HOUSE OF LORDS

Select Committee on International Relations

Corrected oral evidence: UK foreign policy in changed world conditions

Wednesday 28 February 2018

10.45 am

Watch the meeting

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

Evidence Session No. 5 Heard in Public Questions 37 – 49

Witnesses

I: Mr Tom Fletcher CMG, former Ambassador and Visiting Professor in International Relations, New York University.

II: Dr Andrea Calderaro, Director, Centre for Internet and Global Politics, Cardiff University; Dr Madeline Carr, Associate Professor of International Relations and Cyber Security, University College London; Professor Philip Howard, Professor of Internet Studies and Director of Research, Oxford Internet Institute.

Examination of witness

Tom Fletcher.

Q37 **The Chairman:** Mr Fletcher, good morning, and thank you for being with us. I am obliged at the start to remind you and everybody that this meeting is on the record. There will be a transcript of it afterwards, which you are free to adjust and change if you wish. Those who feel that they have a related interest should mention it when they speak on a question.

Mr Fletcher, you have been both a practitioner and an author in the fields that interest us, and some of us have studied your writings. Let me divide the subject into two aspects to start with. One is that diplomats now have to deal with a much wider audience—you were very much a practitioner of that when you were in Lebanon. The other is that, here at home, the foreign policy, international face and contact pattern of this nation has to think of itself or operate in possibly rather radically different ways from the past. Foreign policy no longer stops at the portals of the Foreign Office, as it were.

Those are two big issues. Without covering the whole field in one answer, could you give us your general approach to them?

Tom Fletcher: Thank you, Lord Chairman. It is a great pleasure to join you. The last time I was before the Committee it was a virtual session from Abu Dhabi and I was heavily pixelated, so it is nice to be here in person.

Diplomacy is under pressure in the same ways that other professions are under pressure as a result of the changes caused by digital technology. Many institutions are facing a crisis of trust. We see it across the spectrum, and diplomacy is no different. That trend is accelerated by digital tools, and it is making the context for diplomacy much tougher.

We are operating in a context in which the perception of inequality is growing, and, again, that makes it harder for us to gain and use the trust we need to be effective diplomats. However, specifically with technology, we all know that in the next century we could go through as much technological change as in the last 40 centuries, we are told. That will put not just many industries out of business but many ideas and states out of business, too. So the diplomatic context is very much in flux.

Like everyone, diplomacy itself is being disrupted. It is being disrupted by other parts of government, which feel as effective at it, and in many cases are, and by the corporate sector and by NGOs—by others operating in the diplomatic space. However, we have to be careful in this context not to be buffeted by the latest gadget or the latest tweet from the White House at 3 o’clock in the morning, and to focus instead on the essentials of the craft.

For me, diplomacy matters more than ever in the digital age. If it did not exist, we would be trying to invent it to deal with the consequences of the crisis of trust and with the political consequences of that inequality. We

also need it to deal with the gulf between Governments and technology leaders when it comes to discussing the challenges and opportunities of technology. Reinventing diplomacy means trying to master the new tools at our disposal and trying to get better at connecting with people and reaching out, as you say, to new audiences—new groups of people who we did not have to engage with previously.

Lord Grocott: Picking up on your point about putting states out of business, which is a bit of a theme of yours it is fair to say, you say in your introduction: "diplomacy existed before states, and will exist after they have ceased to be the principal form of geographical power".

My observation, for what it is worth, is that over the past 20 or 30 years, particularly in Europe, we have seen a proliferation of new states in the Baltic and in the Balkans, Czechoslovakia, and the possibility of new states coming into being, whether it is Scotland or Catalonia. It is quite a resilient mechanism, and I would just about make the thesis that it is the international blocs such as the EU, which I take at random, that may be slightly more at risk than the fundamental strength of the nation state.

Tom Fletcher: I am sure that that holds. Diplomats, of course, derive their representation from the state. We are Her Majesty's ambassadors. One of the sections that I had to take out of the book commented on the nature of that representation and suggested that increasingly we feel that we are not just Her Majesty's ambassadors, although that is still a key part of what we do, but Her Majesty's Government's ambassadors, and the ambassadors of Her Majesty's people—of the country more widely. That sense of projecting soft power and representing more than just the state—everything from the Beatles to James Bond—felt to me like a core part of our job.

