

Joint Committee on the National Security Strategy

Oral evidence: Undersea cables

Monday 9 June 2025

4.30 pm

[Watch the meeting](#)

Members present: Lord Sedwill (The Chair); Dame Karen Bradley; Sarah Champion; Mr Tanmanjeet Singh Dhesi; Baroness Fall; Lord Hutton of Furness; Baroness Kidron; Edward Morello; Lord Robathan; Emily Thornberry; Lord Tunncliffe; Derek Twigg; Lord Watts.

In the absence of Matt Western, Lord Sedwill was called to the Chair.

Evidence Session No. 4

Heard in Public

Questions 31 - 46

Witnesses

I: Chief Constable Gavin Stephens, Chair, National Police Chiefs' Council; Laura Catterick, Director, Resilience and Cyber, UK Finance; Alex Towers, Director of Policy and Public Affairs, BT Group; Dr Fenella Wrigley MBE, Chief Medical Officer and Deputy CEO, London Ambulance Service.

Examination of witnesses

Chief Constable Gavin Stephens, Laura Catterick, Alex Towers and Dr Fenella Wrigley.

Q31 **The Chair:** Welcome to today's meeting of the Joint Committee on the National Security Strategy. This is our third session in our inquiry into undersea cables and today we are focusing on national resilience and recovery in the event of severe disruption to undersea cables from a co-ordinated attack. The intention is to explore load-bearing assumptions that underpin business continuity and crisis response plans. This is particularly timely given the recent publication of the strategic defence review, which set out the need to increase our readiness for, as it quoted, "the immediate and pressing" military threat from Russia and the risks of unintended escalation.

We are very pleased to have a distinguished panel with us today to help

us navigate some of those questions. Could I ask you first to introduce yourselves briefly, and then we will get into the questions?

Dr Fenella Wrigley: I am the medical adviser to the central ambulance team at NHS England. I am also the chief medical officer and deputy chief executive of London Ambulance Service, and a practising emergency medicine consultant in London.

Chief Constable Gavin Stephens: Good afternoon, all. I am chief constable and chair of the National Police Chiefs' Council, which is an organisation charged with co-ordinating UK policing's response to operational issues.

Laura Catterick: Hello. I am representing UK Finance. I am the director of resilience and cyber there and I am here on behalf of the financial services sector.

Alex Towers: I am the director of policy and public affairs at BT Group. We operate a large amount of the nation's telecoms infrastructure.

The Chair: Thank you all for joining us this afternoon. You are probably familiar with the procedure, but different committee members will lead off on different questions for you. I will start. I will ask each of you to say something about the first question, but thereafter committee members will probably address certain questions to you as individuals. Others of course can chip in, should you wish to do so, but we will try to keep the session moving, because we have quite a lot to get through in the next three-quarters of an hour or so.

As I said, we are examining the UK's national resilience in the event of heightened political tension and large-scale targeting of subsea cables. We have heard that co-ordinated attacks could cause major disruption, but we have had a variety of evidence on the extent of that.

Starting with you, Chief Constable, are you aware of comprehensive assessments about strategic reliance on subsea cables in your area and in law enforcement generally? Is the contingency planning for that—I will be asking everyone else the same question—in the shape you would expect it to be?

Chief Constable Gavin Stephens: The candid point to start with is that this committee has prompted us to look afresh at our plans, which is always a good thing. We have a fairly comprehensive assessment as to what we think the impact would be. To give an example of that, our Police Digital Service has reviewed 68 national systems that we think are important for the continued functioning of policing. There are only seven of those where we do not have legal guarantees from the providers that the data is held within the UK and could continue to operate within the UK in the event of disruption, so clearly there is still some work to do in those areas.

The disruption for us would largely depend on the amount of time delay that standing up alternative systems caused. For example, we would

expect our radio systems to continue to operate, but there are other systems, such as the storage and retrieval of digital evidence, of which we might see some short-term disruption. It really depends on how long that disruption is. We would look to other industry partners to help us with that.

The second part of contingency planning for policing is the second-order impacts, so the sort of thing that we see at times of any other national crisis. Lack of clarity and communications would be one thing. We have seen many incidents recently where that lack exists. The space is filled with mis and disinformation, so we would very much want to work together, boosting national contingency arrangements and local resilience forums to fill that space.

We know that there is a risk of changing public behaviour if the public become worried, whether that is access to their money or supply chains of usual day-to-day provisions. Of course, we have had the experience of the pandemic where we all needed to respond to that.

Overall, there is a generally healthy position of some resilience, but very much dependent on the length of the disruption as to what the consequences would be for policing.

The Chair: In terms of back-ups and so on—that is not a technical phrase, but you will get the point—a lot of recovery depends on that. To what extent do you have that kind of redundancy built into your systems?

