies, Ofgem.

Examination of witnesses

Witnesses: Chloe Oakshett, Elisabeth Braw and Graham Skinner.

Q137 **Chair:** Welcome to this morning's session of the Energy Security and Net Zero Select Committee inquiry into energy resilience. We welcome our first panel. Please introduce yourselves.

Elisabeth Braw: My name is Elisabeth Braw. I am a Senior Fellow at the Atlantic Council and also the author of the upcoming book "Undersea War", which is about exactly what we will be talking about here, which is undersea cables and pipelines.

Chloe Oakshett: Good morning. My name is Chloe Oakshett. I am a maritime lawyer. I practise in the shipping team at Addleshaw Goddard, which is an international law firm. I am also the Director of the Scottish Maritime Cluster, which is a Scottish trade body for maritime businesses. My expertise lies at the intersection of energy infrastructure and the legal framework governing the marine environment. That includes the deployment, maintenance and protection of assets such as wind farms and subsea cables. Some of the work that I do relates to classified matters but I am happy to follow up with the Committee afterwards in any way if that information cannot be shared here today.

Graham Skinner: Good morning. I am Graham Skinner. I am the Health, Safety and Security Policy Manager at Offshore Energies UK, which is a trade association that represents 450-plus members across the energy sector, including oil and gas, offshore wind, CCS and hydrogen. Our members are the operators of infrastructure and the supply chain that supports that.

Q138 **Chair:** Thank you all very much indeed for joining us and you are welcome. We look forward to your evidence. The National Energy System Operator told the Joint Committee on the National Security Strategy that the conflict in Ukraine has demonstrated that targeting energy infrastructure is part of military doctrine. I will start with Elisabeth. How resilient is the UK's energy infrastructure to current risks of both physical and cyber-attacks?

Elisabeth Braw: The first thing to bear in mind or to look at is how Russia has decided to use means, other than military ones, to weaken other countries. In Ukraine they are seeing it in conjunction with military means but when it comes to countries like the UK, Russia uses exclusively non-military means so far. Those means can be easy to detect, such as cases of sabotage, and they can also be much harder to detect, and they can be almost impossible to attribute to Russia. That is a longwinded way of saying that the UK energy infrastructure is targeted or is accessed in different ways by adversarial activity or by suspicious activity and we may or may not be able to attribute it to Russia but we are seeing an increase in such activity.

So far the UK has held up well, and it is important to remember that no UK undersea cables have been subjected to or have been cut in mysterious circumstances where Russia seems to have been the perpetrator so far. From my perspective, the most important thing to bear in mind is that the Russian leadership, and potentially the leadership of other countries, feel at liberty to target energy infrastructure in ways that were not the case five, 10, 20 years ago. Once you have given yourself the liberty of targeting other countries' infrastructure, you can proceed as you wish and the targeted country just has to strengthen its defences. If they call Russia out, it is not going to be embarrassed.

Q139 **Chair:** We have seen Russian submarines circling North sea pipelines as well as cyber threats. I take it that these are the sort of examples you are thinking of.

Elisabeth Braw: Exactly. In the recent example you are referring to, when Russian submarines loitered above UK undersea infrastructure for an extended period of time, Defence Secretary John Healey called it out, rightly so, but I think it caused no embarrassment in Russia. In fact, the activity has continued, so it clearly didn't cause any embarrassment. Once you have put yourself in the position that the Kremlin has done of not being embarrassed by being found out, you have options available to you that respectable countries would not have.

Q140 **Chair:** Does our mix of energy resources help make us more resilient, which again is something that NESO suggests?

Elisabeth Braw: Yes. Since we are in the Energy Security and Net Zero Committee, I think it is important to remember that the variety of energy sources is a source of strength. Individual energy sources and installations may be targeted but the more variety we have or the more diverse the supply is, the better chances we have of getting through whatever it is that Russia or others may think up. Again, it is to the UK's credit that no cables or pipelines have been successfully damaged by Russia or any other hostile state so far. If it were to happen, the breadth of the energy production in the UK is an advantage.

Q141 **Chair:** Thank you. Chloe, what is your take on what we have discussed so far?

Chloe Oakshett: On energy resilience, I will speak to offshore and the maritime aspects only. It is really important to say to the Committee from a legal point of view that we are quite restricted in what we can do to protect our energy infrastructure outside of the 12-mile limit. The Committee will be aware that our territorial waters run to 12 miles, and of course the UK has important assets outside of that. We do have legal rights in our EEZ but really we are talking about very valuable assets that are out at sea in uncertain waters.

The rule of law on the high seas is UNCLOS, the United Nations Convention on the Law of the Sea, and the rule within the 12-mile limit is our own jurisdictional law. What we are able to do further afield where

many of our very valuable assets are is quite different to the control that we have within the 12-mile limit. That means that we are looking at very expensive equipment far out in an uncertain environment that we have very limited legal controls over, and of course that has an impact.

Under UNCLOS and article 60, you can have 500 m around an installation where you can restrict freedom of navigation, but that is unusual. All states have an entitlement to freedom of navigation on the high seas, meaning that every vessel can go everywhere, with certain restrictions but these are minimal. Energy assets are very valuable assets. It is only in some circumstances that we can put this 500 m cordon, and of course you can't fence it, so we are in very different territory to on-land assets. You have the 500 m but how do you enforce that around your valuable asset? You have very limited resources to enforce it. It is probably a useful deterrent for legitimate actors at sea.

Q142 **Chair:** I am sorry to interrupt. What steps should the Government take to improve protection?

Chloe Oakshett: The process for amending the international law of the sea is extremely complex and requires international co-operation. It is not realistic to imagine that we can respond as we would like to on that.

Q143 **Chair:** There is not very much from a legal point of view?

Chloe Oakshett: No, we are restricted but there are things that we could do to improve our resilience with our responsiveness to this. If we accept that we are in a very uncertain environment and we accept that there are limitations to how we can operate within that, a way of improving things might be to look at our own domestic law and how we respond to that. We have good means of responding in a crisis that are in place. We have the Civil Contingencies Act and powers of requisition, which are a Crown prerogative. We can look at how we use these and we can certainly look at what is available to us in the UK to deploy quickly to defend our assets at sea or to respond where they are impacted, where there is a rupture or disruption.

Q144 **Chair:** Thank you. Graham, what is your take on how we can improve the protection of our assets, especially those out at sea?

Graham Skinner: For the last 60 years we have had an offshore industry that has been incredibly resilient and it has been fundamental to UK energy security, as it is still today. We will continue to require oil and gas to 2050 and if we are going to use it, we should definitely produce it. Our remoteness is part of the reason we have that resilience but our remoteness from Westminster and from the decision making sometimes leaves us out of some of the tactical decision making. We already deal with safety risks offshore, such as drifting vessels towards installations. We have emergency response vessels on site and we manage the 500 m zone very effectively. The recent Granite Resolve exercise that we conducted in collaboration with the Department demonstrated that those

safety practices over the 60 years have made us very resilient to the threats that we face today, whether safety risk or security threat.

However, the exercise also demonstrated that we are somehow unsighted on how those threats might develop in the near future and that is an interesting area that we are very keen to work with Government to explore: what might those threats escalate to and how might we respond to that? Once we are in a war environment that is something entirely different, but we probably have some period of time in this sub-threshold threat environment with the escalation of existing challenges that we are seeing.

Q145 **Chair:** Is there anything you can say to us in public at this stage about what you would like to see or what you think is achievable?

Graham Skinner: Absolutely. The first thing that we need to achieve is taking the plurality out of the debate about energy altogether and realising that we need all energy sources to ensure that we have a resilient economy going forward. We need to understand that the foundation of safe and secure businesses is commercial stability, so we need to make sure that we have a regulatory regime and a fiscal regime that supports companies so that they can invest in security measures as they determine. We need to increase our collaboration across all sectors. There is some great work being done by NESO, who you are speaking to after us, but we need to get to the point where we have NPSA providing subsector pictures and support and then we are well placed to respond.

Q146 **Sir Christopher Chope:** Graham, you and I were on the same panel at the *Spectator* security conference on Monday. One of the issues that came out of that seemed to be the lack of joined-up work between the Government and the security services and the operators in the North sea. We heard from Botan Osman, who was also on the panel. He is the CEO of Restrata and 65% of the North sea operations are his clients who he advises. It seemed from talking to him and what was said at the conference that we are in two separate silos. He is in the private sector advising private sector companies that are paying for his services, but he is unable to get access and individual clients of his are unable to get access to the same information that must be available to the security services. What do you think can be done to have more joined-up working on these issues?

Graham Skinner: We have a governance challenge in this space. While I have to recognise the excellent work of the Department, and particularly the state threats team, they are at times limited by resource, which can be a bit of a bottleneck. If we look at the ways that we could improve governance in this space, designating offshore energy installations as critical national infrastructure would be the easiest way to access existing UK governance for critical energy facilities.

We could also look to other neighbours. The centre-left Government in Norway is very positively behind its traditional energy industry and very

supportive. They have a maritime security forum that brings the industry and the security services together directly without the arm's length link between Government, which increases situational awareness right across the sector from fishermen right the way through to energy companies. The fishermen should not be underestimated in their importance. After all, they played a vital role in Ireland when the Russians were due to conduct war games in their territorial waters. I think we need to look at the maritime space as a whole and not break it down into individual silos.

