HOUSE OF LORDS

Select Committee on International Relations

Corrected oral evidence: UK foreign policy in changed world conditions

Wednesday 14 March 2018

10.40 am

Watch the meeting

Members present: Lord Howell of Guildford (The Chairman); Lord Balfe; Baroness Coussins; Lord Grocott; Lord Hannay of Chiswick; Baroness Helic; Baroness Hilton of Eggardon; Lord Jopling; Lord Purvis of Tweed; Lord Reid of Cardowan; Baroness Smith of Newnham; Lord Wood of Anfield.

Evidence Session No. 8 Heard in Public Questions 65 – 76

Witnesses

I: Ms Merle Maigre, former Director, North Atlantic Treaty Organisation Cooperative Cyber Defence Centre of Excellence, and former Senior Policy Adviser to the President of Estonia (via video link).

II: Mr Peter Wells, Head of Policy, Open Data Institute; Dr Becky Faith, Research Fellow, Institute for Development Studies; Ms Nima Elmi, Head of Policy Initiatives, World Economic Forum.

USE OF THE TRANSCRIPT

1. This is a corrected transcript of evidence taken in public and webcast on www.parliamentlive.tv.

Examination of witness

Ms Merle Maigre (via video link).

Q65 **The Chairman:** Good morning, Merle Maigre. Thank you very much indeed for joining us. This is the House of Lords International Relations Committee. We are engaged in a major inquiry into the enormous impact of the digital era and all its aspects on international relations, particularly, obviously, as we are a UK Committee, sitting here in London, in Westminster, on the United Kingdom's foreign policy dispositions and the need for change.

We will ask you some questions this morning in that context and focus in particular on your expertise as director of the NATO Cooperative Cyber Defence Centre of Excellence. I will start with the first, perhaps general-sounding, question, just so you can set the picture.

To what extent do you think that the digital technologies and the vast changes in technology that are now proceeding, as fast as ever, have altered the interstate pattern of relations and the balance of power between states? We will come to our own UK position later, but what is your broad assessment of that? Is it massive or is it not yet fully developed?

Ms Merle Maigre: Good afternoon. I am happy to share my views and contribute to your understanding of cybersecurity.

On the one hand, with the spread of broadband internet access, where every second person on earth is online, states have become more vulnerable to the malicious-minded use of the internet, either by government-owned clandestine services, which are popularly known as advanced persistent threats, or by criminal syndicates or individuals who possess the necessary skills, computing power and political intent. The threats of these many players are manifold, from spreading computer viruses to stealing personal data to hampering national critical infrastructure or meddling with elections.

On the other hand, the picture is not that gloomy, and I would not like to describe the doom and gloom only. We see that nations have been quick to adapt to the new threats and are taking steps to enhance their posture in cyberspace. Of course, states are various. Allies are at various levels of preparation. There are some so-called first-generation countries coming up with very initial cyber strategies, for example, that outline only in general terms what cybersecurity is and how they plan to achieve it. There are much more advanced countries that are spreading out and drafting several iterations of their cyber strategies that are much more specific, not only about the risks and dangers but about the opportunities. Clearly, the UK is in the latter group.

To sum up, we can say that the balance of power in international relations remains unchanged in principle, but the balance has shifted significantly in relation to the distance. Distant objects can now be

targeted with cyberattacks within seconds. Geographically, the space matters much less.

The Chairman: Thank you very much for that opening comment. We will come back to the precise cyber aspects in a second, but is your view that, now that the whole conduct of international relations is so much more widely shared through public participation and public diplomacy, we are dealing with a situation that Governments find less easy to control and which can lead to some greater volatility in the whole scene?

Ms Merle Maigre: Sure. I think we have come to an era, because of the use of digital services, in which the public require more explanation from the government side of what is going on. At the same time, countries are clearly recognising the importance of international co-operation. No one can really do it alone. More generally, developments last year, such as the DNC hack or attacks such as WannaCry and the attribution of WannaCry, or NotPetya and the attribution of NotPetya, are significant moments in deciding how we proceed as states and Governments. At the same time, they receive public attention through the press and media, so people are more attuned to the cyber-related issues.

The Chairman: Thank you. Let us move on to a more specific area. Baroness Hilton would like to ask you a question.

Q66 **Baroness Hilton of Eggardon:** Estonia was subject to a major cyberattack a few years ago, since when you have improved your technology enormously and have concentrated on digital technology. Do you think there are lessons that we and other NATO allies should learn to enhance our defensive systems on this front?

Ms Merle Maigre: Yes, I think so. The attacks 11 years ago against Estonia served as a wake-up call for the country. Above all, they made people realise that attacks in cyberspace can be just as serious as attacks in physical space; that what is happening in cyberspace is closely linked to what is happening in other domains. They also promoted the first public discussion on the possible impact that cyberattacks could have on national security, and made people—and, more importantly, the political leadership—altogether more aware of the importance of international co-operation and the vulnerability of the country in cyberspace.

The lessons that Estonia has learned include the importance of transparency from the government side when interacting with the public in explaining their decisions regarding cybersecurity. In return, the people's trust in the technology has been maintained. Transparency in policy-making has brought the positive impact of people trusting the technological advances. Estonia is a firm believer in security by design. One concrete lesson learned from these attacks was in understanding the clear organisational set-up and responsibilities that stand after these attacks in 2007.

To sum up, in the digital age we often hear that you can have either online freedom or online security. Estonia has come to understand that

you can have both. You can be transparent and have online freedom while maintaining vigorous cybersecurity rules and procedures.

Baroness Hilton of Eggardon: Do you think that our NATO allies have learned the lesson sufficiently?

Ms Merle Maigre: I think NATO is doing pretty well now in advancing in cyber thinking. The fact that Estonia consciously decided not to keep the attack in 2007 as an internal thing but put it out—the Government were very transparent about it, as well as in the international arena—prompted NATO to put its thinking cap on and think about cyber defence-related aspects. Concrete proof of that is that while NATO had declared in principle that cyber was important as early as the 2002 Prague summit, it was not until 2008, a year after the attacks in Estonia, that NATO adopted its first cyber policy.

Since then, NATO has advanced at a good pace. More recently, the pace has picked up even more; I am thinking of the steps NATO has taken since 2014. At the 2014 NATO summit in Wales, the alliance announced that cyber can be part of collective defence. Secondly, the alliance announced that international law applies in cyberspace. In 2016, at the Warsaw summit, NATO declared cyber a separate domain. Since then it has taken concrete steps to fill that promise with content. If you are interested, I can go into detail about that now, or later.

Lord Jopling: I begin by declaring an interest as a member of the British delegation to the NATO Parliamentary Assembly.

You will have heard of the phrase that a convoy can go only at the speed of the slowest ship in the convoy. I have heard evidence in the past, and I think you have referred to it already, of the very considerable difference in preparedness for cyberattacks among the various members of the NATO alliance, and that because there is a big discrepancy between the good ones and the not so good ones this has a significant negative effect on NATO as a whole. How serious do you see that gap, if you recognise it in the way I describe it?

Ms Merle Maigre: Recognising the challenge is the first good, useful step in travelling the road towards bridging that gap. Clearly the efforts of our centre here, the NATO Cooperative Cyber Defence Centre of Excellence, through our work in research, training and exercises, are aimed at bridging that gap. We are there. The worst would be to ignore it, but we are travelling that road.