What I am trying to get at with the theme, which came up when we did the Foreign Office review last year, is that states are increasingly competing for that influence with big technology companies, NGOs and other institutions and organisations. So there is less oxygen for states. We are trying to deliberate on what we will do about artificial intelligence, for example—the threats and opportunities ahead. When we were dealing with the threat of Napoleon in 1815, we simply got together as states in Vienna for months on end, and it was the diplomats who patched things up across Europe and worked out how we would find a new way to operate. If you tried to do that with artificial intelligence, it would be very difficult as states to have the legitimacy to convene and manage that conversation in the same way.

Our challenge is that we do not know who has that convening power now. I have been doing some work with the UN to try to find ways in which it can move into that space a little more, particularly on issues along the line from liberty to security—those big challenges—online. Evidently, the UN is struggling to move into that space—Lord Hannay and others know that better than I do—and to find the legitimacy in that space. But states are also struggling to lead that conversation. It is a more competitive

field, although I do not think that in my working life I will represent as a diplomat anything other than a state.

The Chairman: In the light of all this and some of the things that you have said before, the Foreign and Commonwealth Office asked you to do some reports and to come up with some ideas. How did that go? Was it just for the Foreign Office or for the whole international interface of Whitehall?

Tom Fletcher: It was primarily for the Foreign Office in the first half of 2016. We did quite a detailed review. It was not just about technology, of course. This being the first post-internet review, there was a danger that we all got caught up with the latest shiny gadget or platform. We thought a bit about social media, but we were looking much more widely at the culture of the Foreign Office and of diplomacy. We felt that traditionally—I was reminded of this, reading Lord Wright's memoirs in the last few weeks—the Foreign Office has not been great at calculated risk, accountability for decisions or the execution of policy.

I worry that digital technology and our excitement about social media—I am at the evangelical end of that spectrum—accelerates those concerns. It puts more of a premium on people who can come up with a quick soundbite or a deft tweet rather than stick around and deliver policy over a long period of time, look around the next corner and think in a strategic way. We wanted to put the emphasis back on areas in which we felt that the Foreign Office needed to sharpen up its act in the digital age.

You have to recognise that the report landed probably two months before the Brexit vote. We were then in a very different world. I am reassured, meeting the team again this week, that the vast majority of the recommendations made are being pursued pretty vigorously. There is a serious process for doing that. I would be worried if every recommendation was being pursued—that would suggest that the report was not doing the job that it should have done—but the vast majority are being pursued. When I bump into diplomats around the world now, I feel that they are much better equipped with technology that allows them to be fleet-footed, flexible and better at information gathering and sharing than they were two or three years ago.

Lord Hannay of Chiswick: I am following your answer and it sounds slightly as though you are saying "Back to the future". You are saying that the old skills of the Foreign Office—to be analytical, to drill down into problems, to have language skills, to have skills in other people's cultures and so on—are needed every bit as much, if not more, in the digital age, when the temptation is to spend most of your days sitting in front of a screen with your eyes gradually turning square and not doing any of the things that you ought to be doing, such as getting out and meeting real people and listening to their views. Have I got that right?

Tom Fletcher: Absolutely.

Lord Hannay of Chiswick: If so, it is an interesting conclusion to reach,

but it is not a revolutionary one. We need to do more of what we used to do but have stopped doing because everyone is glued to their screens.

Tom Fletcher: That is very much my conclusion. I felt that, for example, we had to get away from the idea of the desk officer, which suggests that someone is sat behind a desk. We have to get away from the idea of an embassy as a building and get back to the original idea of an embassy as a group of people, not necessarily just diplomats, sent out to engage, to gather information and to understand the country in which they are serving.

I recommend to the Committee an OECD report, published at the end of January, on the future of education. This is going slightly off track, but I will try to explain why. It suggests that to ensure that robots work for us and we do not work for robots, the skills that we have to develop through our education system are creativity, curiosity, adaptability, flexibility, critical thinking and emotional intelligence. Those are what will set us apart in the next phase. Many people call those 21st-century skills; I call them diplomacy. For me, that puts even more emphasis on the need for diplomacy as a craft and for diplomats—exactly as you say, Lord Hannay—to be away from their desks and out there, honing and using those skills.

The challenge that we have always had is that they are not easy things to test, assess or measure. It is very difficult to assess someone's curiosity or adaptability. For the first time, the OECD report provides the means and the start of the conversation on how you teach and assess those skills. There is a real niche for diplomats in that conversation but also in encouraging our education systems to ensure that those skills are developed in our younger people.

Lord Wood of Anfield: I am interested in what you think embassies offer the home country that you cannot get from the internet in this age. If I want to find out about Romania, I have the internet at my disposal. What can an embassy on the ground add, above and beyond that, with the skills and the outreach that you are talking about?