Elisabeth Braw: I want to mention the example of Taiwan, which has had several incidents of suspicious cable damage. The first few times, or I should say the first many times, the cables were damaged and then it was documented by the coastguard and inevitably the ships that seemed to have caused the cuts had long left. Then Taiwan introduced new legislation that compels cable operators to immediately notify the Government in case of any suspicious variation in what their cables are transmitting. A few months ago, when the Taiwanese coastguard was inspecting a vessel that seemed to be behaving suspiciously, they wanted it to leave Taiwanese waters and while the coastguard was doing that, it received a notification from Chunghwa, which is the Taiwanese telecoms provider, saying a cable had been cut. The coastguard was able to intervene essentially at the crime scene because Chunghwa had notified the Government instantaneously, as instructed.

I think that sort of solution would be an option for the UK as well, including in the exclusive economic zone, where you can't do very much as a coastal state but if the Government can be there or intervene immediately when a fault happens, they can try to convince the suspicious vessel to move into territorial waters and then you try to question the crew, which is better than not being able to do very much at all.

Q147 **Sir Christopher Chope:** Do you think this information sharing should be going both ways? It seems as though the Government and the security services often know more than some of the private operators and there is not enough information sharing.

Elisabeth Braw: Yes, a hotline should go both ways, and it should be a hotline with a designated recipient on both sides, but it is the case that the Government, with their intelligence services, know more than many operators do. I think that the realisation has also been slow among many private sector operators in different sectors that it is a changed world and that anybody can become the victim of geopolitically laid activity. It is not as if your company has to be controversial from the Russian perspective. It is just if your company happens to be a convenient target, you may become a target. It would be extremely helpful if there were to be an arrangement in which the Government were able to share information with the private sector and vice versa. I know, because I was involved in it, that a few years ago the Government wanted to set up such an

exchange, but it didn't go forward. In the six years since then, the need for it has only increased.

Chloe Oakshett: Can I come in on the data point? One of the things about collecting data is that obviously it increases the value of whoever is collecting the data as a target. Quite often in these discussions there is a lot of talk about information sharing, but the risk is not even because the small operators or people who are going about their commercial business do not have the same risk appetite and they are not in the same set-up as, say, those in the defence industry or government agencies. It is always worth considering the chilling factor of expecting people to hold data that increases their vulnerability. For example, with innovation in green technology or in areas where we might want to encourage nimble, small players, to expect them to collect data that might make them the target of a malicious nation state is quite a high ask.

Quite often I hear the scenarios, "We're going to have a hotline here and data reporting there", and it sometimes does not reflect the reality at sea. If you are a fisherman, you have a crew of 10, 13 people and you see something nefarious at sea, you may not be in a situation where your first thought is anything other than, "We need to leave this situation". I think it is really important to say that because the reporting angle is, of course, important but you can't ask people to make themselves vulnerable disproportionate to their own commercial business. Some of the output of discussion can assume that everybody is pulling in the same direction with the same rate of backing and that is not the case. Asking SMEs that are fishing businesses or small innovative technology businesses to defend themselves against some of these threats is a really high ask.

Q148 **Chair:** Thank you. We will move on. I have colleagues queuing up and they will get the chance to follow up on some of the points we have opened up very well in the first set of questions. A question from me before I move to Graeme Downie is: how well understood is the seriousness of threat, the level of resilience required for our energy systems across Government? Graham, as you nodded, you can answer that.

Graham Skinner: There is always a challenge about how much of the intelligence can be passed from the intelligence communities to the private sector. The arrangements that are in place with the NPSA are a good start. I think they are useful. Designation of critical national infrastructure would unlock those opportunities, but we will always struggle as an industry to absolutely understand what the intent might be of these state actors in this space. We will also struggle with the risk velocity: how quickly might these threats face us? Unless we are working closely with Government to do the risk assessments to determine what the levels of resilience are to be implemented, we are not going to—

Q149 **Chair:** On joint working between industry and Government, Chloe, how well do you think government across different Departments understand

what is needed for resilience in these systems?

Chloe Oakshett: Speaking from a maritime point of view, I understand that a lot more is happening on maritime incidents. It has already been mentioned that we need to move out of silos and look at this as part of maritime resilience. Quite a lot of what is needed here is talking about what vessels will service any disruption and who are the people involved who will service this.

One of the things I would like to bring to the Committee is the length of time that it takes to get somebody a security code to do particular types of work, and it can hold up projects. There are lots of skilled workers who might be available to do a job. A job might become sensitive that would not normally be sensitive and the person who is ready to do it is not necessarily security cleared. This goes through various maritime chains, and we would want to look quite deeply into who are the people at ports, who are the people who are able to work the equipment, who are the vessel crews who are cleared to do work that suddenly becomes vulnerable or classified. That might be a chokepoint in our energy resilience, but it also is a chokepoint in our general maritime resilience. That is something that we could address on both fronts.

Chair: Thank you. Practical recommendations are always very welcome at this Committee.

Elisabeth Braw: I have a practical recommendation, which is that there just are not enough repair crews and specifically there are not enough crew members skilled in the repair of undersea cables. We can talk about repair vessels and preparedness, but at the end of the day these are the men—and it is typically men, but it could be women as well—who will make that happen and it takes a very long time to train them. I think there is an opportunity here for the UK to essentially set up a reserve force of people who are trained in cable repairs, not to the highest level because that takes a long time, but who could assist the master. The Government could oversee that and it would function as a reserve in the way that military reserves work.

Q150 **Chair:** To the question about different Government Departments, are there Government Departments that are not in a good place in understanding what is needed?

Elisabeth Braw: They understand what is needed but the fundamental issue is that the UK is very good at detection, it has understood the threats, but when it comes to adversarial activity, if it is outside territorial waters, you can monitor, detect and identify, but what are you going to do if you see adversarial activity happening?

Chair: We understand the risks but it is whether we are equipped to deal with them.

Elisabeth Braw: The fundamental issue is: will the UK risk military escalation with another country because it has spotted, let's say, Russian

vessels in the act of interfering with cables in the exclusive economic zone?

Graham Skinner: I think we underestimate the value in deterrence, which should be our first port of call. If we harden our protection, physical or cyber-security protection, that will be very important and make us a much tougher target, which will deter, but also I would like to see the response in the way that we saw news articles coming out to recognise that we knew the Russians were there. If we see incidents offshore, I would like to see a visible military response. It may be that the horse has bolted, but we need to be able to demonstrate our capability in response and make sure that our adversaries, no matter which state they are, are aware that we will act. A good example might be the Russian shadow fleet, where the French have been boarding vessels and we have made a statement that we intend to do it at some point. I think we could be a little bit bolder in our deterrence.

Chair: That is really helpful. I will go to Graeme now. Everybody else will have their chances. Please indicate if you are planning to ask questions.

Q151 **Graeme Downie:** Chloe, if I can go back to where we started at the very beginning about the legal basis for action, I was in Romania recently and it is building Neptun Deep in the Black sea gas installation. I was speaking to their Minister for Foreign Affairs and Defence, who was talking about how they have created a new legal framework that would essentially allow them to take military action outside of the 12-mile zone. Are you aware of that and in particular—and I will come to Graham on this as well—around drone activity? That is their biggest threat in the Black sea. Are you aware of that work, and what legislation or what work could we do in the UK to extend or make clearer our military ability to act? How would that serve as a deterrent as well? The Romanians see it very much as part of deterrence—"We are passing this to show we can".

Chloe Oakshett: There are some points about this, which is the legal framework can work really well for either innocents or those people who are not coming with malicious intent, because it tends to be reactive. If we are in a situation where there are fishermen who may be skirting a bit around things or people who don't have their technology up to date and they are a bit like, "Where is it? Am I 510 m away or am I 480? I don't know", that is definitely where an enhanced legal framework can improve the situation. We can do that in EEZ.

I think where we probably need to accept the limitations of civil commercial law, which is what I practise in. It is very unlikely that the fine level or the financial risk level will ever deter somebody from flying a drone for nefarious purposes that relate to security and defence. It might identify people as taking a higher risk, and I think that would be relevant. If we say they are well covered by civil and commercial law—so now, "What is this person doing in this area?"—that might well be highly useful for security and detection, but as deterrence the civil commercial legal framework is very limited in what it can do.

Any maritime claim is subject to limitation. I don't want to go too far into that, but essentially if you have a small boat, you have a small backing of insurance, and going after little boats for big trouble is probably not worth it. Increasing resilience by going after the insurers is probably not that helpful. Does that answer your question? I am afraid I can't answer on drones because that is slightly outside what I do.

Q152 **Graeme Downie:** Okay, no problem. Graham, can I pick that up with you? What is your understanding of what action can be taken if there is a drone near an offshore installation? I have tried to get an answer to this from DESNZ and the Ministry of Defence. No one will give me an answer as to whether or not we have a legal right to attack a drone over an offshore oil rig.

Graham Skinner: First, we don't have any intention of attacking drones over oil rigs.

Graeme Downie: No, I am more getting at what your expectation would be.

Graham Skinner: There have been a very limited number of drone sightings around offshore infrastructure. We don't know whether that is because sometimes they are very difficult to spot—grey sea, grey sky; a grey drone 500 m away might be very difficult to spot. When we have seen them, they have been deliberately conspicuous and they have kept a safe distance. We have a good reporting framework that we have developed alongside DESNZ, which has its own drone reporting guidance. We are in a position where we are gathering data at the moment, and I think that is a reasonable place to be.