Chief Constable Gavin Stephens: I mentioned the 68 national systems that we have assessed through our Police Digital Service. As I say, for all bar seven of those we have legal guarantees that the data is held within the UK and would continue to operate within the UK, giving us access to those. I always operate on the basis, though, that we can predict some unexpected disruption.

Provided we have the core ones, such as radio communication and 999 functions, the main features of policing, as we understand it, would continue to work. We would quickly stand up, if there was to be any protracted disruption, two-tier co-ordination arrangements in the usual ways through the Civil Contingencies Act and local resilience forums. Part of my organisation at the national level is a national centre for co-ordination. The most recent time we were stood up was in the summer disorder of last year, where we worked with Government and COBRA to co-ordinate that response. We have had exercises recently, such as Mighty Oak, which looked at bigger disruption, the loss of power for example, which would be much more problematic for us. Our assessment of this is that we would be able to cope a bit better.

The Chair: We will drill into some of those issues in more detail, but Dame Karen wanted to come in briefly on that.

Q32 **Dame Karen Bradley:** Yes, it was the fact that you kept referring to all but seven. Is any of the seven critical? Do you have back-up on the

seven? Are you looking to have contingencies on the seven? What work are you doing to make sure that that data is secure?

Chief Constable Gavin Stephens: We have guarantees about the security of the data. Otherwise we cannot let the contracts, under government arrangements. On those seven we do not have assurances that the data is solely held here in the United Kingdom. It might be elsewhere within our European partners.

Those seven are significant providers and we have verbal assurances from some of those major providers that there is redundancy or contingency in the system. The point I was making is that they are not currently part of the legal agreement that we have with them. That is something that we clearly need to work through.

Dame Karen Bradley: You are looking to change that and make sure that we move stuff to the UK to protect it.

Chief Constable Gavin Stephens: Yes, whether it is moving everything to the UK or achieving those absolute guarantees that it would continue to operate in a disruption such as this.

Dr Fenella Wrigley: With regards to preparation, like all emergency services NHS England and all NHS providers undertake significant planning and preparation for a range of incidents. The incidents could be anything from the pandemic we have talked about to civil disorder, road traffic and big infrastructure failure, but also technical and IT issues. Assurance plans are tested on an annual basis, so all ambulance services and category 1 NHS providers have to go through an annual assurance framework, where they evidence that they have met the framework and standards required. The last annual assurance included assurance around IT and cyber. While not directly looking at underwater cables, some of it can be translated across from the fact that that was done.

To provide assurance, the key NHS systems are all UK-based. The Spine, which holds demographics, the clinical systems and electronic prescribing, is based in the UK. The telephone systems are all held in the UK, as is the computer-aided dispatch of ambulances. In the event that this happened, the usual ability to take 999 calls would be there. We would be able to dispatch ambulances. Where there may be some risk is that the patient notes taken by ambulance crews in particular are now held electronically. If the overarching internet was slowing down, that system may be slowed and we do not know that all the systems held by hospitals would still be working. There are fallback systems in place in order to be able to revert to paper within our control rooms for all the 999 services, but also to be able to take patient records.

For primary care, because obviously patients may be accessing care through their GPs, there is still work to do there. They are not currently assessed under the assurance framework, but that is work in progress to be able to bring them into that situation. It is expected that, from the NHS, all the systems would work. Where the risks would happen is if the

whole internet was slowing down. Then there may be a requirement, under a command and control system, to agree that we went to business continuity plans, which would increase efficiency by reverting to some of the paper operations.

The Chair: Thank you very much. Baroness Fall is going to lead some further questions on the impact on the NHS. Ms Catterick, we are very interested in the impact on the financial services.

Laura Catterick: It is slightly different from my two panellists. We are very reliant on our financial systems to work internationally, so we are interconnected globally. We are one of the biggest hubs in the world, so there would be an impact if there was a severe outage with multiple cables being cut in multiple locations. That being said, if it was one or two cables, we are very able to withstand that. We have seen that happen before and there is significant and robust contingency in place. Speaking on behalf of the sector, we think that this would be a very highly unlikely scenario. If it happened, it would be in a time of very significant conflict.

In terms of contingency, there are three different aspects I will pull out. One is that the cables themselves are very resilient. There is redundancy built into them. Big firms have multiple cables. They are architected in a way that their systems are resilient, so that is the first thing.

Secondly, there are operational resilience regulations in place within the UK. All firms are regulated and have to adhere to those, so individual firms have significant plans in terms of scenario testing, playbooks, disaster recovery, inbuilt resilience, and understanding and mapping the entire supply chain for material services.

Lastly, there is sector resilience. There is something called the Cross Market Operational Resilience Group. That is a public/private partnership with the Bank of England and firms. It works collectively to ensure that the sector is resilient. It does scenario testing. We did one last year on the national power outage. If that happened, what would that look like and how would we withstand that?