NATO has addressed this issue with a pledge by NATO Heads of State and Governments in Warsaw to invest more in cyber. Building on that, NATO has worked out a questionnaire and developed metrics to measure member states' building up of resilience in cyberspace, and is regularly working towards individual recommendations to bring countries up to the level.

In addition, things such as exercises are very useful tools for bringing all allies on to the same page. Being on the same page is crucial. When we discuss theoretical situations such as Article 5, under which implementing a decision requires consensus among the members of the North Atlantic Council, it is crucial that NATO allies speak the same language. This applies both to traditional threats, or kinetic operations, and to cyberspace. In order to be able to speak that language, three things are crucial: first, a common understanding of the threat picture and the impact of the threat picture on national security; secondly, situational awareness; and, thirdly, sharing the same values. These apply both in the analogue world and in cyberspace.

We are getting there. Allies are getting there, but developing this more common understanding of the threats in cyberspace requires continuous effort. The UK is a really good leader within NATO in pushing allies forward, and that kind of leadership is really needed.

The Chairman: We will come a little more to the NATO aspect in a moment.

Going back to the attack on Estonia as an example, this was an attack not on military installations but on the civil structure of society—utilities, government operations, private networks and the entire digital structure, which Estonia was trying to develop at the time and has developed more since.

How do we distinguish in future between the military area, which you are rightly concerned with—it is part of the NATO structure—and the fact that a great deal of the damage and danger of this new situation is going to be entirely outside the military area and concerned entirely with civil and daily life, the things which Governments are supposed to protect for their citizens?

Ms Merle Maigre: We cannot make that distinction at all. On the contrary, we need to recognise the importance of civil-military co-operation but also the public-private partnership. That, too, is one of the clear lessons that Estonia learned and has tried to implement ever since.

I see the challenge as how to make sure that in cyber there is interagency co-operation at state and government level, where you bring in both the military side and the civil side and identify the role that the military plays in cyber defence and cybersecurity. This is an issue that a number of countries deal with when drafting the so-called second-generation cyber strategies.

These are some of the issues that Estonia is dealing with when establishing the right lines of co-ordination among different agencies. One thing is clear: when developing resilience against cyber, we need co-operation between public services, private enterprises and academia. We need a community approach, and building a sort of collective brain in cyber is something that Estonia takes pride in as another lesson learned from the 2007 attacks.

The Chairman: While we are on this main theme, Lord Purvis will join in here.

Q67 **Lord Purvis of Tweed:** You mentioned the Wales summit at which cyber was put on a par with the traditional land, sea or air offences. I read that there was a memorandum of understanding in 2015, but it has still not been concluded by the partners. You say that, even with your three criteria, the 29 allies are "getting there" but are not there yet.

Given that there are ongoing attacks on NATO allies, when do you think a view will be able to be taken about collective defence? It seems quite extraordinary, in this fast-moving world, that it will probably be five years after agreement was reached on the parity of cyberattacks before Article 5 can be activated.

Ms Merle Maigre: The decision by NATO to declare cyber as a separate military domain was made in 2016 at the Warsaw summit. Since then, we have had a comprehensive document detailing all the lines of effort and work in moving forward to fill that declaration with content, called the road map to implement cyberspace as a domain of operations.

Work there has been divided into 10 separate lines of effort, and considerable progress has been achieved in a fair number of fields. I can outline them all very quickly. The 10 lines of effort are: first, systems development; secondly, NATO processes; thirdly, NATO organisation; fourthly, command and control; fifthly, rules of engagement; sixthly, interoperability; seventhly, cyber effects provided voluntarily by allies in support of NATO missions and operations; eighthly, NATO doctrine; ninthly, cyber education and training; and, tenthly, strategic communications.

Full readiness in all these 10 areas does not happen overnight. It is natural that it takes time for 29 allies to declare progress, because it is not only about each nation recognising and investing in the necessary measures but about allies coming on to the same page.

That said, considerable progress is currently being achieved in organisation, whereby NATO, during its last Defence Ministers meeting, declared a special entity within its command structure dealing with cyber: the Cyber Security Operations Centre within Allied Command Operations in SHAPE in Mons. For the first time there is a place dedicated to thinking about and planning the role of cyber in NATO operations.

NATO has also achieved progress in doctrine. This centre takes pride in being the custodian of NATO doctrine on cyber operations, and this is being done by a UK expert in our centre. So the investment that Great Britain is making in this centre is bringing great value.

NATO is also progressing in training and in integrating sovereign cyber effects provided voluntarily by allies. Again, with the latter, the UK is at the forefront. I like to see the glass as half full, not half empty.

I did not really answer the question about Article 5. We can get into that if you are interested.

Lord Purvis of Tweed: A NATO publication last month suggested that in 2016 there were 500 cyberattacks a month on NATO. In 2017, that was increasing. The majority are state actors, but a fair proportion are non-state actors. I read that the trend is more on softer targets and individual devices and, if not on NATO as an institution or its member countries, the bodies that are associated with them.

My very basic understanding suggests that attribution would be very hard, as well as to escalate that up into a potential collective defence. But some of these attacks could be crippling, as we see. Does the trend of attacks suggest that it is even harder for the NATO structures to be able to respond?

Ms Merle Maigre: We are making good progress on that, and steps taken by allies, such as the US publishing, back in the middle of February, the indictment text of the Mueller inquiry into attacks against the US election, are proof of progress in that regard.

I would also add the attribution made by a number of countries, including the UK, at the end of December, for the WannaCry attacks to North Korea, as well as attributing NotPetya attacks to Russia more recently. Here it is important to recognise that invoking Article 5 is a serious matter. That is the ultimate response. That assumes that there has been an armed attack against the alliance. But a lot of these attacks currently going on in cyberspace qualify below Article 5.

While establishing when and how NATO is ready to invoke Article 5, it is also important to look at the whole picture of the measures below that to work as a deterrent against cyberattacks.

Let's start by attribution. It is important to establish above all that the attribution of cyber operations under the law of state responsibility is not only a matter of identifying the correct legal standards and implementing them by providing proof from digital forensics experts. But in addition to the technical evidence, attribution can also be based on intelligence, including reliable human intelligence; strategic context, patterns of activities, and the modus operandi of states and their motivations. So it is also a political issue.

Very often, the attacks themselves are conducted by non-state actors. In the course of developing the legal thinking of attribution in cyberspace, it is important that a legal attribution to a state is established so that a line of command is established linking the non-state actors to a state.

Then there is the question of what we can do about it. While, according to the work of our centre's international legal experts, it is more complicated to envision collective countermeasures, allies can undertake countermeasures individually. What are countermeasures? They are acts that, according to international law, would otherwise be unlawful, but

their wrongfulness is precluded because they are targeted against an attack. There are three conditions: the goal has to be to induce a respective state to resume lawful behaviour, the countermeasures have to be proportional to the injury, and they have to be necessary to stop the violation.

As to NATO and the measures that it can undertake below Article 5, this ground is not yet fully covered. We are all thinking about this, and we can think of various measures that are indicated in the North Atlantic Treaty itself, between Article 3, which requires each state to build its own resilience, and Article 4, which allows states to convene consultations among all allies. That covers the ground between Articles 3 and 4. Article 5 deals with collective attack against somebody.

It is important to look at what already exists in NATO's toolbox. We really do not have to invent the wheel here. We can go back to NATO's crisis response system and look at how the Alliance reacted after the attacks on 9/11, when it evoked some of its counterterrorism measures, and think of developing these measures and making them applicable in the case of an attack against an ally in cyberspace.