However, it comes back to what happens next. What would the reasonable escalation scenarios be? At our Granite Resolve exercise we included the possibility that a drone landed on a deck and you would not know what its purpose or intent was. In those scenarios, it begins to get tricky quite quickly and certainly we are interested to explore what options might be available. It is very clear that kinetic anti-drone technology will be for the police and the military. It is not going to be a private option, so I think that is something that we just need to be aware of.

Are drones the biggest threat for us at the moment? Perhaps because they are exciting, they are unusual, they are flying in a war zone, lots of people like to talk about them, but we need to make sure that our foundational safety is there, our physical security and tackling cyber-threat and cyber-security needs to be at the utmost. Those are the attack vectors where we are seeing hundreds of attacks across cyber-security daily. I think our approach at the moment is proportionate. As I said, we are interested to discuss further what we might do in an escalation scenario.

Q153 **Graeme Downie:** How long has the reporting mechanism to DESNZ that

you talked about been in place and how effective is it? Is that who you call in the event of a problem? Is it well understood by your members that they are the people to call?

Graham Skinner: Yes. We issued that earlier this year, at the beginning of March, so we have had that guidance quite recently, although all the reporting requirements existed prior to that. We simply pulled them together into a single document so that it was easy to access by the managers who run the offshore installations. We have shared that with colleagues in wind and later today I am meeting with the UK Chamber of Shipping to talk about what guidance can be provided right across the maritime sector.

The reporting is appropriate. It is into the right services, including JMSC, so they have the situational awareness of what is going on, although we don't expect to get feedback on everything that happens because ultimately some of that will be classified. There are mechanisms where we can get some general information, which I think is important that we have a look at. Getting feedback that reporting is recognised and acted upon is important for further reporting to create a culture of vigilance. One point comes back to what the response looks like, and could we see a little bit more of it, because that will reassure the thousands of workers who work offshore around the UK who are perhaps most exposed to these sorts of risks.

Q154 **Graeme Downie:** To pick up on something you mentioned earlier about Granite Resolve, there was a debate yesterday in Westminster Hall on the idea of preparedness. What are the lessons out of Granite Resolve on what preparedness looks like for you? Safety procedures, because of the industry, have been practised over decades, but how do you transfer some of that safety work that you have done into preparedness for escalating threat?

Graham Skinner: We are very confident in our preparedness now, as you say, based on our safety culture. However, preparedness for the future requires us to first understand what the benchmark for resilience is that is expected by Government. For example, do we have certain performance standards and expectations for uptime and speed to prepare, and what might we need to do, whether it is a national resource for cable repair or piping repair? We are interested in having these conversations and ultimately we will end up talking about who runs the risk.

We know from Granite Resolve that our safety practice shows us if a threat is unknown or escalating, we would shut down all platforms and make them safe for the people who are on board. That obviously has a financial implication for the companies that they are happy to address as part of their safety practice, but the question might be: what if that happened to 20 gas installations in the middle of winter, and what would be the implications for the UK at that point? Those are the conversations that we probably need to be having now.

Q155 **Graeme Downie:** Very briefly, Elisabeth, if I can bring you back to what you were talking about on Taiwan, I have had some conversations about subsea cables in Taiwan and a concern that some of the lessons in Taiwan could not be shared with the UK directly for political reasons, certainly mil to mil. Are there international forums where Taiwan is currently not involved where it would be helpful for it to be involved so that those lessons can be shared for subsea and other security protections?

Elisabeth Braw: That is an excellent question. As you know, Taiwan is excluded from all UN agencies, which is a massive disadvantage. It is not allowed to join as a full member. If one were to approach it from the industry side, Taiwan is just like any other jurisdiction. For example, Chunghwa could share its practices.

I wanted to highlight one other country, which is Norway. It is extremely good at practising for drone incidents around their offshore installations. It has many and it has successfully looked after them for decades while being exposed to significant Russian activity, including activity linked to Russian fishing vessels that have a perfectly legitimate right to be in Norwegian waters as in the treaty that governs all of that. If the Committee wanted to make a study visit to Norway, I think that could be very instructive because it has worked hard on the issues involving drones and other adversarial activity or suspicious activity in their offshore installations.

Q156 **Claire Young:** We have already had a fairly lengthy discussion about the vulnerability of UK's subsea cables and interconnectors. I want to focus on a couple of things. The European Subsea Cables Association gave evidence to the Joint Committee on the National Security Strategy and alongside some fairly positive comments, they said, "However, gaps remain, particularly in power cable repair processes, which require further policy or other support". Elisabeth, you have already talked about the workforce issues, and Graham mentioned it as well, but those comments suggest that there are other policy-related matters that also need addressing. Could you comment on that?

Elisabeth Braw: Yes; in fact, I remember the comment because I was part of that session too. The issue with interconnector repairs is that there is not the sort of ambulance service in place for interconnectors that there is for undersea cables. "Ambulance service" is my term; I just think it works. For data cables there is essentially a subscription arrangement where you pay for the repair service and you get to avail yourself of it when your cable needs assistance, but the same thing is not true for interconnectors and they take much longer to repair and are much more expensive to repair. The question is how can such a service be established because if it is going to be the case that interconnectors will need more repairs for whatever reason, the industry has not found a way of establishing an ambulance service so far. I think that the Government could perhaps play a convening role or the role of generating a framework under which it could be done.

Incidentally, that would also help to establish better insurance protection for interconnectors. At the moment, it is very difficult to insure interconnectors, which has to do with the fact that they are incredibly expensive to repair, so it is not particularly attractive to insure them. If you think of that from the perspective of operators, it must be absolutely frightening to be an interconnector operator when you know that it will be difficult to get insurance, and at the same time you face the real risk of something happening to your interconnector. Then you would think several times about whether it is commercially viable to operate that interconnector, but with an ambulance service in place, that would take some of the sting out of that dilemma or that conundrum. I think that is where the Government could play a convening function.

Chloe Oakshett: May I add to that? I don't know if it would help to say that most of the operators do have contracts in place for these repairs. They will have a framework in place with a repair operator and they will call down services as they need them. That will have been negotiated and all the commercials will have been negotiated at the same time. With an ambulance service or without, it is likely to be the same people running those services. Even if we put an ambulance service in place as an overarching one, it is likely to be the same people, so the worry becomes: what if there is a volume situation or what if there are two situations? It is the same operators, because we are constrained by the number of operators and that could take some time to resolve. It may be that there is incident A and incident B and the call down would be for the same repair company or the same crew, the same spread, perhaps the same vessels, and they would be needed in two places.

It is possible that an ambulance service would be able to sort priority for the Government rather than being subject to commercial whims, but having said that, it would be quite difficult to negotiate that ambulance service because all of this is commercial information, it is sensitive and there are competing operators. We would not want to create a situation that significantly impacted the commercial operators that are acting there.

Elisabeth Braw: If I can add, with the ambulance service it is first come, first served, unless you have a very significant reason why your cable should go ahead of another company's cable, whereas if you don't have an ambulance service, it really is a free-for-all and you have to fight to find a repair vessel, which is exactly what happened to Fingrid in Finland. When EstLink 2 was struck on Christmas day, they had to call around to find a repair vessel. It took them a long time and they could not find a repair vessel. In the end, they had to improvise and set up something themselves. It took a long time and it was expensive. An ambulance service would not solve every issue, but it would at least create some sort of process and stability to make that a little bit easier for the operators.

Q157 **Claire Young:** Chloe, would you say that part of the further policy would

need to be about some kind of prioritisation?

Chloe Oakshett: In a situation of multiple outages, yes, that might be something that could be useful. Again, it is the same operators, and if you are in that situation, under the Civil Contingencies Act, you could instruct a UK-based operator as to where to go when. Perhaps the most useful thing as part of this would be to have a good audit of who is available, what vessels are available and what the spread is, so that we know what would be deployable in that situation, regardless of the contractual framework. Even if the contractual framework is with the Government, or perhaps they are intergovernmental agreements, they are still the same operators, and if they are working on something in one place, they are not available to work on it in another.

Chair: We need to move on.

Q158 **Lizzi Collinge:** We have already talked about threat reporting pathways. I want to dig into that a little bit more. Graham, you said before that you have pulled together into one document all the different reporting pathways. Are you confident that the energy industry is fully aware of those threat reporting pathways and is able to use them properly?

Graham Skinner: Yes, I am very confident. It has been well communicated with our members, who will adopt it into their emergency response planning. They will make sure that their teams are well briefed on that. One of the complications around reporting is how many different Government Departments and stakeholders are all interested in finding out what is going on. Certainly, that is a bit of a challenge. It is not just the initial report, but then there is quite a bit of follow-up required. It is an administrative task.

Q159 **Lizzi Collinge:** I am very aware, Chair, that we are focusing on the maritime today for understandable reasons. I think it might be worth the Committee's time to try to get evidence on this from the wider energy industry. Chloe, do you have any comments on that?

Chloe Oakshett: I can provide you with some anecdotes from small to medium enterprises. There are lots of people saying, "Come and tell us". I have been to security conferences where NATO will say, "We are setting up a hotline", and somebody else will say, "We are setting up a hotline", and the fishing industry will be setting up a hotline. There is an enormous number of hotlines, but it is not necessarily proportionate to the number of people who want to call them. There can be a bit of a worry about calling them in the first place. That is what I will add to that.

Another thing about reporting comes back to the data point. Addleshaw Goddard was working with a subsea cable owner, and as part of the technical qualities of the cable, it records sonar properties that tell it about damage and repair requirements of the cable. As it happened, recording that sonar data could also tell it about submarine activity in the area above the cable. This was not information that the cable operator particularly wanted to record; they just happened to record it because it

was part of the repair process. Then there was a negotiation about how they were going to hold this data, and eventually it was concluded that the data was to be held for something like 24, 36 hours after recording it. It was an ongoing process. That is a high point of sensitivity, that just reporting things can make things tricky for the operator.