The Chair: Thank you very much. Mr Twigg is going to lead some further questions on impact on financial services and more generally. Mr Towers, you are responsible for the platform on which so much of the economy now rests. I wanted to come to you last to ask about impact and contingency, please.

Alex Towers: The first thing to say, a little bit like Laura was saying, is that there is a lot of resilience built into the system. The internet itself is not a single command and control designed system or operation but is highly disaggregated, and that provides quite a lot of resilience. There are between 50 and 60, I think, international cables that find their way to the UK. On top of that, there is also a whole load of cabling that goes through the Channel Tunnel, which obviously has a different level of security attached to it than anything that is on the seabed. We put all sorts of security measures around the slightly weaker points in the

system, where the cable landing points are, for example, some of which we operate, and the cyber protection that applies to those sites and to the network more generally.

There is a lot of contingency built in in that sense and it is hard to imagine, therefore, the sort of scenario that leads to a very large proportion of all those cables and components being removed in a single incident. At the same time, much as the emergency services have said, the sort of immediate life and death operations that we need to provide, so the basic phone system and mobile phone networks, are all designed in a way such that they have no reliance on the public internet or international connectivity. They run within the UK on UK-based systems. Everything that we do in terms of our 999 platform, for example, or the emergency services network that we will be supplying to the emergency services once the Airwave system is decommissioned, similarly can be done from within the UK, without any reliance on the international connectivity.

That leaves the question of what would happen were there to be a really dramatic, concerted and co-ordinated attack on a large proportion of all that infrastructure at the same time. That is, frankly, a scenario that perhaps we are less well prepared for, in terms of the historic pattern of the risk that we are trying to plan for, than potentially we might be. It is a good time, given what the strategic defence review says and the state of the obvious threats out there, to be asking the sorts of questions you are asking. There probably is some more intensive stress testing to do of all the different component parts of the system, how they talk to each other and where there could be frailties in those or risks to manage.

As I say, I think this is highly unlikely, but, if all the subsea cables were to be severed simultaneously, for a short period of time lots of things would carry on working because they would all be UK-based. It would not take very long for there to be quite significant issues about all the parts of the internet that depend on, for example, what is called the DNS service—the kind of phone book of internet operators—which is not based in the UK but is disaggregated around the world. Everyone's systems that rely on authentication, monitoring or global software providers that might be providing updates, all that sort of stuff, is entirely based on the global fabric, as things stand. While that seems a very distant prospect from where we are today and what we know about everything from the past hundred years' worth of protecting this infrastructure, it is a good time to be asking the question about whether there is a more significant level of threats to start planning for.

The Chair: You will understand that the committee is very interested in the acute as well as the chronic, given the circumstances we are now in. We will pursue some of those points in our detailed questions.

Q33 **Baroness Kidron:** Mr Towers, I love the fact that you said "hard to imagine" but I am now going to ask you to imagine. Sorry about that. If we could just drill down, I absolutely accept that you say there is resilience built in. You raised the spectre of a catastrophe, but what about

a more moderate situation? We are interested in what goes first. Where are the vulnerabilities? I will lead the answer by saying, "What about air traffic control?" Are there certain pieces of the infrastructure and the economy that feel particularly vulnerable?

Alex Towers: That is a slightly bigger question than maybe I am qualified to answer, but I will have a go. The first thing to say is that, as we have variously been saying, there is quite a lot of redundancy built in. Sixty cables is an awful lot. If you look at other international situations that have unfurled in Ukraine, for example, or the situation in the Baltic Sea, where two cables were cut, in the Baltic there was almost no publicly noticeable impact and even in Ukraine everything has carried on working.

In the sense of the scale of the network, the amount of infrastructure that there is and the capacity for traffic to be immediately rerouted automatically to the quickest available route, that provides quite a lot of reassurance. You would have to be talking about a really very significant series of outages for there to be the sort of impact that you are describing. None the less, it is an interesting question and perhaps one that we in our industry should do a little bit more work on and analysis of with the Government.

In terms of prioritisation of physical resources in emergency situations, so the kind of activity we undertook during Covid, for example, or the planning we did for a no-deal Brexit-type scenario, we have a very clear prioritisation of what is important. It is CNI, vulnerable customers and then category 1 and 2 responders. That works very well when you are talking about internal infrastructure that you can send teams to go and fix.

It is a slightly different question if you are talking about the internet itself being dramatically constricted in capacity and whether there are different ways of actually prioritising what traffic is given prominence. It would be a different world to the one we have traditionally lived in, where everything is treated equally, as a matter of principle, in terms of traffic, but it is a question worth considering perhaps. As I say, we probably need a bit of guidance from the people who know about the risks as to what level of risk we should be trying to anticipate.

Baroness Kidron: That is very interesting. Thank you. I wanted to ask a very specific question about the .com versus the .uk, because my understanding is that it may be that the .uk survives a little longer and better. Could you say a little bit about that?