Tom Fletcher: What you are describing is part of the trend that was already gathering pace pre-internet. I am sure that in 1989, as the Berlin Wall fell, the Prime Minister was not thinking, "What I need most now is the telegram from my ambassador describing how the wall is falling". I hope that—although, as Lord Wright's memoirs show, this was not necessarily the case—the Prime Minister would have been looking for the analysis and the judgment: "What's really happening on the ground? What's going to happen next? What are people saying behind the scenes about these developments in Germany? What are the implications across Europe?"

That is still where diplomats can add most value, perhaps even more so in an age when there is so much information and data. As we know, the television in No. 10 is on permanently. It is easy to be buffeted by the latest breaking news and by the 140 words that you need to put on the

Sky ticker to get the Government's view across or the 140 characters on Twitter. I hope that diplomats can offer perspective, calm judgment and a longer-term view at a moment when, as I say, people are chasing the latest tweet from Donald Trump.

The Chairman: Let us just clarify this by picking a specific country and seeing how your model would apply. Kazakhstan is a vastly important country, potentially rich, right at the centre of Asia, dealing with China and the world. If you do not have desk officers, how would the point person operate? Are you saying that much more power should be in the hands of the ambassador on the spot? Explain how this would operate without desk officers in Kazakhstan.

Tom Fletcher: My point is not that you do away with the expertise in London but that we call it a policy officer or country officer rather than desk officer. Your Kazakhstan policy officer would be the hub for all the information coming in. One of the ideas of the review was that there should be a nudge back to the woman or man on the spot. You are indeed looking for the telegram or letter from your ambassador in Kazakhstan rather than a policy paper drafted and turned into a vanilla product by being slightly overworked in London.

I would love to get back to seeing a few more Cabinet memoranda from individual ambassadors on policy issues. In my experience in Downing Street, by the time the foreign policy product got to Ministers, it tended to be fairly watered down. That is not a new thing, of course. Churchill said that Foreign Office memos were, "On the one hand this, on the other hand that", and that one should ignore every second page.

I would like to see more challenging and in some cases less risk-averse advice from posts. One of our worries when we looked at the spread of Foreign Office resource was that we had two-thirds of our people in London and one-third overseas, which did not feel to me like a properly outward-facing foreign service at a time when we need to have a world view formed after having actually viewed the world.

The Chairman: To sum up this general point—we will get on to specific areas—is digital technology changing the whole nature of the operation of diplomacy, or is it just a useful tool that should be deployed more by officials?

Tom Fletcher: It is an evolution rather than a revolution, as Lord Hannay suggested. The key to diplomacy is still the traditional skills. Certainly at the moment, with the sense that I think we all have that time is speeding up around us and that with the rate of technological change it feels as though technology is having a huge impact on how we do the job day to day.

The smartphone with which I was trying to engage people in Lebanon was also the means by which terrorists were tracking my movements. It is a metaphor for this as an opportunity and a challenge. I was finding that for the first time I could reach out and have a conversation with the

public at large. If power is perhaps slowly shifting away from states towards individuals, we need increasingly to engage with and influence those individuals.

The Chairman: That is a very good answer, if I may say so. Thank you.

Lord Purvis of Tweed: First, I will follow up and challenge your answer to Lord Wood on the need for human intelligence and human contacts from our embassy staff. When we had Lord Hague in front of the Committee, I asked him for his view on the massive reduction in our in-country staff over the last few years. The number of postings has gone up slightly, but I am talking about the number of staff. That is slightly counter to what you said was its value, and I wonder whether your review looked at that.

Also, there are now more than 2.2 billion monthly users of Facebook. When it comes to forecasting what social movements are likely to be major events that will put pressure on a Government, the technology firms now have a greater capacity to understand what will happen soon and the ability to forecast more than any traditional diplomatic posting from any country. Is that not a fact?

Tom Fletcher: I would agree entirely if the Foreign Office model did not change. If diplomats still based their reporting on two gins and tonics at a reception and a couple of editorials, clearly we could not compete in that world of sentiment mining and data mining when companies can put analyses together very quickly. But at least for the next 20 or 30 years we can be pretty confident that you will still need a human in the mix, asking the sentiment miner or the data miner the right questions. That is where diplomats can add particular value, to come back to Lord Wood's point. Understanding the key questions to ask and how to analyse and interpret those trends for government will, I am certain, be an added value for several decades yet.