Q160 **Lizzi Collinge:** Thank you for that. The Government have said that they are going to develop a reporting portal. I think it was specifically for drones but I would have to check that. Do you think that is just adding another layer, or do you think that is a helpful collation of the reporting structures?

Graham Skinner: A portal would be helpful. I think that intention has been around for some time, but the reality is a little bit more complicated because reporting into a portal is just half the battle. What we also need to know is who is receiving the reporting, how often it is monitored and what happens after that, so there is a complex element to that. We would welcome that for simplicity down the line and for a single point of contact.

Q161 **Lizzi Collinge:** Thank you. Obviously there are different levels of threat. There are safety issues that the industry is used to dealing with, as you said before. Things can move from a safety issue to a security issue and then potentially from a security issue to a defence issue. Who decides what level of threat or threshold an individual attack, attempt or surveillance meets? Is there guidance for that?

Graham Skinner: My understanding is that any report of suspicious activity or incidents that has a security dimension would go into the JMSC and they would then take the lead on all that decision making. From our operators' perspective, we would assume that any decisions on escalation into some sort of defence response would not be particularly quick because these are significant, weighty decisions that need to be made by Government. We would continue to use our emergency response capability in the short term to make sure that we are keeping people safe and minimising the environmental impact of anything.

Chloe Oakshett: On cable damage, anything at sea is extremely difficult to collect evidence about, as I am sure the Committee knows. It is possible to work out who was where and what kind of damage you are dealing with. What is not possible to work out is intent. I suggest that the intent angle will have to come from outside the commercial maritime information space. It will not be something we have held unless we have been warned in advance that this vessel is in the area or we think something could happen in this particular space. Otherwise, it is completely outside the commercial space and most damage is accidental and non-nefarious.

Q162 **Lizzi Collinge:** The next question is for Elisabeth and Chloe. I want to think about co-ordination if there were an event that needed a response from the Government or from military. We have other energy

infrastructure that has long been seen as a security threat. Nuclear is the key example there, where there is a well-rehearsed response ready that is practised. Do you think the same is true for maritime installations? Do you think that if something happened, the coastguard, the Navy and energy operators would be ready to spring into action? I will come to Elisabeth first.

Elisabeth Braw: They would. If we look at other countries, for example around the Baltic sea, which is where the most activity has taken place so far, you have the Baltic Sentry, which is a NATO initiative. It essentially has the task of patrolling undersea installations. It is not 100% comprehensive because there are more undersea installations than there are vessels that are available to Baltic Sentry, but it is something that was not in place a few years ago.

In the UK, the question that always becomes the crucial point is who should respond. In Estonia, Finland, Sweden, Poland and Germany, it is the coastguard response, and the coastguard is responsible for constabulary matters along the coast. In the UK, the coastguard is a little bit different, with a focus on search and rescue, and the responsibility of constabulary duties has essentially been left to the Navy. For boarding shadow vessels, the announcement was that special forces would do it, but that is very different from the coastguard intervening when there is what looks like a suspicious criminal activity. I am not saying that the Committee should ask the Government to create a proper coastguard, but there is a gap there in the UK. It is a criminal matter, destruction or tampering with infrastructure, and sometimes it can be geopolitically motivated.

Q163 **Ms Polly Billington:** I am going to ask a little bit about cyber-security. Once you are moving to a more diffuse and renewable energy system, you have different kinds of risks. Do you think the energy sector cyber-security strategy adequately mitigates these risks, as you understand them?

Graham Skinner: We welcome the publication of the strategy last week. It is very helpful that there are some clear timescales and commitments for action. It is a matter of time to see if that drives significant change. I think we are as confident as you can be in the cyber-security space that our energy installations are following the correct regulations and are preparing to adapt to the new forthcoming regulations, and that we have strong levels of cyber-protection. I think that continues to be one of our biggest risks going forward.

Q164 **Ms Polly Billington:** The way the energy system works actually creates new risks, doesn't it?

Graham Skinner: Absolutely. In the OT cyber-security space—I think our colleagues at Ofgem will speak better to that after this session—a very different response is required across industry. Equally, a lot of our emergency response capability sits within the IT space, so we need to

manage both of those quite carefully. We are beginning to take a total security view. Equally, as your system security increases, your vulnerability to insider threat, for example, then increases, so you shift the risk. Therefore, physical security is important. We need to keep moving everything forward and managing the continuous improvement cycle.

Q165 **Ms Polly Billington:** I am interested in the contrast between what Elisabeth said about the mix of energy resources increasing resilience and how changing the structure of our energy system to become more diffuse has significant resilience implications, and the new cyber-security regulatory requirements we therefore need to establish as a result.

Graham Skinner: I accept that there are benefits and risks from having a distributed energy system, such as we have. Ultimately, I think the more variety there is in the energy system, the more unlikely it is that we will have a single cyber-attack that could fundamentally take out our infrastructure.

Q166 **Ms Polly Billington:** Talking about one single one, what lessons do you think the UK could learn from the recent cyber-attack on Poland's energy grid?

Graham Skinner: I think everyone working in the cyber-security space is working very hard to learn as much as possible from that.

Q167 **Ms Polly Billington:** What do you think are the top takes?

Graham Skinner: The top takes are: do the basics. The basics are very important. That means you have to follow all good practice to make sure you protect your systems. You have to update them regularly. You have to close the open doors that are within the system. You have to look very carefully at the cyber-security practice of the supply chain as well, to make sure that that is not introducing any new entry points.

Q168 **Ms Polly Billington:** Can you explain more about the supply chain risks?

Graham Skinner: Supply chain risk is probably better spoken to by my Ofgem colleagues later on. I hope they do not mind me passing that one over.

Q169 **Ms Polly Billington:** No, that is fine. Is there evidence that offshore wind turbines are particularly at risk from cyber-attack? What should be done to increase their cyber-resilience?

Graham Skinner: I do not believe that there is any specific difference between where they are located as to the cyber-risk that they would face.

Q170 **Ms Polly Billington:** Notwithstanding all the things that we have been talking about with the physical risks of it being offshore, does that increase or affect the cyber-resilience?

Graham Skinner: I do not believe so.

Ms Polly Billington: That is helpful. Thank you.

Q171 **Torcuil Crichton:** Thank you all for coming in. Fascinating stuff. Time is short, so I will keep my questions short. Somebody has to pay for all this and Graham raised the question of who owns the risk and Elisabeth talked about the high cost of insuring all this. Chloe, perhaps it is best to ask you: where is the boundary between the private sector paying the insurance and the state stepping in and paying for the security?

Chloe Oakshett: Yes, I think we come back here to the limitation of the liability of vessels. If you have small tonnage, you are restricted in the amount that you will be paying out. If we are talking about a small fishing vessel doing large damage, it is almost meaningless. With the current set-up, the way that marine insurance works, if a significant-sized vessel does significant damage, we might be in the ballpark of, "Yes, this is something worth pursuing". Realistically, when we are talking about an anchor drag from a fishing vessel, the harm caused is potentially disproportionate to the vessel size and the ability to recover. Civil recovery is perhaps not the best route here. I think that getting the insurance companies to pay is low.

Q172 **Torcuil Crichton:** Elisabeth, you talked about an ambulance service and recovery. Should there be a better regulatory framework to make sure that we can step in to recover connections and to recover infrastructure when incidents like this happen?

Elisabeth Braw: I am not sure that the Government need to step in quite as much, but there needs to be more communication around the fact that this is a crucial profession. Nobody who has not experienced the cable cuts has paid any attention to the profession of cable repair crews, yet they are indispensable when there is a fault to cables. The industry has trouble recruiting simply because not enough people know that it exists. If there were to be more public communication around the fact that this is one of the most crucial professions in the UK, we would at least have more people going into the profession. Then we could start talking about the Government perhaps owning a repair vessel or two, but it will be futile without experienced people serving on those vessels. I think a convening function would be useful. I do not think a regulatory function will be necessary.

Q173 **Torcuil Crichton:** I will come to the convening function, but should we see the spending in this sector as defence spending?

Elisabeth Braw: It would certainly fit within the 1.5% of GDP, and it was an ingenious move by Mark Rutte when he got the member states to agree on the 1.5%, because it is very loosely defined as infrastructure that relates to national security. It could fit within that 1.5%.

Q174 **Torcuil Crichton:** We are running out of time. Graham, I want to go back to drones, because we are all excited by drones, as you know. You said that there were a limited number of incidents in the North sea. There seem to be more in Norway. Can you put a number on the drone

incidents, and I think you have said this before, drone incidents versus cyber-security attacks? What is the proportionate risk there?

Graham Skinner: There have been fewer than a handful of drone incidents in the last couple of years in the UK. Although there have been more in Norway, there is still a very small number, whereas our critical infrastructure is subject to hundreds of cyber-attacks daily. There is a fundamental disproportion of cyber-threat to drone threat.

Q175 **Torcuil Crichton:** I have one quick last question, picking up on what Polly said about offshore wind infrastructure and its vulnerability to cyber-attack, but also this fear that there could be things built into these turbines that help to monitor our activity at sea. Have you seen evidence of that?

Graham Skinner: I cannot specifically comment on that. What I will say more generally is that decisions such as components within the supply chain, countries of origin, and so on is definitely something on which we would expect Government to define whose components we could use and incorporate.