Alex Towers: That is also my understanding. I need to caveat by saying that I am no one's idea of a deep technical expert here. Yes, .uk and all that data, systems and caching is done within the country, so that should survive for a period without any noticeable impact, whereas .com and .eu are things that clearly need to be travelling backwards and forwards internationally and are more vulnerable if there is literally no way of passing traffic internationally.

At the same time, if you had an absolute total outage, which, as I keep saying, seems extremely unlikely, it would not take a huge amount of time for .uk to start encountering problems as well, I think. All these systems rely on constant refreshing for different services and directories. I caveat for my lack of deep technical expertise, but I do not think that it is the sort of situation where we would be fine for weeks or months with that system. We would need to also be worried about that.

Baroness Kidron: You said that it is most likely that, if anything happened, it would be a couple of cables, and I understand that. Are there agreements in place about rerouting, or is it automatic?

Alex Towers: Yes, it does not really work like that. It is kind of automatic with networks. The internet is based on a series of protocols about how all the different networks talk to each other. In effect, that will happen automatically and the traffic will find the most efficient route.

Q34 **Derek Twigg:** Ms Catterick, can we maybe drill down a bit more into the potential impacts of any internet disruption? It could, I suppose, range from a complete freeze of the financial system globally to, for example, where people cannot use their cards or you cannot use internet banking. I would be interested to know what scenarios you have, for want of a better phrase, war gamed, in terms of what could happen. Do you actually know the number of cable systems that the financial services rely on?

Laura Catterick: I will take your last question first. We know that the individual firms know which cables they rely upon. We do not have a financial services sector view of those cables. We do not know whether there are choke points, vulnerable cables or more important cables. That would be something that we would be wanting to know. One ask would be, "Could we have that view?" That would help, from a sector perspective, plan resilience exercises. That is answering the first question.

Derek Twigg: The obvious next question is what you are doing about that.

Laura Catterick: We are engaging with our service providers individually and collectively. This scenario is on the national risk register. It is one of the scenarios where we play war games, to your point. We definitely need more transparency on the chokepoints or vulnerable areas.

Derek Twigg: As things stand today, on 9 June, the financial services sector does not have a grip on what cables can bring the whole system down if attacked. It is just individual financial services organisations.

Laura Catterick: We do not know. Yes, that is correct. That is one of the asks coming out of this. Your first question was the impact. It would depend on which cable was cut, when it was cut and how many cables were cut. That could therefore lead to various impacts.

Derek Twigg: You must have war-gamed something in terms of what

the worst possible scenario is. It must be the global financial system freezing.

Laura Catterick: Yes, but the ecosystem is made up of multiple firms. It would have to impact multiple firms in multiple ways to bring it to a complete freeze.

Derek Twigg: Are you ruling that out as being in any way possible that that could happen?

Laura Catterick: We are not ruling it out as a possibility. It is, like I said, on the national risk register. It is something that the firms are considering. Multiple firms have discussed this with their boards. It is part of their scenario exercises. Like I said, it would have to be multiple firms in a very co-ordinated effort and attack.

Derek Twigg: It was reported with the incidents in Shetland a few years ago that people could not use their cards. Is that correct?

Laura Catterick: That is, but my understanding is that there is only a very small number of cables that connect Shetland. That would be an area that would be vulnerable in the UK, and we have seen that happen.

Derek Twigg: Right, but it could happen for the whole of the UK if certain cables were severed or disrupted.

Laura Catterick: Out of the 50 or 60 cables, the majority of those would need to be severed.

Derek Twigg: What about contagion? If this hits the financial sector, have you looked at what contagion there could be to affect other sectors?

Laura Catterick: It would absolutely have downstream impacts, again depending on the scenario, how many cables were cut and what the impact was.

Derek Twigg: What is the worst-case scenario that you have looked at?

Laura Catterick: The worst-case scenario would be that the payment schemes would be impacted. That would impact our ability to connect globally and do international trading and international payments.

Derek Twigg: The markets would come to a standstill.

Laura Catterick: Correct.

Q35 **Mr Tanmanjeet Singh Dhesi:** I want to come on to emergency services and response plans. Chief Constable Stephens, to what extent might police work be affected by severe national internet disruption?

Chief Constable Gavin Stephens: As I explained in the opening, in the short term we anticipate that we would be able to operate the vast majority of our systems in the usual way. The police service has a good

track record of being able to pivot activity at times of national crisis if the disruption was more than anticipated.

In our planning, our main concern is the second-order impacts, some of which we have just been exploring. For example, if the public could not access their money, that leads to changes in public behaviour. If they could not access certain goods and services, that leads to changes in behaviour. It would be the response to the policing of those that would require us to pivot our activity, but we have some confidence that the function of policing itself would continue in the usual way.