Q38 **Lord Purvis of Tweed:** I was quite shocked when I read in your report on the FCO that, "we lack accurate data on language speakers, on previous postings and on staff numbers. This means that we do not understand the true costs of inefficient processes and struggle to measure productivity gains or to evaluate broader outcomes". Is better progress being made on that? Do we have a better handle on the language and skill sets of the people we have in the FCO now?

Tom Fletcher: I am no longer in the FCO as of a couple of years ago, so it is harder for me to say precisely—

Lord Purvis of Tweed: You can ask them when you meet them this week.

Tom Fletcher: I did indeed ask the question when I met them this week and was quite reassured. One thing that Sir Simon McDonald, the Permanent Under-Secretary, is very focused on at the moment is improving the cadre of hard-language speakers in particular, trying to avoid the situation that we found with the Ukraine crisis where we lacked

Ukrainian speakers, and certainly Ukrainian speakers who could be deployed quickly to do all the things we are talking about: reacting and understanding the crisis.

I do think it is getting better. There is much more evidence of long-term planning to rebuild the Arabist cadre, for example, and to build the Sinologist wing of the office. There is a big effort under way there, but with the caveat that others could give you much better data and more compelling answers than I can.

Lord Purvis of Tweed: Even though English is in many ways a global language by technology use, in many cases it also facilitates people using their own dialects or their own languages. What is your view of having a much greater number of language sets across the whole breadth of Foreign Office staff, given that people are now communicating by technology in their native tongue and in English.

Tom Fletcher: There is an important point to make about the way we use English itself. The language of diplomacy has often been quite exclusive and not engaging. The danger of the platitudes of democracy—the "warm bilateral relations"-type language—is that it turns off the public outside, giving the impression that we think that what we do is some sort of impenetrable craft that is far too complicated. It is a bit Sir Humphrey, to be honest. So when we use English on social media, there is a lesson for us about how we communicate with people in a more authentic, engaging way that makes them connect with the content rather than be switched off by what we do.

I recommend several accounts to you, such as the Foreign Office Twitter accounts, that are in host-country languages. The most successful tweeter in diplomacy, the Pope, tweets in at least nine languages, and we have ambassadors out there who tweet almost solely in Arabic, for example. John Casson, our ambassador in Cairo, has over 1 million Twitter followers now, which is an extraordinary number. So these accounts definitely have an impact.

Lord Purvis of Tweed: I will be there tomorrow evening, and I have seen some of them myself. On data, to quote from your report again: "90% of data was created in the last two years. Business has woken up to the transformational potential of Big Data. The FCO has not". You alluded to that in your previous comment. Can you give the Committee an example of what we should be doing by mining this data—by using it—that we are not doing at the moment? What opportunities are we missing by not doing this?

Tom Fletcher: There is a broader point here about knowledge management. The nature of foreign-service postings, which are for three to four years, is that we are not always terribly efficient about retaining the expertise and knowledge that has been gained. In Lebanon, if I was going up into the mountains to meet a warlord, he would almost certainly have a pretty clear bank of information in his head about the exchanges he had had with the 14 previous ambassadors—a body of information

that I would not have had access to. It was probably there somewhere, but there is no Wikipedia equivalent I could dig into to ask, "What did my predecessor really discuss with him in 1976? Does he still trust us or not? Did we let him down or did he let us down?"

We have not been very good traditionally at handling that sort of knowledge. The Foreign Office tends not to have very sophisticated handover programmes between ambassadors. It is almost slightly frowned on to be in country at the same time, for example. We have to get much better at that and understand much better that knowledge does not just reside in the person doing that job on that day. We tend to be quite protective of our postings and we should be a little bit more open with the information that we have. It comes back to your earlier question about the new tools that we now have to mine enormous amounts of data through social media and beyond. We can get much more sophisticated with that.

One of the experiments we are working on at my university is trying to build something called Diplopedia, a knowledge management tool that would allow you to ask the big data miners the right questions but also to preserve the information that you have coming in much more effectively. If your ambassador in New York is going into a Security Council meeting, she or he would be able to reach much faster into all the information sources in the network and ensure that they have more information than anyone else around the table.

Lord Purvis of Tweed: Are there other countries that to your knowledge are doing better than the UK at the moment?

Tom Fletcher: Not necessarily. To take that example of the UN, I would argue that our ambassador in New York has more immediate information from around the network at their disposal than anyone else around the table. However, others, particularly the Americans, are ahead of us in anticipating the next phase of data management—of information-gathering and analysis.