Q176 **Torcuil Crichton:** Such as the Ming Yang decision?

Graham Skinner: That is correct, but the reasoning and the motivation behind that has been held on to by Government. I think that is probably appropriate. It would be very difficult for industry to reach those conclusions ourselves.

Torcuil Crichton: Thank you all.

Chair: Thank you very much indeed. That concludes our our first panel. Thank you all for your evidence. We will take a short recess while we change panels.

Examination of witnesses

Witnesses: Deborah Petterson and Stuart Okin.

Q177 **Chair:** Welcome back to the Energy Security and Net Zero Select Committee and this morning's session in our inquiry into energy resilience. Could our second panel introduce themselves, please?

Stuart Okin: My name is Stuart Okin. I am the Director for Cyber Regulation and Emerging Technologies, which include quantum and artificial intelligence, at Ofgem.

Deborah Petterson: I am Dr Deborah Petterson. I am the Director for Whole Energy System Resilience at NESO, the National Energy System Operator. You will be familiar with NESO's role in running the electricity system of today and planning the system of the future, but you might be less aware of our new duty to provide independent advice and guidance to Government on any risk that might impact any part of the energy system.

Q178 **Lizzi Collinge:** We heard evidence in the first panel about the threat to our energy infrastructure and we have seen stark examples, for example in Ukraine, of what can happen when an energy infrastructure is targeted. With that in mind, do you think we should be moving to more of an emergency mindset with Government and agencies around increasing energy resilience? Should we be acting with greater urgency than we already are? I will come to Deborah first.

Deborah Petterson: Thank you very much for your question. Obviously, geopolitics, and the increasing threat we see with geopolitics, is in the forefront of all our minds. I find that the energy industry is extremely well-exercised, partly because the eventual impact is an outage and, therefore, storms, cyber-attacks, all the things you have been discussing in your first section this morning, are issues that the industry is well versed in. We have regular exercising programmes. However, the Strategic Defence Review and the resilience action plan produced by Cabinet Office all have this focus on building home defence, and that conversation about, "Is there more to do?" What I can say at the moment is that the way NESO is designing the system, the cyber-security requirements and industry's approach to that absolutely meets the current risk appetite set out by Ministers and regulated by Ofgem.

Stuart Okin: I have been in this role for seven years, and we have a well-established cyber-resilience network for gas and electricity. That being said, we have seen over the last two or three years an acceleration that has been conducted by our operators of essential services, which essentially is critical national infrastructure. It is something that we live with every day, as Deb has just said. We have to lean in to constantly manage the risks and the changing and evolving risk landscape.

Q179 **Lizzi Collinge:** Do you get what you need to be able to meet that changing, emerging and increasing risk?

Stuart Okin: Are you talking about our resources?

Lizzi Collinge: Resources and responses from Government when those are needed with intelligence and information.

Stuart Okin: We have a very good working relationship with all the Departments. We understand our swim lanes and what we do, and we support each other in these areas. This is why you saw the strategy that was released last week, which was a quad strategy by ourselves, DESNZ, NESO and NCSE. We have working lines. Would it be useful for the Committee and for the public to hear about how the set-up is arranged?

Lizzi Collinge: Yes, briefly.

Stuart Okin: Very briefly then, essentially, under the Network and Information Systems Regulations 2018—that is the standard Act that we support—there are some very clear lines. Regulations 10(1) and 10(2) mean that there have to be appropriate and proportionate controls and measures in place to manage the risk; 10(3) looks at the state of the art;

and 10(4) is being responsive to the competent authorities. We are a joint competent authority with DESNZ. DESNZ does the designation. The OESs, the operators of essential services, should designate themselves or say that they are an OES, but the designation itself is conducted by DESNZ. That is then handed over to us to operate.

We do that in conjunction with NCSE and CCU, as part of GCHQ, which is the technical authority, and they have the cyber-assessment framework. DESNZ will set the risk appetite, the type of attackers that it is looking to prevent, their capability. It sets the risk appetite, and then we assure against that. We inspect—we have done 40 deep-level inspections, which have led to fines of £30 million over the last few years. We ask them to do self-assessments and we engage directly with the industry. Of course, they have to exercise an audit as well.

Q180 **Lizzi Collinge:** Thank you very much. I want to move on to threats that are not geopolitically related. When we think about ageing critical infrastructure—we have had the example of the North Hyde substation fire—what standards are being set for the maintenance and inspection of ageing infrastructure?

Stuart Okin: We are currently investigating. That is a current ongoing investigation with North Hyde. On the recommendations of NESO, we went and looked at National Grid specifically and looked to see whether there are any other areas where they might have assets under similar condition as well. We looked through that. We are looking to see what we can do with standards that can be utilised for the future. I cannot talk about the ongoing investigation.

Lizzi Collinge: That is fair enough.

Deborah Petterson: I will add that North Hyde, the substation that led to the eventual closure of Heathrow, was the first Secretary of State-instructed review for NESO to do. Although NESO sits outside regulation, we have this power to request information for any near miss or for any incident that happens. Referring to your first session too, I think it is a nice example of how in those initial stages you do not understand what has happened. It was exactly the playbook we expected for hostile state sabotage. In that moment, what you saw was NESO mobilised, DESNZ, National Grid, SSC, but also counter-terror and policing, the intelligence agents, all come together into this well-rehearsed—the London Fire Brigade particularly.

North Hyde is not critical national infrastructure—it is a substation in the west of London—but it led to an outage that included traffic lights, underground, rail, data centres, hospitals and GP surgeries. Fortunately, it was in the middle of the night, so that was all resolved very quickly. In our recommendations, we made a whole set about the cross-cutting nature of critical national infrastructure, and that is being picked up by DESNZ. They accepted every single one of our recommendations to look at the cross-cutting, underpinning nature of the energy system. Also,

interestingly in that report, those recommendations have been picked up by the aviation sector, the rail sector and the energy sector. I think having someone who is a step away from Government but without that regulatory lens, to build a more secure system, is already proving to have value.

Q181 **Lizzi Collinge:** That is very helpful, because you have gone immediately into something I wanted to ask about, the interdependency. As you said, North Hyde itself was not critical national infrastructure, but the impact it could have—and the impact any energy outage could have on things like transport and healthcare—is clearly very important and could lead to a risk to life. Are there any further comments you would like to make on how you map those dependencies and how you manage the second-order effects?

Deborah Petterson: Yes, you are right, energy underpins our way of life, and I have started to describe energy security as our national security. You cannot launch a defence of your country without energy. That understanding, as it becomes more interdependent, along with telecoms—there is an interesting interconnection there. There are various parts to this. First, DESNZ asked us to look at the methodology for defining critical national infrastructure. You can imagine that we used to have these big blocks of power stations, and now we have this logically interconnected network of digital, telco, energy all coming together to operate the system. We are doing that, and then we will apply that methodology.

But as you rightly stated, something classified as critical national infrastructure in energy—there are lots of things that are not critical national infrastructure that underpin other critical infrastructure and therefore the mapping of that system. I have to admit being a bit partial to this. When I was at the National Cyber Security Centre, the knowledge base was created by my team there and that has now been handed to the Cabinet Office, which obviously has a cross-cutting view of Government. I understand that its situation centre is picking that up to look at how these are interlinked.

On the resilience action plan, the Cabinet Office said that it will move very quickly to looking at how all the different sectors critical infrastructure map together, but we are looking at that at NESO too. If we have that map of the infrastructure, it allows us to support the questions about where we best protect to support our national resilience.

Q182 **Lizzi Collinge:** Thank you. I want to move on to a different threat but one that is extremely important, and that is more frequent extreme weather events. Do you think we have the correct strategy and operations in place to mitigate that threat to our energy system?

Stuart Okin: We have just set up a resilience hub within Ofgem. Inside the resilience hub we are looking at all the cross-cutting—cyber; weather; we are looking across all these different areas. I think that as we diversify

and as we have more or different types of energy systems in place, including the flexibility of localised, that will likely be able to give us more resilience. It does increase the attack surface from a cyber perspective, that is true, and there is also pressure on the supply chain, but on the other hand, if it is designed correctly, it will give us the diversity that we need for resilience.

Deborah Petterson: If I could build on that, NESO is there to provide independent assessment advice on any risk to the energy system, and that also includes climate resilience. In our first year we have brought in a professor from the Met Office, Professor Emily Wallace, to support NESO in understanding. Weather is our fuel, but it is also a risk and inherently variable. We take the security of supply of weather as seriously as we do gas and electricity, and making sure we can hone that data.

We model 30,000 weather patterns every single day to work out the parameters for what energy we require: when it is on a cold, grey day that we have sufficient gas and other sources of electricity; how we manage the system when there is excessive sunshine or wind. The more accurate data we have, the more economic and efficient the system can be. We are working with the Met Office, who are fantastic at using AI and their machine learning, but what they do, because at the moment we look at historic weather patterns 34 years back, and we use that to model these 30,000—

Lizzi Collinge: Is there a risk there because our weather is changing?

Deborah Petterson: Yes. The Met Office is bringing to us the forward projection of the weather we have yet to see but they have relative certainty in looking 10 and 20 years ahead for infrastructure. Emily has been pulling through that expertise into our strategic energy planning so we can look at regions and understand where there will be sea level rise.