As we have heard from the health and ambulance sector, we also have well-trying and tested procedures so that, if we have loss of systems, we are able to still keep going. For example, it is not unusual for a force to lose a command and control system. Often it is associated with a software upgrade that goes wrong. You have to roll back and it takes a day or two, or three sometimes, to get it going again. We are used to dealing with those sorts of scenarios.

The question would be if it became much more widespread. Our assessment of that depends on the duration of the impact. I know from speaking to colleagues that we can expect repairs to be done in 11 to 14 days to make the system more stable again. For us, it is the second-order impacts, and we are well-practised at dealing with those.

Mr Tanmanjeet Singh Dhesi: We saw during last summer the racist riots that were triggered by misinformation and disinformation emanating predominantly from social media. That was without a severe national disruption. With a severe national disruption to our internet, would you anticipate any public disorder or protest? What challenges would that pose?

Chief Constable Gavin Stephens: Whether there is disorder would depend on other impacts. The assessments of the precursors for disorder are pretty well trodden. It tends to be in the summer, when the weather is hot. It tends to be when there is dissatisfaction with government and there tends to be a trigger event that sparks it. Last summer we saw that take place in the most awful way.

One new phenomenon that we now have is the speed and pace at which mis and disinformation can spread on the internet and not just policing but government and public services' ability to counter that narrative. It is in a scenario like this where policing would very much welcome national co-ordination of any messages. For example, if it was in the financial services sector or disruption to the broader internet, we would look to others to be able to get accurate, timely, honest information out there to the public, so it enables us to manage the response much better. It is in the absence of those that you start to see changes in patterns of behaviour. Certainly, if people cannot access their money, for example, we would expect disruption at that point.

Mr Tanmanjeet Singh Dhesi: Dr Wrigley, as the chief medical officer

and deputy CEO of London Ambulance Service, we have already heard from Baroness Kidron about the differences between .com and .co.uk. Do any of your systems involve servers or support protocols based outside of the UK?

Dr Fenella Wrigley: Across the NHS, the main NHS systems are all based on UK servers. NHS Spine, which is your demographic summary care records, the NHS App, NHS login, the electronic prescription service, NHSmail and GP Connect are all UK-based. The vulnerability would be if there was a co-ordinated attack on to multiple UK landings, where you may lose a regional area, in which case there are very well-practised and clear plans about how we support each other in different regions to take telephone calls, pass telephone calls back again and dispatch ambulances.

If it became wider spread, the vulnerability, linking back to the British Telecom update, is if you cannot take the telephone calls or 999 calls, and then how you communicate out what the patient or the public need to do in that case. As assurance, each of the telephone systems within the emergency services has two tiers, so it has an immediate fallback. If the first one was taken out, there is an automatic fallback to a second system, which is held on a completely separate server. It would be fair to say that, for emergency services, not being able to answer a 999 call would be the greatest risk. We have heard from BT that that would require a catastrophic event to happen to the cables.

Mr Tanmanjeet Singh Dhesi: Chief Constable, there is a lot of international partner collaboration, especially your policing work with Interpol and other agencies across the globe. What impact would there be on intelligence sharing with our international partners in the event of a severe national internet disruption?

Chief Constable Gavin Stephens: The impact would likely be on the speed of the intelligence sharing. For the most high-risk scenarios, we have separate and secure systems to communicate with international partners. Clearly, there is a scenario where they could be taken out as well, but, as we have heard, we are unlikely to lose telephony systems and so on that would enable that to take place. With the EU reset process, we are looking to reinstate some of the automated systems that we lost in EU exit. There is the potential for some of those to be disrupted, but we have been working around that since EU exit.

Q36 **Dame Karen Bradley:** Chief Constable, I have a quick question. You have talked about centralised functions for dealing with miscommunication. You will know that the Home Affairs Select Committee looked at this as part of our work and you gave evidence to us. I am wondering whether you have any messages for the Home Office in regards to the forthcoming police reform White Paper and whether that is something you would like it to be considering.

Chief Constable Gavin Stephens: I have just come from a two-hour session on police reform with colleagues in the Home Office. Our ambition

on police reform, regardless of the difficulty of the current spending review we find ourselves in, is unabated. I am pleased to say that, in the current financial year, post summer disorder, we have already received some additional investment from the Home Office to strengthen our ability to deal with mis and disinformation, and strengthen the national co-ordination of that response, particularly in order to pick up on one of the recommendations from our national inspectorate, which was about the earlier identification of potential flashpoints for disorder. We are making some progress.

- Q37 The Chair:** We are thinking about a concerted attack. We are thinking here in circumstances of potential state conflict. Imagine a scenario in which undersea cables are cut, probably not all of them but some of them, there is a cyberattack and a deliberate disinformation campaign. All this takes out the mobile phone networks, disrupts food supplies to supermarkets, disrupts financial services and then tells people that the country has ground to a halt. At the beginning of Covid, we saw fights in supermarkets over loo rolls, as I recall. Without over-catastrophising it, how good is the contingency planning against a concerted set of scenarios, as opposed to looking at individual potential risks?