Lord Grocott: Can you reassure a non-tweeter like me? Tweeting, to me, seems almost to be the opposite of diplomacy. As far as I understand diplomacy, it is to an incredible extent to do with putting the comma in the right place and being absolutely precise and cautious in the use of language, particularly in Northern Ireland, the Middle East or anywhere else. What are the risks involved in ambassadors tweeting out? Have there been any catastrophes? Does anyone else see the potential tweet? Can anyone else in the embassy tweet away to their heart's content? It seems a slightly unmanageable process and full of potential risk.

Tom Fletcher: I used to find Twitter one of the most challenging ways of using language. In a way, every comma matters and every word matters even more because of the scarcity of language. If you are a diplomat, particularly an ambassador, using Twitter—and I would not say that it is essential for everyone; I would not argue that everyone should be out there, feeling uncomfortable in this terrain—you have to ensure that you

are doing it authentically and in an engaging way, but what is most important is that it is purposeful. When you stack up all these tweets at the end of a posting or a career, do they in some way contribute to Britain's prosperity, security and the promotion of Britain's values? If you are just using Twitter to gain popularity or attention, to bully people or to act in a narcissistic and self-promoting way, then frankly you are no better than the President of the United States of America.

We have to hold ourselves to a higher standard, whichever form of social media we are using. There are security risks. I mentioned one, which is that I would never be able to tweet from a public event because it would draw attention to where I was; I would tweet only after I left.

There have been mistakes. I made a few of them myself, at least two quite significant ones. However, while there are risks, the greatest risk is not to be out there engaging where everyone else is engaging. If there is a huge diplomatic reception and all our contacts are there, exchanging information, influencing each other, arguing and promoting their view, we would not delegate it or ignore it; we would be in there, interacting. That is what we have to do. I can go into more detail on the mistakes, if you would like a mea culpa.

Lord Grocott: Within the structure of the embassy, with you as the ambassador, do the staff all tweet as well on the same subjects, and is there any co-ordination?

Tom Fletcher: We are building that plane as we fly it. Some ministries of foreign affairs used to have a system whereby you would have to clear every tweet with the Minister. Clearly, that will not give you a quick response and is not a fleet-footed means of communication. The early days, when there were only four or five of us on Twitter, were glorious times. We had a lot of liberty, freedom and autonomy. It was like being an 18th-century ambassador, three weeks' boat journey away from London. You could experiment a bit more.

Quite rightly, the rules have tightened up now. The centre has to establish the key messages and our national narrative—the GREAT Britain narrative is a good example of this—and then you tweet within that framework.

There was a period when one of the main bits of guidance was, "Fine. Be visible wherever you are, but whatever happens, do not be visible at home". I think, Lord Hannay, that used to be the guidance for media more widely at various points. That is very difficult to do on social media; it is one big audience. So the guidance has evolved.

I am becoming slightly more conservative about people tweeting in an embassy. You need more message discipline. I am sure there is a certain degree of message discipline in individual political parties, for example. You want to hear the individual voice, but it needs to be within a framework. You cannot simply have everyone tweeting whatever happens to come into their mind.

The Chairman: Lord Balfe, do you have a question or do you want to move on?

Lord Balfe: My question was just answered, towards the end of that answer.

Q39 **Lord Hannay of Chiswick:** Perhaps we can go a bit further into this question of the risks and opportunities in individual countries. Please do not interpret this as being hostile to the message you are giving; it is quite the contrary.

I lived through one of the previous communications revolutions, which was called the CNN revolution, which basically abolished Foreign Offices communicating with the press at 12.30 pm every day and only then, and introduced the 24/7 thing, which was called CNN and which we had to cope with in New York, at the time of the first Gulf War in particular.

It strikes me that as you look around the world there must be a very sharp difference in operating rules for an ambassador, depending where he is. I should think that the ambassador in Beijing would have to be pretty careful about what he did on Chinese social media if he did not want to find himself frozen out completely from any dealings with the Chinese Government. The same, I suspect, is true in Moscow, where the risks must be very great indeed if you start tweeting things that upset the Kremlin.

There are probably plenty of other countries around the world where you cannot lay down rules and say, "Let it all hang out". In a sense, you had a benign environment in Lebanon, because in effect there was no Government, so when you went over the head of the Government you were going over the head of a vacuum. However, that is often not the case.

Can you talk a bit about these limits? It strikes me that if one is too enthusiastic about encouraging ambassadors to do this, there may be some nasty accidents down the road. You need some internal rules about how best to approach this.