Baroness Smith of Newnham: Following on from the suggestion that we look back to 9/11, was not one of the problems then that President Bush did not really feel that a NATO response was going to be the right way forward, so he looked to bilateral support from the United Kingdom?

In the current context, do we really expect that, when the American presidency is led by Donald Trump, NATO is more likely to be minded to work on a NATO basis than George Bush was? Is 9/11 therefore really the best model that we can look at?

Ms Merle Maigre: Naturally, we have to keep the political realities in mind. I refer to 9/11 only because this is the only time when Article 5 has been evoked in NATO. I recognise that the political realities are also different, and that above all it begins with an ally being interested in taking the issue to NATO in the first place.

That in itself is not a given. Allies may prefer to think of a response individually, or to build a coalition of the willing, which we are currently seeing in the process of attributions, or to take it to the European Union. NATO is only one of the options, and it is not a given, of course.

If it is taken to NATO, in order to reach a consensus in the North Atlantic Council of the alliance it is important that allies are similarly attuned to the threat picture. Here I refer back to the importance of being able to speak and understand the same language, and of having these basic shared values in cyberspace. I am thinking, first, of a common understanding that international law applies in cyberspace; secondly, that there is basic cyber literacy or situational awareness of where we are with cyber; thirdly, that all allies must be similarly attuned to the threat picture.

Attribution is the step before evoking any articles or countermeasures. Before those are evoked you have to attribute the threat or the attack to some state if NATO as a collective body or any Government are to respond. I would draw a parallel here with the situation that we had with Crimea in late February/early March of 2014. In that regard, European allies as well as NATO allies were taken by surprise by the appearance of so-called little green men—or, if you prefer the Russian approach, the polite people in Crimea—and there was a bit of confusion about who all these military people were who were not wearing any insignia.

It was an interesting case study that bears some parallels with the current situation when we need to attribute cyberattacks. Because it boils down to how much Governments trust their decision-making upon intelligence and how much they share their intelligence with allies, as well as how much allies trust intelligence that comes from partner services. More generally, it is related to how much allies share, if at all, a common threat picture and think that the situation at hand is the new normal, as we have come to think of occupied Crimea today.

Looking back at it, while we were all pretty confident that the military forces occupying Crimea were the Russian special services, back in early March 2014, there was a fair bit of a discussion and a debate about this within EU and NATO

This bears an interesting comparison with the situation that we might have when we want to take cyberattacks to a more collective body, because an ally that takes an attack to the table needs to provide convincing evidence in order to convince the others. It boils down to how much you want to share your intelligence, which very often is sensitive, and how much the others trust it. It also means, as I said, that in addition to the facts, the technical forensic expertise in cyber, you have in attribution the other layers—the operational level and ultimately the strategic level—and ultimately these decisions are political.

Q68 **Lord Jopling:** There are three aspects to my question. Apart from the work that you do leading the NATO Cooperative Cyber Defence Centre of Excellence, could you tell us what else NATO is doing, and tell us, to the extent that you can, about the inadequacies or the limits of that role?

Secondly, you mentioned earlier the exercises in dealing with cyberattacks. Can you tell us a little more about that?

Finally, as you know, there have been serious delays in establishing the new headquarters in Brussels. I think it was 2003 when it was first proposed that people should occupy the new building three years ago, and they are still not in. To what extent are these delays due to concerns over electronic issues or cyber communication and defence problems? One has heard that these issues have been one of the major causes of these delays.

Ms Merle Maigre: Thank you for your questions. I will try to answer them as well as possible.

Where is NATO today in its debate on the role of cyber operations and the changing nature of conflict? NATO, as I said before, has taken cyber defence increasingly seriously in recent years, especially on the back of more active thinking on this since 2014. First, NATO made clear in Wales in 2014 that cyberattacks with a severe impact could trigger a collective defence call. More recently, in Warsaw in 2016, it defined cyberspace as an operational domain: that is, a likely battlefield.

Today, NATO thinking on this, as the NATO Secretary-General explained recently in mid-February at the conclusion of the NATO Defence Ministers meeting, is that when it comes to different national cyber capabilities, they are owned by nations, and nations then volunteer to offer these capabilities to support allied operations and missions. It is a bit like with special operations: each ally owns its own capability in this, but it can be offered in support of an allied mission.

Therefore, NATO is now adapting its command structure to accommodate this. NATO has set up the Cyber Security Operations Centre within Allied Command Operations in SHAPE in Mons in Belgium. That centre, which was set up in mid-February after a decision by NATO Defence Ministers, will start thinking about and planning how to strengthen the cyber elements in NATO's operational planning.

NATO has also made progress with regard to drafting a cyber operations doctrine. The second draft is out, and next week marks a deadline for each NATO ally to comment on it. We are looking at possibly having a NATO cyber operations doctrine ready in a year or so.

NATO has made good progress on training, which leads me to answer your second question about the importance of exercises in cyber. NATO has clearly recognised that. Allies think that cyber exercises are important because effective protection requires preparation, preparation requires knowledge, knowledge needs practice, and practice can best be conducted in a lifelike environment.

Cyber exercises offer that lifelike environment, which is second best to actually being attacked in real life. NATO conducts cyber defence exercises at the strategic level, such as Cyber Coalition, which focuses on advancing the thinking on cyber. Our Centre, CCDCOE, supports various other NATO exercises to make sure that cyber storylines are part of them. In addition, our centre organises exercises at the strategic, operational and tactical level. We are seeing increasing interest in that.

Lastly, as of January this year, our centre has been given the responsibility that lay formerly within NATO Allied Command Transformation—ACT—the NATO military command located in Norfolk, Virginia. ACT outsourced that responsibility to us. It is about identifying the cyber-operations training requirements and co-ordinating cyber-defence operations training solutions for all NATO bodies across the alliance.

That is what this centre does, and I can tell you that there is global shortage of cybersecurity skills in various parts. We are trying to identify the requirements and bring them together with institutions that offer cyber training. At NATO level, these include the NATO Defense College in Rome, the NATO School in Oberammergau and the NATO CIS School in Latina, Italy.

The centre also organises exercises, as I said. We are currently preparing what we consider to be the world's largest and most complex live-fire cyber-defence exercise, called Locked Shields. That takes place in April. We are continuing with a series of high-level table-top exercises, tailored for Ministers. For the first time in history, in September last year as part of Estonia's EU presidency, the Estonian Ministry of Defence organised a table-top cyber-defence exercise for EU Defence Ministers.

We are carrying on with this and we are currently discussing ways of making it happen and making sure that it will not stay as a one-off event but that these types of exercises will take place regularly, and potentially not only for Defence Ministers but for Ministers of Foreign Affairs, Ministers of Finance, and so on.

The Chairman: Does that answer your questions, Lord Jopling?

Lord Jopling: It does not answer the last question, which was about the delay in moving into the new building and the extent to which that has been caused by problems over cybersecurity.

Ms Merle Maigre: This centre being safely located in Tallinn, Estonia, and outside the immediate NATO command structure, does not leave me in an appropriate position to comment on the movement of NATO headquarters. I would not like to share rumours and urban legends. When I was in Brussels last week, I heard that the move is proceeding according to the new, delayed plans and is going well. I apologise, but commenting specifically on the technical requirements of NATO's new headquarters is outside my mandate. I just do not possess that information.