Chief Constable Gavin Stephens: The short answer is that it is not good enough at this stage. We are all recognising the change in the global security picture that you describe. In that sort of scenario, we would be into a different mode of operation in policing. In parallel to this scenario, we are already in planning with colleagues in the Home Office and Ministry of Defence about what the role for policing would be in times of international conflict such as that. Clearly, we would take on responsibilities for other aspects of, if you like, a home defence response, which I know the Prime Minister has spoken publicly about recently. We would need to pivot our activities.

It then becomes a question, as other colleagues have commented, of prioritisation. Policing would have a view, for example, on what prioritisation of traffic we would want to see over the internet if we were in that space. That would be a view that we would need to feed into the national decision-making structures. If I can add a bit of levity, just for a moment, there would be some internet services that we would be happy to see offline. Others clearly would be critical to operation.

The Chair: That is a fair point.

- Q38 Lord Robathan:** Just to be quick, you can tell me I misunderstood your preceding answer, if you like. You said that you have been to the Home Office and come up with all sorts of superb plans as to how things were sorted. Is that broadly what you said?

Chief Constable Gavin Stephens: I wish it was as positive as that. In the summer disorder we recognised some of the weaknesses in the national system of how policing responds. We have worked with the Home Office on a business case to strengthen some of those national capabilities and that is in the process of being implemented.

Lord Robathan: What exactly are you going to do?

Chief Constable Gavin Stephens: One function of the National Police Chiefs' Council is the National Police Coordination Centre. The function of that is to provide co-ordination of resources across the totality of UK policing's interests, whether it is here or overseas. We have, as it stands, a limited central intelligence function, which is going to be strengthened as part of that investment. We have a limited capability to get earlier warning, if I can put it that way, on things that might be flashpoints for disorder. In the summer disorder of last year, we relied very heavily on Cabinet Office capabilities, for example, and capabilities that other partners were able to bring to bear, but we would like to bake some of that into policing so we have that capability for ourselves.

The Chair: We would like to move on to health. Baroness Fall, you are going to lead us into this.

Q39 **Baroness Fall:** We have touched on some of this topic already, but I would like to come back to a few points. So I am absolutely clear, you are content that we are not so reliant on international servers that, in an emergency, we would be unable to operate an ambulance service and continue in operation as usual in the NHS. I wanted to start with that overall question.

Dr Fenella Wrigley: While UK-based servers are working, the NHS critical systems are on UK-based systems, so they would work. The challenge would come when the position changed such that the flow of information across the internet, as has been described, began to slow down the UK-based servers, at which point there would be a decision made, potentially, as to which parts of the NHS needed to revert to business continuity plans in order to maximise the efficiency, maintain patient safety and be able to serve patients.

Baroness Fall: You have contingency protocols in terms of prioritisation under that.

Dr Fenella Wrigley: Yes. If we found that we could take the 999 call but the system by which we triage using a computer system and dispatch an ambulance was slowing down, we would revert to paper and using the Airwave radio to be able to dispatch the ambulance. We could revert to paper for our patient notes, handing over paper when a patient was taken to hospital. Prescriptions can be done on paper, so that we are able to maintain services and those critical urgent and emergency services for patients. The data that is held on patients has redundancy built in, so there are second levels of data being held. Again, as the international internet issue began to impact on the UK-based internet, some of that may be lost and therefore you would revert to being able to do real-time assessment of patients.

Baroness Fall: To focus in on this point about paper, as we are moving towards a more digitalised NHS, are we not moving away from paper? Is that something that you have been discussing in terms of a strategic

decision to keep some on paper as a contingency?

Dr Fenella Wrigley: Most of our systems are now digitalised within hospitals, the ambulance service and primary care. However, there is paper available so that, in the event of either a situation like we are talking about today or just an upgrade happening that requires us to be able to take down a whole system, the teams are all trained and practise using paper and being able to do all of their clinical care on paper.

Baroness Fall: They could not necessarily access a patient record.

Dr Fenella Wrigley: No.

Baroness Fall: Okay, so there is an issue there.

Dr Fenella Wrigley: Yes. It would take longer to see each patient because you would not have the advantage of being able to look at their past record and their medication that they are on. It would take longer, but it would still be deliverable.

Baroness Fall: It looks like we have a sort of bottleneck around 999, and I am looking at the Chief Constable on your right. You have two emergency services both reliant on one number, which you have pinpointed as a potential weakness. Should we be looking more carefully at how we mitigate that as a high risk?

Dr Fenella Wrigley: That is potentially for our BT colleague. All our phone calls come in through BT and then go through a switchboard out to the right emergency service.

Alex Towers: That system already has quite a lot of contingency and resilience built into it. We operate a number of call centres that then interface with the different emergency services. As I say, none of that system relies on any international internet connectivity. Although, if you are talking about a significant civil disorder sort of situation, you might see a peak in calls, there should not be any technical reason why the system is not able to handle it in the same way that it does today.