The other area we are doing at NESO is creating international partnerships. Our colleagues in America and Australia are well versed at dealing with wildfire. We saw a 600% increase in wildfire in this country over the last two years. We do emergency preparedness exercises, so we are there for the whole sector. We report to Ofgem and Government every year on the season ahead and how the industry is prepared. We are exercising emergency preparedness for the summers of the future and for now.

Q183 **Lizzi Collinge:** Stuart, you touched on supply chain and things to that. Should the UK be prioritising the domestic manufacture of components, which could affect the cost of them, to reduce the risks of supply chain dependency and the dependency of our energy system on foreign supply chains?

Stuart Okin: First, that is a decision for Government, clearly. That is DESNZ's decision, and—

Lizzi Collinge: Do you have an opinion on it?

Stuart Okin: There are two parts to this. First, there is a risk and then there is a growth. On the risk side of things, we should always take a threat view that is based on intelligence—and that is intelligence not just about the country but also about the company, the individuals—and that threat intelligence should give you an idea or a view of what we should do in any particular component or system area. That is the first part of it.

Then there is a growth part, which is that if something is being developed from a domestic perspective, obviously we need to be very careful of the value for money and the cost, as I know this Committee is very focused on as well. There is the balancing between the cost of building something locally versus the risk.

Deborah Petterson: NESO is one of the areas—so where we provide independent and expert advice, often it is driven by the sector that has a particular interest in supply chain. Also, interestingly, in April we had our first international security roundtable where we brought the Five Eyes over, along with some of our European counterparts, to bring together our security concerns. One of those areas was supply chain and how you secure the supply chain.

Our view is that we should have a diverse supply chain. We would not want a monoculture of one type, but also I think from my previous experience in cyber-security that it is about always looking at your vulnerability. If it is what I would call a dumb piece of kit, a piece of metal, I would advise someone to have a diverse supply chain so you have options but the threat is less, whereas if it is something that is enriched with data: where do you want your data, who has access to it, who holds it, are you comfortable if it is in another country, what you would do out of hours, maybe that is a huge benefit? By asking those questions and then taking that judgment, we support industry in providing advice and guidance.

Q184 **Lizzi Collinge:** Finally, we had some interesting evidence in the last session about the risks of putting too many burdens on operators, especially smaller operators and smaller businesses, around their responsibilities for energy resilience. Do you think there needs to be a dissemination of responsibility for energy resilience to wider society and to operators and businesses, rather than it just being held in central Government? What are your thoughts on that?

Stuart Okin: We have a number of different Departments, as I pointed out at the beginning. DSIT is doing a huge amount of work in setting the new Cyber Security and Resilience Bill and the setting up of the security unit inside there. We have DESNZ, ourselves and NESO, so there are quite a few, and of course NCSC.

If I understand the question where you are aiming for, for the larger operators of central services that are critical national infrastructure, I

think the focus needs to be on them making sure they step up. We should hold them to account to make sure that they do that. The cyber-assessment framework that they utilise covers everything from risk governance right through. It is an outcome-based system, but it is very thorough.

We have added to that—we have 300 pages of added guidance to that—which includes some of the physical elements as well. All outcome-based, not prescriptive, it gives them the idea of what we are expecting to do but I would expect them to set up.

Smaller entities and licensees, the 1,400 licensees that are not the CNI, are a different area. We have gone to consultation recently saying for the CNI base should we change the thresholds, but for all of the others, the 1,400 licences, "This is a baseline standard. How do you feel about that?", which is basically around Cyber Essentials and Cyber Essentials Plus. We have asked the industry to come back on that. However, it should be pointed out to the Committee that that is really a baseline. They do not look at governance and risk. They look at five different areas.

Q185 **Ms Polly Billington:** I would like to ask a little bit about the energy sector cyber-security strategy, particularly the changing nature of our energy system. We are now changing the risk profile quite considerably because of the nature of the more complex and decentralised grid, much of which we have talked about. What I noted in what is said in the strategy is that, "The integration of legacy infrastructure with new technologies presents a complex challenge requiring careful management to ensure seamless and secure operations". How does the framework put forward in the strategy interact with the Cyber Security and Resilience Bill and Ofgem and DESNZ's consultation reshaping cyber regulation in downstream gas and electricity?

Stuart Okin: It covers a number of different areas but I will just pick one, for example, to give to the Committee. Supply chain is a key part of that. Inside the action plan that we have in the energy strategy, we will be looking at supply chain standards and supply chain guidance. In fact, we released yesterday some principles that we would like the supply chain to look at. How that relates to the Cyber Security and Resilience Bill is that the Bill at the moment is intended to have supply chain as a regulated entity.

Ms Polly Billington: Much like your answers to Lizzi.

Stuart Okin: Exactly. We started developing this over a year ago. We had sight of the Cyber Security and Resilience Bill, so we needed to make sure the strategy aligned with that. That is just one example.

Deborah Petterson: You are absolutely right. There is an increased attack surface, a much richer set of assets. However, one of the learnings from the conflict in Ukraine is to move to a far more distributed system to

give you a greater resilience and a more diverse supply of different energy resources, a greater basket to operate from.

Lizzi mentioned the Polish cyber-attacks. What we need to bear in mind is that the adversary was already targeting these. There is a question mark: what was their motivation? Was it to distract people from distributed energy resources because they have an interest in oil and gas sales or was it just to start testing and trying their capability in that space?

I think what is important are the smaller operators. There are things like Cyber Essentials, there is a free offer from the NCSC. We are very lucky to have an outward-facing intelligence agency there to support. I cannot believe I am going to quote Spider-Man but with great power comes great responsibility. If these industries wish to be part of our energy mix, the national security implications of the role they provide has to be taken seriously. NEOS has this whole-system view now and we are building new relationships with wind and batteries and solar, and bringing them into this community to better understand the threat.

Q186 **Ms Polly Billington:** That is helpful. It is interesting you mentioned Spider-Man, when you were talking about what happened at Hyde. I think of how this can sound extremely dull until suddenly you are in a "28 Days Later" scenario and so forth. We need to understand what the risks are when you have something that is more distributed and what that means. On your point about interconnecting very strongly with telecoms, we have two separate regulatory bodies for telecoms and energy and yet those two are increasingly interconnected in regulation. Do you see one of the roles of NESO is to co-ordinate those two aspects and is that in your mandate? Is that formally there or has that grown up as you have been established?

Deborah Petterson: Our duty is to provide the Government and industry with independent assessment advice on any risk of the energy system. Some people question that that sounds unbounded. For me, the energy system is dependent on digital and telco, therefore it is helpfully unbounded because it allows that if it can provide a risk that needs investigation, NESO has the reach to do that. For example, one of our learnings from the Iberian peninsula outage—of which there are many because of the lived experience of our partners, some of the best learning you will ever have—is in the restoration process, the fragility of the telecoms.

We are absolutely now moving to exercise with our partners and the focus of our emergency preparedness assessment, which we do in consultation with Ofgem and DESNZ about the areas of focus. We will be looking at operational telephony and how that works under crisis and stress.

Stuart Okin: That exercise is being conducted at the end of this month.

Q187 **Claire Young:** Sticking with the issue of the security strategy, what

specific metrics will determine whether it has been successful in increasing cyber-security resilience in the energy sector, particularly given increasing distribution and changing threats? The absence for a period of any successful cyber-attacks does not necessarily mean you have a comprehensively resilient sector.

Deborah Petterson: I will pass to Stuart in just one moment, but there is a thing about working in risk that the absence of an incident, the crisis that did not happen, is hard to judge and assign a value to. It has been estimated that the outage in the Iberian Peninsula cost the economy in one day €1.6 billion, I think it is. There is that very extreme example. The Jaguar Land Rover and Marks & Spencer incidents have shown the potential for loss to the UK economy, but for the actual metrics I will pass to Stuart.

Stuart Okin: The key metrics for the strategy will be around exercising and testing. You should not be looking at, as you have just said, incidents in that respect. You should be looking at exercising and testing. There are a number of different measurements even underneath that. With the operators of essential services at the moment, the critical national infrastructure, we have an assurance programme that we expect them to be sending to us every year—their assurance plan, how they are exercising, how they are testing—and we can pick up on particular areas. We have made it very clear in the objectives, that it is not about having a clear test result. In fact, we want you to go and find those problems, and that is very clear in our documentation. When you find the problems, how are you going to mitigate them? That is what we will hold you accountable to on the timelines. That is done with either individual or groups; the operators can group together and test that.

Then the systemic testing, which NESO will be conducting—we also do exercising and testing for big gas outages—usually in October, also includes electricity downward effect. Exercising, testing, constantly looking for problems, gaps and fixing those gaps are the KPIs that we measure the success on.

Q188 **Claire Young:** Given that we have new and emerging threats, such as rapid advancements in AI weaponisation by threat actors, how will the strategy be changed to counter those?

Stuart Okin: We have written, as a quota actually—we did this very quickly after the Mythos on 7 April. We wrote quite quickly to the operators to ask them to focus their attention on that particular area and indeed Poland's lessons as well.

The thing about AI, and it is really important, is that machine learning has been around for some time, and AI is just an extension to this. It is an incredible powerful thing and it will be absolutely necessary for us to balance the system. When we were talking about the weather system, there are some great AI solutions in cloud casting that I know NESO are using, so this is incredibly important, but also it can be used to

weaponise. NCSC recently came out with a blog about the fact that we now expect huge amounts of patching off the back of the Glasswing programme, and there are other similar models.