The Chairman: Fair enough. We will move outside NATO with a question from Baroness Coussins.

Q69 **Baroness Coussins:** You have already touched on the role of international law and institutions, but there seems to be some disagreement among commentators on cyberspace, with some arguing that cyber activity is operating in a legal vacuum and others arguing that international law and existing institutions such as the UN, and the rules they are based on, are actually perfectly capable of being applied to the new phenomenon of cyber. Are existing international law and institutions fit for purpose in this context, or should we look at establishing new laws and new bodies?

Ms Merle Maigre: Thank you for your question. This is a very important subject. This centre has published the *Tallinn Manual* and the *Tallinn*

Manual 2.0, which form the most comprehensive guide so far to how international law applies in cyberspace.

We maintain that the existing international law, with all its complexities, does apply to all state activities, be they carried out in the physical realm or in cyberspace. That said, we recognise that international law is always evolving, through state practice as well as the creation of new treaty law. But when it comes to cyberspace it is evident that that the political will that is required to establish new treaty law is very often overwhelmed by political disagreements on the conceptual level. Here I refer to the understanding of cybersecurity principles that are initiated by the like-minded nations of the West vis-à-vis information security, which is a term I would apply more to countries such as Russia and China. I would also refer to disagreements on a practical level. For example, every now and then, countries in the East bring out the issue of whether international humanitarian law applies in cyberspace.

All parties are well aware of this, and we can even say that the eastern bloc, led by Russia and China, is taking great advantage of this situation. Those countries come up with proposals saying that new law is needed in cyberspace, but it takes decades to negotiate new treaties and, in the meantime, they are free to operate in cyberspace as they please, claiming that existing international law, or at least big parts of it, do not apply to cyberspace.

Therefore, there is a great amount of cynicism about these calls for new law, with the implication that the current law is not good. This centre firmly supports spreading the understanding that current international law applies in cyberspace.

What is positive is that we see increasing state practice that addresses issues such as public attribution to nation states of major cyber incidents. I applaud the leadership exercised by the United Kingdom in publicly attributing the WannaCry ransomware attack to North Korea and the NotPetya attack to Russia. These incidents of state practice are accompanied by statements of opinio juris, meaning the legal explanation of what states believe the law is, which will eventually form new customary international law. Those are steps in the right direction.

In conclusion, yes, there are issues in cyberspace that need to be further addressed in detail, but the idea of creating a new international agreement or setting up new supranational institutions is cynical and unrealistic and will not take us in the right direction.

The Chairman: Thank you. We have a final question, about ourselves, sitting here in London.

Q70 **Lord Grocott:** You have been complimentary on a number of occasions about Britain's capacity in and contribution to a number of the subjects that we have been discussing. Could you generalise on that front and say how the UK's cybersecurity capabilities are viewed? I am not exactly asking where we are in the league table, but I would like an overview,

please.

Ms Merle Maigre: The UK is one of the world's leading digital nations, and it is a leader in the field of cybersecurity. That is how I see it from the cyber centre in Estonia. The UK has taken a central role in advancing the cyber agenda, internationally and within NATO. That is useful and important, because at the end of the day someone within the alliance needs to take the lead.

It is very positive that the UK is exercising that leadership role. The National Cyber Security Centre, which opened in London in October last year, is a good example of interagency co-operation and of understanding how that works—national resilience against cyber threats needs to be built across the board and needs to include civil and military co-operation. The National Cyber Security Centre is a good example of that.

The UK's approach to cyber defence includes a wide range of technical, operational and administrative measures, with the aim of ensuring that the UK Armed Forces can project power in cyberspace and assist during a significant cyber incident as well as respond to cyber threats, as to any other kind of attack. This is visible in the UK sharing its best practice in workshops at NATO level, leading discussion on the topic of cyberattacks, with information provided voluntarily by allies in support of allied operations in NATO.

Last but not least, the UK has not shied away from the fact that there are offensive capabilities and has acknowledged possessing them. It has taken that conversation into NATO. That is important, because it makes the alliance much more aware of the realities. In order to defend ourselves, we need to understand how the attack works. Speaking about it is the first step. It is great that the UK is taking a lead in these conversations in NATO.

The Chairman: That is a nice, positive note on which to end this interesting discussion. Obviously, we have touched on only part of your immensely complex and important work. We live in an age where everything happens in nanoseconds, so we have to adjust our institutions to respond in nanoseconds. That is clearly a challenge for you, too. Ms Maigre, thank you very much indeed for your time and your patience in answering our questions. You have helped us a great deal in our inquiries and we are most grateful to you. Thank you.

Ms Merle Maigre: Thank you for reaching out. It has been a pleasure.

Examination of witnesses

Mr Peter Wells, Dr Becky Faith and Ms Nima Elmi.

Q71 **The Chairman:** Good morning, Mr Wells, Dr Faith and Ms Elmi. Ms Elmi, I understand that you have just come from Geneva this morning. I hope

you have got over any travel lag and we are very grateful you are here. I begin by formally stating that this session is on the record. A full transcript will be available afterwards, which you may alter or approve. As a formality, I remind my own colleagues that we have to state any interests we have in opening our lines of questioning. The Committee is conducting a fairly wide-ranging examination of the enormous changes which the digital world is imposing on international relations, in particular how we in the UK respond in terms of resources, equipment, general posture and structure to meet these new conditions.

Let us begin by looking at the great canvas of the world and seeing how digital technologies have impacted on the internal politics and attitudes to democracy of the major and developing economies. We have seen a huge power shift to the east. We have seen the vast growth of activity, wealth and economic strength in Asia. We have seen democracy of various kinds come under a great deal of attack. How do you see this relationship between technology and politics evolving? That is a big question but we are looking for opening statements. Mr Wells, please will you begin?

Mr Peter Wells: I will introduce the Open Data Institute, in case people do not know. We are a young organisation, five years old. Our global headquarters are in London. We are not for profit. We work with communities, businesses and Governments around the world, and our vision is for people, organisations and communities to make better decisions with data while protecting against harmful impacts.

The question of technology and politics is very complex. We are quite early on in the information age and the revolution we are going through. It is hard to predict what could happen next and what is happening now. We can see huge negatives around the world in some contexts. We can also see huge positives. A lot of our work is about trying to accentuate those positives and to get to a more positive future—the better world that technology can help create. That challenge will be very different in different contexts. So we find that our work in Europe is very different from our work in Africa or Latin America. The rates of change and of technology adoption in those countries are very different.

The Chairman: Dr Faith, what is your general take on my rather general question?

Dr Becky Faith: The Institute of Development Studies is the UK's leading global institution for development policy and research. We are based at the University of Sussex. I co-lead the digital technology and research group, which looks at precisely these questions. We think that the issue of how we use technology in international development is fundamentally important and should be at the centre of all our discussions. As Peter said, the outcomes of technology use can be negative as well as positive.

The Institute of Development Studies—the IDS—led the research component of major governance programme, Making All Voices Count, which lasted four and a half years and was funded by DFID, USAID, Sida

and the Omidyar Network. It looked at the use of technology supporting for citizen voice and accountable, responsive government in 12 countries in Africa and Asia.