Q40 **Dame Karen Bradley:** I have a follow-up on the concern around ambulance services and this use of paper. If I look at my own area, West Midlands Ambulance Service is now responsible for ambulances across Staffordshire. We used to have Staffordshire that was on its own and we are now part of this consolidated much larger ambulance service. Are those very large ambulance services able to get to all parts of their area using paper? How on earth would you prioritise and make sure ambulances were in the right place if everything is being done by paper and not digitally?

Dr Fenella Wrigley: When a 999 call comes in, it is triaged through one of two systems, using two approved triage systems, which gives us the priority for the patient. A patient who was unfortunately in a cardiac arrest, so their heart has stopped beating, is obviously a category 1 and immediately dispatched. That is done, on a daily basis, electronically. It is

sent down to the ambulance crew through an electronic system and the ambulance drives to where the patient is.

In the event that that system was not working, the ambulance crew and operators within the emergency operations centre have radios. They would say to the ambulance crew, "We need you to go here". That enables them to use map books and get to the patient. The patients are prioritised in exactly the same way. We would inevitably see some delay for the lowest category of patients. We would work in conjunction with the police, because obviously we do not want more people out on the streets, but they may be advised to make their own way to an urgent treatment centre or hospital, or indeed self-care pharmacy first. The seriously ill patients regularly, when this work is going on, can be dispatched by radio. The crews and emergency operations dispatchers are trained to do that.

Dame Karen Bradley: The size of the area you are covering does not matter.

Dr Fenella Wrigley: No. In the event of one ambulance service not being able to do it, there is a way to dispatch ambulances from another ambulance service through a hailing channel. It is probably similar for the police force. We could lose sections of the country and still be able to support each other.

The Chair: We have heard about the number of cables we have, but of course they come ashore, and Mr Morello is going to ask about some of that.

Q41 **Edward Morello:** We heard in previous evidence sessions about the actual physical difficulty of deliberately targeting undersea cables. It was raised that a weakness in the system is the point at which they land in the UK. I am interested, Mr Towers, in the industry perspective on whether we have enough protection around those landing points, whether they require upgrading and whether that should be the responsibility of the sector or the state.

Alex Towers: There is never any room for complacency about that particular risk, because it is an obvious thing to ask, as you say, as to whether that is a weaker point in the system than something that is underneath the ocean. We have a lot of physical security measures that we take and put around those sites. We do not operate all of them. I think that we operate about 10. The security measures range from very basic and obvious locks, fences and things through to CCTV and more complex cyber stuff, but we are always reviewing it. At the minute we are in the middle of a programme of upgrading those sites, which will run for the next few years.

It is a good question as to whether there should be more joining up between the industry and the other emergency services and security agencies. We feel like it is our responsibility to keep those sites safe, but

we are constantly trying to talk to all the different actors to make sure we have done the right amount of contingency planning.

Edward Morello: Chief Constable, I am interested. At the moment, the broader security around critical national infrastructure, including those landing points, falls within the responsibility of the police. The strategic defence review included proposals for the creation of a new reserve force to guard critical national infrastructure. I am wondering what the view of the police is as to whether you have the skill set required to secure that, whether it requires an additional service or whether a defence force is the right track to go down.

Chief Constable Gavin Stephens: We certainly do not have the resource levels at this stage to do it. Not associated with this contingency plan but for broader plans that we are making, we are looking at the number of colleagues we have who are already military reservists, for example, or indeed are in that period since they have left but have now joined policing, who could be recalled in times of international conflict.

We fully understand that, if we were in a time of conflict, policing would have a role to play in that. As we have seen at other times in our history, other things then do not get done. We would make those choices. I guess that it is a choice for the Government whether they want this capability to be readily available or want uniformed civilian services to be able to pivot towards these choices at the time that they were made. What I could say with some confidence for policing is that we are an organisation of problem solvers and will lend our hand to whatever challenge comes our way. We have got a considerable amount of work to do to dust off some of the plans that perhaps have not been looked at for a few years.

Edward Morello: Can I clarify your answer there? You started by saying that the police do not have the resources currently to protect critical national infrastructure.

Chief Constable Gavin Stephens: No, sorry. We play our role now in the protection of critical national infrastructure, alongside other partners. I am sorry. I misunderstood. It was the point about moving to a sort of Home Guard arrangement where, for example, we might have to be guarding supply chain routes for manufacturers, ammunition and munitions, supply routes for military colleagues getting equipment from the UK across to other nations and so on. We might have a much broader role in a time of international conflict. We are not resourced for that.

Edward Morello: Do the police currently have, if not the resources, then the skill set? Should this be a function of the police going forward, or actually a separate force, as proposed in the SDR?