How does it change? It means that certain things like island mode become incredibly important. That is part of our inspections, to make sure that operators can literally pull the plug if they need to be able to do so. It is a requirement under our guidance and our overlays that they are able to work with either no digital or partial digital; it is actually an area. It will be tricky. We are expecting AI defence mechanisms to come as well in place, but there are mitigations we can take today.

Deborah Petterson: Can I build on that as well? The Claude Mythos or the ChatGPT 5.5 is already rolled out. I always like Jen Easterly's view on this—the ex-head of CISA in the US—that we do not so much have a cyber-security problem as we have a software coding problem with bad code. In some ways, rather than this being apocalyptic, it is also an opportunity because it is good at finding bad code. We will have a wall of patches to fix the bad code, like draining the swamp of all that enduring and legacy code that was not well-written in the first place. We have this sprint now, but it will leave us in a stronger place.

Q189 **Claire Young:** It has been suggested to us that it is not clear what types of cyber-attacker the Government are now expecting OESs to protect the energy networks from. Do you think that is a fair criticism?

Deborah Petterson: Do we care what cyber they are?

Stuart Okin: I am not sure it is a fair criticism. We have a very clear definition that NCSC has led us towards, which is then signed off as a risk appetite by DESNZ, which is the type of attacker—whether it is state or non-state—that we are trying to protect against is professional in nature, is able to use known vulnerabilities, and is able to stay undetected for some time and laterally move around the systems. That is the definition.

Then against that definition, NCSC have basically looked at all the different scenarios that they had seen in the past where people with that definition have been able to attack and have then developed the risk appetite. That is what we suggest that you have for controls and changes in place to prevent that type of thing from occurring or that type of attacker profile and their capability. That is what we work towards today.

Deborah Petterson: There are those that wish to do us harm and have intent to do us harm—and that could be hybrid, cyber, physical—and it is about our industry being prepared. What we have seen in the current geopolitical context is that we cannot predict tomorrow but what we can do is exercise and be prepared for a system that is agile and able to respond; so that is the objective.

Stuart Okin: The last thing I would like to add on to this—and this is probably more Deb's area from her past—is that essentially we are part

of an ecosystem, so we must not forget our cyber-offensive capability and our military defence capability. The operator's essential services are our last line of defence not the first line of defence.

Q190 **Claire Young:** You don't think there is any difference between nation state-level attacks versus compromised supply chains?

Deborah Petterson: I would anticipate a compromised supply chain would probably be a nation state anyway because you need a huge amount of resource behind you to do something in that space. I think on what you mentioned earlier, and you are absolutely right about AI bringing new threat, is that it almost democratises or allows the least skilled to become skilled. Whereas maybe even 18 months ago, the National Cyber Security Centre would have split your hacktivist from your nation state attacker, you are giving the nation state attacker skillset and capability to a less skilled individual. Hence my question that I am not sure that the definition matters any more.

Our operators of central services, and certainly in the energy system, see themselves as the frontline of defence. They are home defence, the Dad's Army of our day, who are there ready to defend and motivated to do so.

Q191 **Claire Young:** Stepping back from that, do you think there is sufficient Government and regulatory oversight of the cyber-protection of electricity transmission networks?

Deborah Petterson: I will allow Ofgem to defend themselves.

Stuart Okin: Again, in the last two to three years we have seen an absolute acceleration of focus, and you have designated a good Permanent Secretary as well.

Q192 **Claire Young:** Are there any gaps you would identify in that oversight?

Stuart Okin: The gaps are the ones that I have mentioned earlier on. There are quite a few gaps and they will be addressed by the Cyber Security and Resilience Bill, the supply chain being an example of that.

Deborah Petterson: The threat changes fast. When it comes to an outcome-based system, for us it is often loss of load expectation or the ability to restore in certain timeframes, because you cannot predict what the threat of the future will be. We have been admired overseas for having regulation that is outcome-focused, which does not assume a certain type of threat and a certain type of attack, and I think that is right.

We do observe gaps, and one of the benefits of the policy Department not being present in NESO's governance to create that independence means that we can observe, which can obviously bring a healthy tension sometimes between the policy Department and NESO. An example of that was observing where there was regulatory uncertainty in North Hyde and observing where there were issues that needed to be addressed by

Ofgem and DESNZ in who was responsible in certain areas. We are empowered to do that with the duty of candour that NESO has on risk.

Q193 **Claire Young:** Do you feel that your feedback on that is being listened to?

Deborah Petterson: They accepted every recommendation from North Hyde. Another example where again it was an uncomfortable message was our gas security of supply assessment, where last October we published the report that observed an emerging risk to our gas security of supply in five and 10 years' time. The Secretary of State ordered an immediate consultation on how to mitigate that risk that was emerging.

Stuart Okin: I was just going to say very quickly, one recommendation, as we move forward in the Cyber Security and Resilience Bill, is: do not be too prescriptive. There is always this challenge or there is this need to write everything down and to specify what every organisation should do. The problem with that is that we move so fast or whatever is written is out of date as soon as you write it, so be high level. One of the beauties of the new regulation is that an appropriate proportion of it is very high level.

Q194 **Claire Young:** One final very quick question. Stuart, how do you assess the adequacy of funding for cyber-security upgrades under the RIIO-3 price control framework?

Stuart Okin: For RIIO-2 and ED2, that period, about £2 billion was allocated for cyber, although that includes some control room upgrades, some big areas. That is not just for upgrades, that is for operations as well, the whole area. For RIIO-3, £1.2 billion has been allocated to the security side of things. Again, that includes full operations. In the RIIO-2 and ED2 period, the previous period, that created about 2,000 roles inside the sectors, which I think is incredibly important—you need to have that capability. As I said, that is where we are starting to see the sea change.

Q195 **Torcuil Crichton:** I am going to ask some questions about gas security, and, Deborah, for you to update us on what you have told the Ministers about that. First, you have been in cyber-security, infrastructure security, running the risk assessments for over two decades. Do you sleep at nights, should we sleep at nights and should Ministers sleep at nights?

Deborah Petterson: Just over a decade on the national security side. The UK is admired for the way in which the intelligence services have reached out to industry and partners and are more open, and the creation of the National Cyber Security Centre allowed for that. I feel that my job is to have the sleeplessness on your behalf. Having been immersed in the threat and the intent and the capability of those who wish to do us harm, it is really serious and it is not something we take for granted for the resilience of our system.

It has been fantastic joining NESO. There is a sense of mission by our power system engineers to maintain a secure and resilient system—itis like it is in their DNA. It feels like a very similar environment to that in national security. Therefore, our ability now to reach into the national security community, the outreach by defence and home defence to ensure we have greater and deeper partnerships, the information sharing that is being set up and is starting to flow, means I think you can feel confident in the UK, along with the real openness to the international security roundtable I mentioned the first we had.

We had our Five Eyes nations with the Ukrainians, the Latvians, and the Norwegians, talking through what it is like to have an aggressive neighbour testing your infrastructure all the time or destroying it, and then taking us through step by step what they are doing and what we need to think about. It is important not to be complacent, but you have an industry that really is not.

Stuart Okin: Just to add to that, you are two decades, mine is three decades. You can sit there and get very depressed continuously reading threat reports and risks and outages and also having to deal with them on the ground. Therefore, you also have to balance that with the costs that are associated with fixing that. Do we want to build bunkers around every single substation, and so on? Is that appropriate?

There is a constant flow between that risk profile and then the cost of repairing it, but I make no apologies. We have fined £30 million-worth of fines under NIS because we had not seen appropriate and proportionate action being taken, and we do so. I think that is where we have to take action.

Deborah Petterson: We must, of course, add we have an incredibly resilient grid—like, 99.999% resilience; it is one of the best in the world. I think that diversity of energy sources, the redundancy we have in the system already, and although that has been there—it was designed between the war periods to be a resilient grid in wartime, and it is absolutely right. We reassess the geopolitical threat.

The grid has been designed and our markets have been designed to drive efficiency and lower cost, but cost, resilience and clean are like three dials that we have to dial up and down depending on circumstance, and it is for Ministers to decide at any time where that priority is. We will always prioritise a secure grid, but we need to build in deep, increasing redundancy, increasing resilience. I think there is an active conversation at the moment about whether we can justify that investment.

At NESO, we have literally just been given the resource to create a new team, to look at cascade and compounding risk, to see if there is a sweet spot where we can invest that gives us both security, clean and affordable all in one place. I look forward to telling you more about that in future.

Q196 **Torcuil Crichton:** Can I ask your advice to Ministers on the gas network resilience there, where we get it from the North sea, from Norway, from through Europe and LNG?

Deborah Petterson: That is absolutely right.

Torcuil Crichton: What is your advice to me on what the best and most cost-effective way of securing gas supply is?

Deborah Petterson: As I have mentioned, we provide this independent assessment and analysis to Government on any risk to the system, and a fundamental tenet of resilience is having adequate resources, and gas is an integral part of our system. We are required under licence to publish each year a five and 10-year outlook on security of supply, and there is an emerging risk. The Secretary of State acted immediately on that to do a consultation that closed—I think it was about three or four months ago—and we are looking forward to hearing the assessment and how and what the approach will be to addressing that risk.

For me, as I have mentioned before, like with our supply chain, with our types of energy, equally with gas, having that diverse mix of gas—just to assure people in the middle east—this Committee is probably all aware but I do not think the public are—that we only secured 5% of our resources from the middle east. The vast majority of gas that we do not take from the North sea was secured from the US and Canada. After 2022, the gas split into two basins, with the middle east going towards the east and Asian nations and Europe being supplied by Australia, Canada, America. What we had anticipated before the conflict was the gas markets going to oversupply by the end of this year. In some ways, the conflict has brought it back into balance, but there is no shortage of gas molecules.