The overarching finding, in a simple sentence, was that problems of democracy cannot be fixed by technology. To quote from the final report, "unaccountable and unresponsive governance problems are deeper, more complex and more intractable than information asymmetry". Information asymmetries are typically the kinds of problems that technology can address. Systemic weaknesses such as corruption, malpractice and power issues cannot be fixed by technology. That is the top-level finding in relation to democracy.

When it comes to technology's role in addressing issues of weak democracy, we know that there are enormous asymmetries in ownership of and access to technologies; in particular, strong gender asymmetries. There is a huge gender gap in technology use and access. Women in low and middle-income countries are 10% less likely to own a mobile phone than men are. If you think about the role of technology in voice and accountability and democracy, women are de facto less represented simply because of those asymmetries in ownership.

The Chairman: Ms Elmi, we have before us the paper by the founder of the World Economic Forum, Dr Klaus Schwab, who argues in very positive terms that we can call in aid the new technologies in a vastly positive way to transform economies. Indeed, that seems to be happening and has happened already. What is your general take on how strong you think the technological drive is in raising living standards, in making poor countries less poor, and in changing the pattern of world power?

Ms Nima Elmi: Thank you for having me. This is an important discussion and a timely inquiry. As you have just said, the forum conceptionalised the fourth industrial revolution almost three years ago now. It is really a call to action, because we feel that emerging technologies are very different in the way that they shape our societies. They make us much more interconnected, integrated and interdependent.

Because of this, and the pace of change of these technologies, they have immense power in bringing developing economies out of their into a faster state of growth, but at the same time there is a lot of discussion about the potential digital divide. At the forum, we see the positive elements of advanced technologies as being the determinative factor for us to engage in multi-stakeholder collaboration, to showcase how we shape the fourth industrial revolution, looking particularly at those opportunities where we can harness fourth industrial revolution technologies to provide opportunities to leapfrog the second and third industrial revolutions.

We are seeing a lot of this—I am sure we will come to it—in sub-Saharan Africa, with mobile money technology giving access to millions who would otherwise be unbanked and would not have access to financial services. We see this in the solar space, with renewable energy circumventing the

need for on-grid infrastructure. We also see this in relation to drone technology, which is being used to circumvent or bypass the need, where there is a lack of infrastructure, to deliver blood or medicines to rural parts of developing economies.

So we see a number of positives, but we are also very mindful of some of the negatives. What we really try to define within this broader discussion are three overarching challenges. First, fundamentally, how should we as a society distribute the benefits of technology fairly across the world? Secondly, how should we minimise any potential negative externalities? I am sure you have heard a lot about the potential misuse or unintended consequences of technologies. Thirdly, and finally, how do we ensure that emerging technologies empower humans and do not replace human beings and create social upheaval and disruption?

The Chairman: I think you have all answered this, but I will put it more bluntly: is this a revolution that brings more power to the powerful or more power to the powerless?

Mr Peter Wells: I think that is still to be seen. We are still in the middle of the revolution, so we can still shape its outcomes.

Going back to Becky's point about information asymmetries, I come from what we call the open movement. We are trying to level out those asymmetries. We are trying to broaden the conversations and bring more stakeholders into them by giving information, capacity and skills to more people. We are still in the middle of that revolution and we can still shape its outcome.

Dr Becky Faith: You cannot substitute technology for a lack of political will and capacity. That is one of the findings from our research.

The Chairman: Yes, but political will itself is shaped by the participation now of millions—billions—of people. The public shaping of will is much more powerful than it was in the past. Is that not the problem?

Dr Becky Faith: That is the case, but if we think about the shaping of political will as something that now happens both offline and online, we are increasingly seeing a worrying trend towards internet shutdowns—when internet services just cut off at times of political crisis. According to the organisation Access Now, there were 55 of these shutdowns in 2016 and 61 between quarter 1 and quarter 3 of 2017, so that is a significant rise.

This is in breach of Human Rights Council resolutions. The previous speaker talked about whether our existing international legal frameworks are fit for purpose. The UN Human Rights Council has called for "the promotion, protection and enjoyment of human rights on the internet". If we are seeing an increasing use of these politically determined internet shutdowns, that is a cause for concern—for freedom of expression and a lively political public sphere—but it also has a big financial cost. According to the Brookings Institute, this cost $2.4 billion in 2016. It also has

financial and reputational concerns for the businesses involved. If you are a mobile operator in a country which is then shut down by the Government, that does not look good for your global reputation.

Lord Grocott: There is so much in that. You have been saying what we perhaps should have realised from the start: that it can be negative or positive, really. It is a tool that can be used well or badly. I was enormously reassured, Dr Faith, by you telling us that the problems of democracy cannot be solved by technology. As a lifelong politician, I am glad that it will be a while before I am replaced by a robot.

I have two questions. The first is about the effect of these technologies on the machinery of democracy—on elections, to put it simply. Certainly in this country—obviously I know a lot more about this country than anywhere else—for the past four general elections at least people have been saying that the days of old electoral practices have gone. We are now into new digital elections, with forensic focus on individual voters through the various mechanisms that are now available. Is it too general a question to ask what the impact is of all these new developments on the machinery of democracy?

The Chairman: Who would like to start on that? You are all looking at each other. Nina Elmi, you tell us, because it came up at Davos this year.

Ms Nima Elmi: Again, that is a very good question. Fundamentally, as Peter said, we are on the cusp of the fourth industrial revolution, and shaping it is something that is unfolding for us.

On the positive side, we are finding that because technology is endearing to the younger generation, platforms such as social media are making young people more politically active. They are much more engaged and have much more interest in politics. We have seen an increase in digital diplomacy. There are many more politicians using online platforms such as Twitter, some more famous than others. That is a gateway of access to information for a demographic that might not have been as active in previous years. It is something that teenagers and the younger population would have grown into rather than already been aware of.

The other thing that we are seeing, which is another positive, is that this is empowering many more citizens of developing economies, who otherwise would not necessarily know where to go to access this information. We are seeing many more constitutions of developing economies being available as apps to download. This is empowering citizens in a number of countries to understand what their rights are.

We are also seeing applications whereby there is a little more accountability on the part of representatives. With the eID system in Nigeria to Pledge 51, we are seeing citizens getting greater access to what their representatives are doing with their time—tracking their participation in committees, their attendance in their parliaments, what legislation they are voting on and how they are voting.

So we see that there are a number of positive influences that the fourth industrial revolution technologies are providing. I will save the negatives for later in the conversation.

Q72 **Lord Grocott:** I can give you some negatives as we go on.

My second question takes us from the micro to the macro. We have had evidence, both written and oral, from people who in one way or another are saying that the state is changing and maybe diminishing in its significance because of globalisation and new technologies and the extent to which the power of traditional state structures is diminished by those new technologies. Would you like to give us some observations on that? Some people have been very extensive in their statements, almost looking to the decline of the state. That is not obvious to all of us. Do you have anything to say on that?

Dr Becky Faith: Just this week, Tim Berners-Lee, who invented the internet, warned of the concentration of power in companies such as Facebook and that a handful of platforms that control which ideas and opinions are seen and shown, and the algorithms that underpin what you see on newsfeed, are unaccountable and unknown to the general public.

If we look at that as a development issue and within the framework of the sustainable development goals and the achievement of equality and freedom of expression, the UN's Fact Finding Mission on Myanmar warned just yesterday that Facebook has "turned into a beast there"— Facebook has become a mechanism by which hate speech is being spread about Rohingya Muslims, and we see that in other contexts around the world. Then we come back to the issue of what the government in Myanmar is doing.