Chief Constable Gavin Stephens: There are organisations within the policing family. The membership of the National Police Chiefs' Council is broader than the geographic forces in the four nations. It includes our colleagues in civil nuclear, for example, and Ministry of Defence Police. If I was asked for advice on this, my advice would be that we develop the

conversations with those organisations where those capabilities might best fit, but that is not part of how it is now.

- Q42 **Lord Watts:** Following that, Chief Constable, you say that, if you had to scale up the operations to protect vulnerable assets, you would not have the resources at the moment. I would take it you would go to the Army as the first port of call for support if that was the case. Is there a practice between you and the Armed Forces about how that would happen?

Chief Constable Gavin Stephens: Yes, but I am making the assumption in this question that we would be in a time of conflict and our colleagues in military services would have other responsibilities. If it was not the case, there are well-worked protocols for how we get military assistance to the civil power. What is becoming more common now is how we get civil assistance to the military power. It is those sorts of plans that we are doing some contingency work on at the moment.

Lord Watts: If it is not the Army, who would it be?

Chief Constable Gavin Stephens: It would fall to prioritisation of uniformed civilian services. We would drop some of our other responsibilities, as we did during the pandemic, for example.

- Q43 **Lord Robathan:** Chief Constable, I would like to drill down on this a little. I am not trying to get at you, because I understand you do indeed have a shortage of resources. I blame the last Government as well as this one, so let us not make it partisan. Is a landing station like an electricity substation?

Chief Constable Gavin Stephens: That question is outwith my knowledge, so perhaps I can hand over to my colleague.

Alex Towers: It is like a very large phone exchange, basically. It is a building with lots of cables and servers.

Lord Robathan: Is it surrounded by barbed wire?

Alex Towers: Yes, it is surrounded by security fencing.

Lord Robathan: I am not trying to put anybody on the spot but, apart from CCTV, it is quite easy to break into.

Alex Towers: It depends what kind of scenario we are talking about.

Lord Robathan: We are talking about tomorrow.

Alex Towers: If you had a large number of people, it would be a crude thing to do to break in and probably try to set fire to one of those buildings.

Lord Robathan: One could do that, because there is nobody there.

Alex Towers: Some of them will have some people and some do not. We have CCTV. We have all manner of protections. If you were suitably determined—

Lord Robathan: I am not trying to blame you. I am just saying that, if you wanted to break into it, you could.

Alex Towers: Yes. We would be trying very hard to stop you, but, if you were really determined, there are probably ways of doing that, yes.

Lord Robathan: It is CCTV, not people.

Alex Towers: Some of them have people and some have CCTV.

Q44 **Lord Tunncliffe:** Could I go back to the financial problems? Assuming a catastrophic failure—you presumed it would not be that, but I am not entirely sure—of communications with North America that took a number of days and weeks to mend, what scenario would be followed? Would there be an automatic catastrophic failure in the financial systems in the UK, or could we survive with Ireland and GB?

Laura Catterick: It would depend on the scenario. There are domestic banks and the cash system is domestic, so there are some aspects of the financial system that would continue to operate. However, anything international would be impacted. Depending on the scenario, we would have to work with the other global financial centres to understand and consolidate our position. We have a sector response framework, where we work with the Bank of England and the other authorities, where we would have a co-ordinated incident response plan.

Q45 **Lord Hutton of Furness:** This is a question for you, Laura, from what you were saying earlier, but you made the point again just now. Am I right in saying, listening to what you said to us today, that you have not actually modelled, in the financial sector, the risk of a total loss of transatlantic telecoms? You have looked at other scenarios but not actually thought through what a total loss of those telecommunication links across the Atlantic might mean for the financial sector. Is that true?

Laura Catterick: Not to my knowledge have we done something so catastrophic, but we have modelled aspects of it.

Lord Hutton of Furness: Is the whole basis of contingency planning not that you work on the worst-case scenario first?

Laura Catterick: Absolutely, but we also have a range of risks that we have to assess and mitigate. Based on that, we look at the likelihood of a risk occurring and focus on those.

Q46 **The Chair:** May I thank the panel? We have slightly overrun, but you will have detected that that arises from the profound interest this committee has. Thank you very much for your evidence today. If you feel that there is anything we missed—I suspect you do not—or anything you wanted to clarify, please submit written evidence after the session and we will incorporate that into our report and share it as we would testimony here.

Chief Constable Gavin Stephens: In preparation for the committee, there was one question I asked my team that I was not able to get an answer to. That was, if such scenario occurred and there was a concerted

attack on the cable network, whether that would increase the risk for cyberattack by a determined actor or reduce it. I have not been able to establish an answer to that question. It would be important for our broader contingency planning. If that is something the committee is going to look at, certainly policing would find that response useful.

The Chair: I suspect that we are now, even if we were not before. Chief Constable, thank you. May I thank the panel? We are going to adjourn briefly. We have another panel to join us in a moment or two.