Tom Fletcher: Your point about the CNN revolution is important. It is important to remind ourselves that diplomacy had to react to previous waves of innovation. There is the famous line, "You can replace the Foreign Office with a fax". The fax has been replaced; the Foreign Office has not yet. Palmerston saw a telephone and said, "My God! This is the end of diplomacy".

At every moment, people felt that diplomacy could not necessarily adapt to the new conditions, but it found ways to do so. Ultimately it comes down to judgment, and it is a recruitment problem, not a communication issue. We need to ensure that we recruit people who, if they are in Moscow, Beijing or Riyadh, have sufficient judgment to know how to use the new tools and how not to use them.

As you say, Lebanon was for me a very benign environment in that there was not a huge amount of UK Government day-to-day engagement,

naturally. There was no entrenched state, Lord Grocott, in Lebanon, to make me worry about what I was doing. It was quite an unusual environment. However, it was not always benign. It was a country in which Hezbollah was the most powerful organisation, and we were in a region where embassies were being stormed and in some cases attacked, sometimes because of mistakes made on social media. I therefore felt that I had to weigh every tweet carefully. There was less of risk about the UK end, but there was a risk of creating issues for other posts in the region, and threats to my own post.

I had my own set of rules at that stage, which was then in the foothills—the early days of tweeting diplomats—but they were quite strict rules about when I would tweet and not tweet. Certainly, I never tweeted in anger. However, those rules apply whether you have a TV camera or a journalist in front of you. You have to trust our people to have the right judgment, and if they do not, they are not the right people.

Lord Hannay of Chiswick: Carrying on, but switching a bit, if we become even more active in this field, to what extent will we encourage other countries to do it to us? After all, there is quite a lot of speculation about the activities of the Russians, both in the American presidential election, possibly in the referendum here, in the German and French elections, and so on. I am not saying President Putin did that because we did it to him, although that is his story. He says that is why; he says we have been interfering in Russia for years, so why on earth should he not interfere with us? To what extent does a free-for-all in this area have risks for us too?

Tom Fletcher: The reality is that it is a free-for-all anyway, and we can choose to roll up our sleeves and get stuck in, trying to create a more positive conversation around diplomacy and the issues and values that we care about. I would not want to leave the terrain purely to the wall-builders, the trolls—in the case of Putin, the diplomatic trolls—and to those who are using the new tools to radicalise communities, including our own. So we have to be in those discussions and those arguments.

One challenge is that it is anarchy; there are no clear rules. I have been doing work with the UN to help it to establish what some of those rules should be. But it is very difficult to stand up those rules. We have seen that in particular with the way the Russians use social media. When I tweet about Bashar al-Assad I am often hit by several hundred abusive messages within minutes, and it has a chilling effect. We hope that we are all resilient enough to take that—you are in politics and will know this better than I do—but it does have a chilling effect. But I would not want us to run away from those arguments.

Q40 **Lord Balfe:** Digital technologies have been used to bring pressure, both legal and illegal, on foreign ministries. To what extent do you think that this constrains the abilities of Governments to act effectively? There is always at the back of your mind the thought that something may be used against you or used to try to shape the way in which government policy emerges.

Tom Fletcher: That is a tough question, to which we probably will not know the answer for several decades. My instinct and my hypothesis—I hope I am right—is that, at each stage at which diplomacy has been democratised and there has been greater accountability and transparency, we have become better at it. The number of people who have died in conflict is one measure of the effectiveness of diplomacy, and we are getting better at it somehow. To have more oversight, transparency and accountability instinctively feels to me like a good thing.

There will always have to be secret channels, but I like the idea that we do more of our work out in the open. It challenges us to be better at what we do. I welcome more transparency, but it makes us more risk averse. We tend to be more fearful of the public inquiry or the leak. Sometimes in diplomacy you have to take calculated risks. Many of the judgments that you take are 51% to 49% and you do not know until you have the benefit of hindsight whether you are right. I worry a little about that aspect.

Lord Balfe: You mentioned the Bashar al-Assad tweets. I have taken one or two controversial positions in life, including recently here. You get overwhelmed by people who clearly have a different point of view, to the extent that you think, "Should I say that at all?" Instead of encouraging transparency and thought, it may go the other way and you think, "I'm not so sure about that, so maybe I'll just shut up and keep it to myself, because I'm not going to influence many people anyway".

Lord Grocott: Do not tweet.

Baroness Smith of Newnham: Do not tweet.

Lord Balfe: I do not tweet; I am thinking of other media.