What are the mechanisms of accountability? I do not think it means that there is no longer a role for the state, but the state needs to evolve in these changing times—I suppose that is what the inquiry is about—and new insights and new capacities need to be built to understand these shifts of power. I do not see the disappearance of the state, actually.

There will be countries where it is really important that you have institutions such as the Open Data Institute—countries that do not have the legal framework and the capacities in their Governments to deal with these new issues: the new floods of data, the new capacities of their populations. Actually, I do not think that is an argument for rolling back the state; I think that is an argument for building capacity and a strong civil society.

Mr Peter Wells: The role of the state and the levers that it can use have changed. It still performs a vital role, but the levers that it can use to achieve its goals are new, and I think we are still working out what those levers are and whether they will shape and influence these new global institutions or give that capacity to citizens who are already connected to people in another country and who might feel part of a community of, say, YouTube gamers; citizens who feel part of other communities as well as their national community and their local institutions.

The question is how we evolve to adapt and understand who in that world shapes society and how we make sure that everyone in society benefits and that the state is carrying out its role to spread things equitably and fairly. Those are some of the questions that we are all looking at.

Q73 **Baroness Coussins:** My question follows on from what one or two of you have touched on.

One of the statements made by our earlier witness—I think you heard her—was that every second person on the planet is active online. Another way of putting that is that half the world's population has no access to the internet. So there is the question of access to it as well as the responsible and positive use of it once you have it.

To pick up on what you just said, Mr Wells, if states are going to measure and assess public opinion by what they see going on online, what about half the world's population, and what do any of your institutions think about that?

Mr Peter Wells: We draw a distinction in the language that we use. We talk about organisations that become data driven and that think, "We've got the data. We can get hold of it. We can make decisions from that data", and think that they can eventually build robots to replace people in their jobs. We say that is daft. It does not work. Data is always imperfect. There will be always be gaps, whether it is the people who are offline, who might be offline might choice or because there is no access or because of the cost, or for a variety of reasons.

So we talk about being informed by data, about recognising the imperfections, the confluence levels and the quality, and about realising that we need a range of channels to understand and engage with communities. That might mean gathering sensible data from social media. It is also about going out and talking to people, whether it is a politician on a doorstep or a local town hall meeting. All those routes need to be open.

Baroness Smith of Newnham: I will draw on both Lord Grocott's and Baroness Coussins' questions and go a little deeper into the answer that you just gave, Mr Wells.

To what extent do you think there is a move away from individual citizens? Dr Faith just made the point about the algorithms behind what Facebook throws at us that are unknown to ordinary citizens. One of the things that we saw during the EU referendum was the algorithms that were used to ensure that the huge numbers of messages coming into our Twittersphere, and so on. Political parties do the same thing—they use Mosaic or other things, and Barack Obama's campaign did the same—to try to work out who to target.

In 2015, the Conservatives, as I understand it, had a 40:40 target for holding the 40 most marginal seats and winning 40, which would get them a majority. That means that you are leaving swathes of the country ignored, not just the 50% who may not be online. Is technology

potentially leading to some citizens being more important to policymakers than others?

Mr Peter Wells: There is a famous science fiction short story by Isaac Asimov—I think it is called "Franchise"—in which a computer would decide, "This year, this is the representative citizen, the most typical citizen". It would pick that person and the state would say who should be in charge, or, "You're in charge, and you're making all the decisions". It is a dystopian vision, in my view. So, yes, we are fragmenting, and there is a risk that we are sending very targeted messages to individuals.

A strong part of the counterbalance to that, though, is transparency in advertising, whether political parties' or other people's, so that we can see what is being said to people, and an informed media in civil society that can challenge and inform people about those messages and about other things.

We are still in a period when people adapt. Those of us who are on Twitter and Facebook have seen those things come into our timeline and read the stories about what that means. Our behaviour will now change. It is that wonderful human thing of, "We will change, but we're not quite sure how"—and no other people spending all that money on political advertising.

Dr Becky Faith: We are looking at this in a global context. We are sitting on robust political institutions in this country, and these issues make it even more important to build the capacity of Governments around the world and to build strong, accountable governance and to support civil society that represents the voices of the most marginalised around the world to ensure that those voices are not drowned out. Again, that is a political rather than a technological issue.

Ms Nima Elmi: Going back to your point, Lady Coussins, about half of the world not being online, an important aspect that we do not consider much is how development policies can assist.

We are finding in a lot of emerging economies that the large technology companies are the ones funding wi-fi access and community networks because they want to expand their consumer base, which brings about certain kinds of advertising and algorithms that are perhaps not as well understood by the local jurisdictions.

This could be an area where forward-leaning and advanced economies can ensure that they incorporate and implement internet access, which the UN said in 2016 was a basic human right, in their development polices, to ensure that that 50% who are offline have the ability to get online. We are finding in a lot of emerging economies that actually the number of people with mobile phones is incredibly large—I think over 80% now.

So there is potential there to make sure that more people's voices are heard, but the way it is being done at the moment could perhaps be improved upon.

Q74 **Lord Purvis of Tweed:** Should technology increasingly be seen not just as a tool of delivering development aims? A lot of the discussion has been about technology being the method through which development can be achieved. Is sufficient thought being given to how technology will shift the development needs?

In previous industrial revolutions we have seen development being skewed quite considerably—within the least developed countries, the third industrial revolution has allowed large corporations and elites to completely dominate and has made it very hard for those excluded to participate in the economy and for there to be equal education and healthcare. What is markedly different about this?

You say you want to be an optimist, but we have been hearing that there are trends with very strong ingredients that are leading to a huge amount of inequality and complete dominance by western technology companies, which can massively outweigh these developing countries, especially when, as Dr Faith said, they are still on the path to having stronger institutions, the rule of law and a regulatory environment that can combat that. I am instinctively an optimist, but I just wanted to put that challenge to you: what is markedly different from the previous times, when you could see different development opportunities?

Ms Nima Elmi: I will give some quick reflections. It is important to highlight the pace of change but also a couple of misconceptions. First, emerging technologies themselves are not values-neutral. We are very clear in advocating that technologies have political and social values embedded in them depending on what part of the world they are developed in and which users they are disseminated to. So it is important to understand that if these technologies themselves have, not necessarily a political agenda from the left or right, but certain social values embedded in how they are developed and used, it is down to us to understand and develop a shared common standard that ensures that any development policies or other uses of these technologies are for the common good.

The other important thing to flag is that this revolution provides us with much more access to information that is relevant, digestible and real-time, or near real-time. We have a great opportunity to understand the needs of the recipient states that development policies could be aiding. It is a twofold position. First, we have a lot more insight so that we can address these challenges and utilise local solutions for those domestic challenges. At the same time, we can also help to shape in a positive way, understanding that these technologies that we are developing and using in certain ways have certain social values.

I guess in some ways it is an evolution of the political or democratic ideology behind development policies of years gone by. Now we are

seeing that the penetration and use of technology in emerging economies is shaping how they view their societies but also the rest of the world.

Lord Purvis of Tweed: What are the institutions on which those decisions will be based? For example, we know that e-commerce in particular has the best opportunity for allowing women to participate, even acknowledging the lack of access that many have. Equally, we hear Jack Ma from Alibaba at Davos and at the WTO calling for massive deregulation, arguing that the international rules system should not apply to e-commerce to allow much more fluidity within it. Those positions do not match.