Q197 **Torcuil Crichton:** All that imported stuff is LNG that comes in?

Deborah Petterson: Yes.

Q198 **Torcuil Crichton:** How do we deal with the scenario of peak winter demand and bad weather and tankers trying to get into ports, for example? Have you looked at that?

Deborah Petterson: Yes. As I said, that comes into the modelling of 30,000 weather scenarios every single day. In the UK we have a security of supply standard, and that is that we have sufficient margins to supply gas on a cold day, which is a one-in-20 cold day—that is a period, actually, which stretches to 11 days, so we are looking across an 11-day cold, grey, still period—and with the loss of our largest piece of infrastructure. We compound both those things and then if we have sufficient margin to take us through our peak demand—for this January, I think our peak demand was about 45 GW—we feel we have sufficient supply. That is a security of supply standard we thought might to be at risk in five and 10 years' time that is looking forward to address now.

Q199 **Torcuil Crichton:** What is best to guarantee gas supplies? Should we build more storage? Should we import more energy? Should we take more out of the North sea?

Stuart Okin: Again, I am going to push back and say that is a decision for DESNZ.

Deborah Petterson: I think it is absolutely right that we have this broad and diverse range. You mentioned we have the Norwegian continental shelf and the UK continental shelf, which still provides just over a third of our gas. We have LNG and we have storage, and we have the interconnector to Europe. We have this basket of supplies that means we are not reliant on one single thing. The North sea is declining and it is declining at a faster rate, but of course we still have that and it is still there.

Stuart Okin: NESO are working on the spatial planning as well, so that will have a big influence on the design of the future.

Q200 **Ms Polly Billington:** I want to follow up, before I go to my international co-ordination question, on your reference to the people who do this as the sort of Dad's Army of the 21st century, which I like. I also note, however, that in the strategy it cites the fact that the UK faces a significant shortage of professionals who have the required combination of cyber and engineering skills with an insufficient number of security-cleared industry staff. Whose responsibility is it to tackle that problem?

Stuart Okin: I would say it is all of our responsibilities.

Ms Polly Billington: Forgive me Stuart, when it is everybody's responsibility it ends up being nobody's.

Stuart Okin: It is no one's responsibility, no, I get that. At the moment DSIT is running a big programme to try to improve that, but when I say it is all, we have been encouraging our operators of essential services to reach out, have apprentice schemes to connect in to do that training. There is a responsibility on ourselves to make sure that as part of the investment funds that are coming through RIIO, which was mentioned earlier, there is the ability to train an apprentice.

There are responsibilities there and then you have DSIT that takes a broader perspective on these things. It is a challenge and there is no doubt about that. I remember reading a report that said one in three posts are not being filled, which is not good. It is something that we all need to focus on. We have been running campaigns and we have had no shortage of applicants. For any particular campaign that we run we will get 500 applicants coming through. It is then making sure that they have the right skillsets. In Ofgem we pride ourselves on training people through. We bring them in early careers, train them through, and then if they leave and join the industry, so be it. It is something that we have responsibility for across the piece, but I understand your point.

Deborah Petterson: Skills is not an area that NESO covers, but we have our own apprenticeships. I know from my experience in the National Cyber Security Centre, the CyberFirst programme, the CyberGirls programme—I have always thought there should be a CyberSecond, so that would be my hat, a scheme for people looking to retrain. There is a degree to which the frontier AI will support building those skills and provide the tooling that is needed at greater scale. I know that there is a lot of government programmes in this space and we are certainly involved in the apprenticeships.

Q201 **Ms Polly Billington:** How serious is it as a risk? It feels a bit like our frontier is short-staffed.

Stuart Okin: It is a risk. I am not sure I have a number to put on to the risk. As I say, 2,000 roles have been created in the last few years, and been filled, and they cross everything from policy right through to engineers. We have some of the best universities in the country and some great apprentice schemes. It is a risk and something to be constantly focused on, but I would not put a number against it per se.

Q202 **Ms Polly Billington:** My final question is about international co-ordination. We went as a Select Committee to Brussels and visited NATO, talked to them about energy security and how it links into national security, as you mentioned, Deborah. How has sharing best practice with Five Eyes nations helped to better protect the UK's national infrastructure?

Deborah Petterson: We had an excellent meeting, and it is the Five Eyes learning from our European partners, too. In fact in my team we have one of the UK NATO expert advisers; my head technical officer for resilience also supports the UK in that way. Some of the best practice that the Five Eyes nations brought—New Zealand on that, the isolating—I think it is bringing up the drawbridge and operating independently and they talked us through that.

AEMO, our Australian partners, were talking through how they do whole-sector live exercising every year, and that is something we are certainly going to look to explore and how we could roll out with NESO, where you bring—and not just desk-based, like doing operational exercising across all market participants annually. Texas is talking through some of its work with data centre and intelligence sharing, and there is something called the Lighthouse Project in Canada, where they have this very deep partnership of how they enrich intelligence for their energy sector and get that out.

Equally, they were fascinated hearing Latvian stories, about how they are managing drones, the Norwegian total defence concept that you referenced earlier, and of course the Ukrainians talking about how they are securing their substations against drone attack and conflict. It was a really meaningful exchange, and we will be meeting with them in a couple of months' time to then decide the next steps of following up.

Another area involving the Five Eyes—actually, it was not that particular roundtable, but my team went for the first time to Washington for Five Eyes on space weather. Not all risks are geopolitical in nature; some are just the sun. The UK was in a period of intense solar activity that can have an impact on our grid and our digital infrastructure and how it operates. My team have worked with industry and partnerships to come up with new guidance, new codes for how we manage this period of high solar activity. Partly it is the Met Office supporting so we can predict it, and now we have rehearsed processes and exercises in place so we know how to step through that.

But New Zealand is well ahead on that and they have already rolled out some of the things that we are planning, and were able to say, "Actually do less of that, do more of that, we invested there, we recommend". The ability to share information freely and openly is enabling us to learn the lessons of others before we make mistakes ourselves.

Stuart Okin: That is a long list, so I will keep my list very short. We have to work internationally on all areas. Two years ago, as an example, we were involved in a European exercise—the very first European exercise on cyber—even though we were outside Europe but we were invited to participate. Ofgem participated in that.

One of my members is a voting member for the 62443 standard, which is an international standard that everybody looks to from the operational technology perspective in cyber and energy, and indeed in other areas like water and so on. Looking at the internal energy markets and coming together on that requires even further integration potentially with our European colleagues. There is a lot of work that we do.

To finish off, again, my pick on the area of supply chain, there is no way that any single country can dictate a supply chain. It has to be an international effort because we have suppliers coming from all sorts of places. We are very lucky in the UK. We have General Electric and Schneiders and a few others where they send to themselves software development here in the UK. That is very good but we cannot rely on that. We have to work with our international partners, especially the Five Eyes, in developing standards and guidance, and so on to help the supply chain secure us through the future.

Q203 **Chair:** To come back, Stuart, to what you said about the European energy market, how important do you think it is that we have closer integration in energy? We have seen the discussions around closer ties, but there is some way to go in finalising arrangements. What is your position on where you think we need to get to?

Stuart Okin: Again, I want to be very clear, it is DESNZ's decision on internal markets and our integration.

Chair: But as you mentioned it.

Stuart Okin: But as I mentioned it, we obviously therefore will respond to that. DESNZ has said it is looking towards that, so we need to respond. Our response from a cyber perspective is to look into what we need to do differently. Things have moved on in the last few years, and generally a lot of the guidance and standards in Europe still have not been ratified themselves. We are in a very good place to be able to integrate from a cyber perspective. I think that a little bit more work will be required to make sure that we are at various parts of the various different committees that are run there. But in enacting it within the UK, if we decide that is the route that the Government wish to take, from a cyber perspective it will be okay.

Q204 **Chair:** What about from a supply perspective, supply of energy, energy resilience?

Deborah Petterson: We are physically connected to 10 European nations. Our control room is speaking every single day to our European partners on managing supply and connection. Also we have been invited as NESO again, because we are set slightly apart from Government, to sit and observe on ENTSO-E. We are part of Coreso and part of the Hamburg Declaration on the North sea and offshore co-operation. As I said, there is real openness to partner and regularly partnering and speaking and joining. While we will also give formal advice to DESNZ and the Cabinet Office on any negotiations looking at the formal European arrangements, informally, on a partnership level, we are working with them day in, day out.

Q205 **Chair:** Deborah, to come back to what you have been saying about civilian and military resources working together—and in particular you quoted the Norwegian approach—it strikes me what you are advocating here is seeing the energy resilience funding that we have, whether it is with NESO or more widely, as a part of defence. It feels like you are suggesting that doing something along those lines would be helpful.

Deborah Petterson: I would not dream of suggesting how the Government spend its money. However, it is absolutely true that article 3 of NATO talks about resilient grid infrastructure. Article 3 is how we defend and look after our own nation, and a resilient grid infrastructure is listed as one of the elements. I have certainly been talking to home defence, understanding joint command in MOD about our closer partnership in this space.

Q206 **Chair:** Even if we do not formally allocate it as defence spending, we should be confident in seeing it in those terms?

Deborah Petterson: I would describe energy as mission-vital infrastructure for defence, and therefore would expect them to be extremely interested in the resilience of our grid.

Chair: That is very helpful. Thank you, both, for your extremely helpful and informative evidence, and that ends our session.