Tom Fletcher: A good practical example of this was in the summer of 2013, when we were debating whether to take military action against Bashar al-Assad. At that stage, we were rightly having an open and transparent public debate about our policy options. That meant that, in the game of diplomatic poker with Putin, he could see our hand. We may be in a period a bit like the first 100 years after the printing press, when the ranters, slanderers and those who abuse the new technology tend to have a slightly louder voice, before the rules and a values-based system can catch up. In such a period, it may be harder for countries that value transparency and openness to do diplomacy in an adversarial setting with countries that are more willing to use the dark arts of these new tools.

Q41 **Baroness Smith of Newnham:** You mentioned that your FCO report came out a couple of months before the Brexit referendum, just as this Committee was set up—we had one meeting before the referendum. Context is obviously important, but even then you were calling on the Foreign Office to reassert its role. For years, the potential tension was between DfID, FCO and MoD and whether there was sufficient dialogue between them. Since the referendum, we have DExEU, the Department

for International Trade and a whole new set of competitors for international influence.

What advice do the Government need on that, and to what extent does your original advice—that the FCO needs to reassert its role—become even more important in the context of Brexit? It is not just a question of learning hard languages but of learning other European languages, because if the fax did not end diplomacy, in many ways EU membership has, to the extent that Ministers talk to each other at meetings, which will no longer happen.

Tom Fletcher: That is quite a challenging question. As I spend more time away from the day-to-day trench warfare of diplomacy, I feel less competitive and adversarial about some of the conclusions about the Foreign Office needing to fight its corner and so on.

If there is one advantage to the context in which we find ourselves at the moment on Brexit, it is that there is plenty of work to go round, so we do not need to fight over every little bit of policy. I believe that there will be a moment, probably the other side of Brexit, when there will once again need to be a consolidation and tighter co-ordination of all the overseas instruments. That will be a good thing for British diplomacy and for the Foreign Office.

It is quite positive. If you look around some of the departments that you mentioned, our brightest and best diplomats are all involved. The Foreign Office has seen this as an opportunity for its people to go out and get experience on the front lines of the overseas, diplomatic effort. It is not just retreating into King Charles Street and sulking about the fact that there are too many other departments.

The Chairman: You used the word "consolidation". It is fascinating that people are now saying that DfID is producing its own foreign policy, the Department for Education is producing all kinds of links with education establishments across the world, and the MoD is talking to all sorts of partners, which does not necessarily fit in with FCO priorities. It is a very disparate scene, so how will you consolidate it?

Tom Fletcher: For me, this comes back to the role of the ambassador and the role of the embassy, which is where I think the Foreign Office can demonstrate most added value. If you are having a meeting in Whitehall about climate change, you do not just want diplomats in the room. You want to have climate change experts and everyone else; you want your sources of knowledge, information and wisdom there. But if you are having a meeting on how to influence China on climate change, you want your ambassador there on the video screen or in person. That is where Foreign Office expertise adds the most value to what is happening in Whitehall. The more that people are out there on the ground doing that, the more we justify our existence.

The Chairman: Back in 1970 there was a huge upheaval in the pattern of departments in Whitehall, with the creation of the Department of the Environment, for example, which did not exist before and brought

together all sorts of other departments. Do you see upheavals of that nature ahead in Whitehall to adjust to this new world that we are talking about?

Tom Fletcher: As an observer from outside now, it feels to me that there are way too many government departments, but I am not an expert on that. I think there are opportunities. The Foreign Office is quite good at developing generalists who can move across different disciplines but then can bring that particular added value of an understanding of the country context—how to negotiate and how to gather the right information and present it in a helpful way to the experts back in Whitehall. That has to be the niche for the Diplomatic Service.

Q42 **Lord Hannay of Chiswick:** Could you give us an idea of how much you think the ambassador in an individual post has proper co-ordinating control over all the staff who are in that post, given that the digital revolution has meant that those staff can communicate directly with their own departments without going through either the ambassador or the Foreign Office, in a way that did not happen 30 or 40 years ago, when all the formal communications took place in the ambassador's name, even if he outsourced its content? To what extent do you think the ambassador's role remains valid in that sense, or do you think that the disparate parts of his embassy are each pursuing their own policy?

Tom Fletcher: I fear that it had got slightly out of control for a while. This was a particular challenge in some of the Africa posts where we might have had more senior DfID staff in country than the ambassador. There were moments when it was the head of DfID who would go to see the president and the ambassador might get to tag along. However, it was the head of DfID who had the leverage in the conversation because of his influence and seniority in Whitehall.