How do we get the governance level and that kind of values-added component in the face of the trend we see at the moment, which is saying that there should not be political or government elements because they would be stifling? What is your guidance for how we try to navigate this?

Dr Becky Faith: I would argue strongly that as well as representation from a company such as Alibaba you need representation and advocacy by government and civil society to ensure that everybody can take advantage of these opportunities. For example, we know that the gender discrimination in women's ownership and use of technologies and access to mobile technologies does not extend just to their ownership and use but to their experiences of being online. Women experience gender-based violence online, which means that not only are they unable to express their political opinions, they are less likely to be on the platforms that might enable them to take advantage of these economic opportunities.

I do not think that at the moment the companies themselves are showing the political will or the capacity to seriously address these issues. You need civil society and regulatory involvement. We cannot leave it up to the companies to ensure that the economic benefits of digital technologies are available to everybody.

Mr Peter Wells: Standards for a lot of these technologies are being developed by organisations such as the IETF—the Internet Engineering Task Force—and the World Wide Web Consortium set up by Tim Berners-Lee. There are other infrastructure elements. We think of data as a form of infrastructure, so we say that we are trying to make data really boring, like roads: it is there when we need it, it is safe to use and we know the rules of the road.

So we take those things down to infrastructural elements, and then it is about building capacity within different regions and countries to build services by creating local jobs that are suited to their social context and needs, and then creating that capability there. That infrastructural capability needs to be as open as possible. It needs to be standards-based so that we can leverage some of the commoditised components, but then we need to build the capacity.

I have something in the back of my head that I was trying to remember. In the early stage of this revolution—the 1970s, 1980s and 1990s—when computers were first coming online and the first wave of data protection legislation came through, that happened mostly through the OECD and in high-income countries. Lots of low and middle-income countries have either very weak or non-existent data protection legislation. There was a great report from the World Wide Web Foundation last year on this topic. There is a certainly a risk for low to middle-income countries.

There is an opportunity to leapfrog ahead to some forward-looking legislation, which is probably further ahead than the European Union's general data protection regulation, that learns from some of the mistakes there. That would be a bulwark to provide the capability for organisations and services to grow and then be exported back to Silicon Valley or Shenzhen in China. Those are the two forces coming towards them at the moment and that legislation will be required to provide protection and enforcement.

Ms Nima Elmi: The forum sees this governance challenge. One of our efforts to contribute to this in a positive way has been to establish a global network of fourth industrial revolution centres that bring together multi-stakeholder collaboration to co-design and pilot governance protocols for some of the more advanced technologies. We are looking at nine areas. The idea is that business has its motivations, Governments have their motivations; civil society has a role, as does academia.

We can get to a near-optimal outcome only if we have this as a shared conversation that is a multi-stakeholder collaboration: bringing together these communities, not only in dialogue but in becoming a "do tank", and these different actors from different parts of the world in several locations to sit down and see how we should govern these technologies—what are the parameters for the way they are used?—and then use our relationships with international organisations to scale them. For example, we are doing a project in Rwanda looking at the commercial use of drones, and making sure that the Rwandans have regulations that make sense for them but also for the international community.

The commercial use of drones brings about another question for civil aviation—how close drones fly to airplanes—which could be dangerous in the future. All these technologies have potential benefits, but at the same time they come with risks. So for us this is one way of trying to help that conversation.

We are also seeing that in the private sector, following pressure from civil society and Governments, a lot of these large technology companies are actually coming together themselves. You will probably have heard about the Partnership on AI, which was launched by Google, IBM, Facebook and a number of large US-based technology companies, which are coming together to try to understand what the regulations should be, understanding that they have a much deeper level of knowledge and understanding of these technologies than a number of policymakers and members of civil society, who in many cases are trying to catch up as the

changes happen. So we are finding these pockets of collaboration, both driven by the private sector and in the more international platform space.

The Chairman: There is a question behind that fascinating comment that I would like to pursue. In democracies, there is great concern that the giant algorithms, the giant electronic companies—you have just mentioned Google, IBM and so on—are creating political and development power beyond the reach of nations and Governments. In the non-democracies they may take a different view: these things can be controlled. Do you see a dichotomy here: a problem that can be clarified and addressed in any way?

Ms Nima Elmi: That is a very interesting question. I think there are several layers to that. We are trying to get to grips by making sure that we can help to shape governance protocols that are as relevant to advanced economies, where you do have these large companies innovating and developing technologies that are predominantly market-driven, as to emerging economies that could benefit greatly from some of these innovations but perhaps do not understand some of the risks.

There is a big discussion—perhaps Peter knows more about this than I do—about data being the new gold and these companies already being able to extrapolate a large amount of information about citizens in foreign countries, potentially making them more powerful than the Governments of those countries, because they have much more insight about those people. So we definitely see that we are at a fork in a road.

There are definitely several layers to tease out. The forum is trying to provide that multi-stakeholder collaboration as a way of making sure that the private sector is just as invested in positive outcomes for the governance of these technologies, and the way they are developed and scaled, in the same way as Governments and civil society are focused on social benefits.

Q75 **The Chairman:** Finally on this development issue, I will mention what some people regard as the central word in the whole story: education. Can technology really transform the entire pattern of education across the planet and create secondary schools where there are none, penetrate primary schools to give better education, maximise distance learning so that every child on the planet is connected, and create universities on a scale right across the planet, giving every young person the opportunity for further education? Can that be done, or is this all still pie in the sky?

Mr Peter Wells: I am not an education expert. Again, it is not the technology that will do it, it is the institutions and whether we build the right methods and tools to help children get the education they need. We can certainly see in developed countries right now that the overflow of information is showing up a gap in our critical thinking because we have accepted all sorts of stuff that has been thrown at us. That has highlighted a gap in our current educational thinking.

But there are always positives. I remember a friend of mine telling me about her two daughters at Christmas who created a document that they would work on together, on different tablets in different parts of the house, and wrote a story together, sharing bits and pieces of the story. That could have been two children on different sides of the world. I think that is really lovely.

What might happen if that emerges I do not know, but it sounds as though there could be some very positive things to connect humans together.

Dr Becky Faith: At the Institute of Development Studies we produced an evidence review on the impact of digital technology on service delivery in health and education. We found that the evidence is patchy on the state of the use of digital technologies for education in developing countries. There have been lots of pilots, but lots of projects have failed because they just replicate funding models from wealthier countries and there are no models for sustainability or support mechanisms in place for the human infrastructure required, for training up teachers and so on.

I think there are amazing opportunities there. I did my PhD at the Open University, so I have to be an advocate for these technologies, but you need to look at what the World Bank called the 'analogue complements'—infrastructure, regulatory mechanisms, training and so on—in the *World Development Report* in 2016, in which it outlined this idea.

Q76 **Baroness Coussins:** Focusing specifically on the UK, can you say to what extent, if at all, you think the UK has already proactively taken on board the increasingly digital world and begun to adapt international policies, specifically development policies, accordingly? If you think there has been movement there, can you give us one or two specific examples, and say, if it is possible to say yet, how effective those adaptive policies have been?

Dr Becky Faith: I will focus directly on DfID and its recently launched *Doing Development in a Digital World* strategy. We thought there was a lot to like in that, actually. We really welcome its vision and ambition and its focus on leaving no one behind in the digital world, its focus on gender inequalities, the messages that we found in it about the new risks of harmful concentration—just the kinds of issues that we have been discussing. It is important not to exaggerate the possibilities of digital technologies to transform developments. Again, there is a need to focus on offline interventions, as we keep saying.

In terms of good practice, we produced a report on Ten Frontier Technologies for Development for DfID in November 2016, and the report has been really well received. It looks at exactly the kind of fourth industrial revolution technologies that we have been discussing, such as drones and new batteries for small scale-solar. From this, DfID launched a Frontier Tech Livestreaming programme, which provides pots of money to fuel innovations in these frontier technologies. There are small, adaptive, responsive projects like that with a research learning partner,

as in this programme, which is very encouraging. I see some very encouraging signs from DfID's digital strategies.

Mr Peter Wells: I declare an interest in that we have done work with DfID and the Foreign and Commonwealth Office.

Both DfID and the FCO seem to have seen the possibilities. They have gone past the stage of seeing digital and data as a way of measuring outcomes and reporting things to seeing how they can use it to shape and create outcomes—in line with the UK Government's policy, obviously. I do not think they have quite got to the point that Lord Purvis talked about: how it can change the needs of Donor and recipient countries. There is a bit of that in there, but it still needs to come through a bit more to get to that stage.

The DfID strategy talks about the need to help recipient countries to build data infrastructure, just as previously it might have helped to build road or transport infrastructure. It is now seeing the need to build data infrastructure. We are seeing the UK Government building standards. There is now an open contracting standard to describe public sector contract opportunities, which the UK Government helped to sponsor. A global civil society group developed that, but the UK Government have been adopting it, exporting it and saying, "This is the way to create common ways for organisations to trade back and forth across trade paths". There seems to be some very well-positioned stuff there.

In terms of the UK Government's digital government work, there is the Digital group of five nations all collaborating in similar ways to bring digital and modern technologies and thinking into government and public services.

The Chairman: Ms Elmi, what about the UK in all this?

Ms Nima Elmi: A lot of our analysis is much more global and regional in scope. One of the forum's key publications is the Global Competitiveness Report, which is an index that looks at how a country is doing across the globe at several levels of industry and governance. The UK ranked eighth in the last global competitiveness index. Within that, it performed very well on technology readiness and the sophistication of its business sector—at 4 and 7 respectively.

I came across an interesting publication that is not published by the forum but by a combination of Portland Communications and the University of Southern California. It is called the Soft Power 30 index, and is considered to be the world's most comprehensive comparative assessment of soft power. It lists the UK as number two. One of the key elements that it looks at is digital, and the UK is ranked very strongly in digital diplomacy.

Finally, it is very encouraging to see that the UK has been very forward-leaning in relation to certain foundational fourth industrial revolution technologies such as AI, and the UK Government recently announced that

an AI ethics commission will be launched that will look at some of the important questions about the use of artificial intelligence, how it is evolving and how it should be governed. These are very positive steps forward, from our perspective.

The Chairman: That is encouraging. Most of us have been led to believe over the years that the United Kingdom must stick close to our American allies and that the western world must stick close together and support the democracies—until recently, we were told that our destiny was in Europe, but now it looks a little different, or it will look a little different—and most recently of all that global Britain has global reach that will develop in new ways.

Could you comment on all that? Is that really going to change the position in the world that we have been used to for the past 70 years? Are we entering a new pattern of networks, with new friends and new allies? Will the way we conduct all that change, because we have the old-fashioned system here in Whitehall that we have had for 100 years? Do we need a bit of a stir-up? You are all smiling and leading us to think that the answer is yes.

Mr Peter Wells: I am thinking of my friends watching through the camera. Yes, things are changing. In any major wave of technologically driven change, it is hard to see far ahead. It is like there is a foggy road in front of us. We can see only a certain distance, and it is a shorter distance than in more stable periods of change. We need a certain amount of agility and responsiveness during that period to be able to adapt to those situations.

There might be a lesson here for Whitehall—some of the brilliant, talented and committed parts of Whitehall—in thinking about that responsiveness and agility and how to adapt and bring that into their working patterns and practices. What that means for the UK and who its friends, allies and enemies will be in the future I will leave to wiser people to judge.

Lord Grocott: I want to be sure that I am hearing you accurately. I am surprised but reassured that you seem to have avoided hyperbole with regard to the technology we are talking about, whereas for so many people in the field it is almost New Jerusalem territory—potentially it will change the world and we can all sit back.

I have noticed that several times you have used phrases such as "not to exaggerate the impact of technologies"—I think that was your phrase, Dr Faith, in relation to education. Is that a fair characterisation of your position? A phrase like "the fourth industrial revolution" is so grandiose. I used to represent the constituency that was the home of the first Industrial Revolution, and that is probably where I still am. Is that a fair generalisation?

The Chairman: That is a good final question: how fundamental is all this really?

Dr Becky Faith: I think it is fundamental, but for me it speaks to the value of evidence and research to examine critically and rigorously the claims that are being made for the impact of technology and the disruption caused by technology, and to look at the impact on people's lives and their ability to lead lives they value—and, again, to bring that back to the sustainable development goals and the UK's commitment to achieving those goals. For me it is about having your feet on the ground and the need for rigorous research into and evidence on these issues.

The Chairman: Mr Wells, do you agree?

Mr Peter Wells: Yes, very much so. One of my concerns about the hyperbole in my industry is the timescales. WhatsApp will tell you, "We built a messaging app that had a billion users within four years, so everyone can do that". That is not a systemic change. That is just a point solution. Systemic change takes much longer—decades or a century—to work its way through. This wave of change is fundamental, like other waves of change have been.

A lot of the decisions that we are making now will have lasting influence. I come from Lancashire, but I now live near Newcastle. Next to my home is an old wagonway that was used to transport coal trucks from the mines down to the docks. The width of that wagonway ended up being the width of our railways, because that is where the first steam engines were tested, and the width of standard railway gauge in most countries around the world. There is a story that no one knows if it is quite true: it affected the width of the rockets in the Apollo space missions. The decisions we make, such as where the Romans built their towns, have lasting implications. It is important, but there is a long time to go.

The Chairman: Ms Elmi, what message are you going to take back to the Swiss Alps: that the Brits have isolated themselves and are floating off into the North Sea or that we are going to be more interdependent and integrated in the new world networks than ever?

Ms Nima Elmi: You probably know the answer to that, Lord Chairman. I agree with my colleagues that it is not about viewing the fourth industrial revolution in isolation—as simply concerning emerging technologies.

This is a bigger conversation that requires systems thinking, as Peter was saying, because of the convergence of technologies against the backdrop of globalisation, urbanisation, climate change and demographic change. Professor Schwab's second book with my colleague Nick Davis is really talking about how we shape the fourth industrial revolution—now that we are at that fork in the road, about the key things that we need to address and have in our thinking as policymakers, business leaders and innovators, and civil society to make sure that the decisions that we make today are positive and not disruptive?

It would be remiss of me to say that it is not important: it was the topic of our Davos conversation a couple of years ago and has been permeating since. For us, it is in a context of responsible and responsive

leadership, and it speaks to agile governance: how do we help to inform policymakers and civil society leaders so that they are not just reactive but, as best they can, a little more proactive in the way they shape this?

The Chairman: That is a very good note on which to end. Thank you very much, all three of you, for enlightening us, answering our questions patiently and helping us as we move through this forest—this labyrinth—of new complexities and new worlds.