It was one of the things that we looked at quite closely in the review and one of the areas in which we wanted to reassert a little the primacy of the head of mission. In my experience in Downing Street, Prime Ministers really understand this. In the end, they see the ambassador as the key fount of knowledge on what is going on in that country. While you might get a bit of departmental mischief here and there, when it comes to any big decisions they respect that hierarchy in the post.

I think that any good and effective ambassador will be keen to use all those experts and departments in the embassy. I always welcomed it when we had more people from outside the Foreign Office in Beirut—the military, defence and trade experts and so on—but there is a way of mobilising and using that group and giving coherence to it that adds value to the embassy rather than detracts from it.

Lord Hannay of Chiswick: You do not think that the digital revolution has made that more difficult.

Tom Fletcher: I do not think so. Sometimes the challenge is that because everyone is so keen to show that they are acting in a

collaborative way, you are deluged with information. Your DfID colleague will make sure that he is copying the ambassador in on everything that DfID is doing in country, while the military and defence advisers are doing the same thing.

To stay on top of all that information is quite a challenge for the ambassador, but I would rather have too much information than too little. I never felt that that was a problem in Beirut. Sometimes it is a problem that is down to individual personalities, but again that comes back to being a recruitment problem and an issue about messages coming from the centre on the need to work together.

Lord Purvis of Tweed: I have been struck in previous evidence sessions by the concern about Ministers' ability to use WhatsApp groups and to communicate directly with their counterparts, thus bypassing some of the traditional routes. It was not possible to do that 20 years ago before text messaging.

I also want to come back to your answers on how you deploy some of the digital technologies, primarily social media, as tools for communication. On a recent visit to Amman, I was struck by the fact that the embassy cat has three times more followers than the French ambassador. It creates a huge amount of pleasure in our embassy in Amman that Lawrence of Abdoun has a larger following than the French ambassador, but it might only be a following among people who like cats. It does not necessarily help in communication.

Baroness Smith of Newnham: Is that an example of soft diplomacy?

Lord Purvis of Tweed: Yes, very soft, indeed fluffy, diplomacy. In your view, is there co-ordination across the other agencies such as DfID, the MoD and even the Royal Household: that is, those that are part of external-facing voice of Britain? What is the level of co-ordination? You mentioned earlier that putting out strategic messages works best if it is co-ordinated. Is that happening sufficiently across the different departments?

Tom Fletcher: Briefly on the WhatsApp point, diplomats have always been slightly frightened of any form of communication that allows leaders to speak to each other more without having to go through them. I am sure that it would have been the same with the telephone, but it is going to happen. In my time, it was happening more with text messages. David Cameron would have been the first Prime Minister to be texting his counterparts more readily.

One worry I have about the government process is that because WhatsApp is quicker and easier, you see policy groups using it increasingly. A lot of policy decisions are being taken in that group, but there will never be a historical record of how they were taken that can then be looked at in the future by historians and Committees like this one. That, I think, is a great loss. If people are taking risks, they are

more likely to take those risks on those sorts of closed networks than they would in official minutes.

I worry about social media that ends up leaning too far towards cute cats falling off chairs. I do not think that we are there to chase followers. If the cute cats bring greater attention and respect for what we are doing more widely, that is fine. It helps to lift the lid on life in an embassy because it makes us seem a little less remote and elitist. I do not want to be snobbish about cute cats, but if all we are doing is cute cats, other people can do that better.

Lord Reid of Cardowan: First, I should apologise for being late. Take my advice: do not hold breakfast meetings in the middle of a blizzard in London.

Following on from the question put by Lord Hannay, you said that when you step back from diplomacy you can look at the bigger picture. One of the futures of the networked world is the obviously increasingly interlocking nature of almost every problem both in terms of information coming in and the responses made to it.

I suppose the classic instance is counterterrorism. In the 1950s, it was a matter for foreign affairs, with the exception of the IRA, and defence. Now the threat is seamless in that it is part of foreign and domestic affairs. It cannot be responded to just by defence and domestic legislation. It runs through prisons, through education and through immigration. In other words, the seamless threat requires a seamless response.

To what extent can the Government, who have traditionally siloed departments and left co-ordination to the Cabinet Office, which has a very small budget and almost no power to compel, realistically respond seamlessly to many of the problems that are now completely interlocked and run through or above the silos of governmental departments?

Tom Fletcher: It is a huge challenge, and we have to do the best we can. The Buzz Lightyear quote, "This isn't flying. This is falling with style", perhaps applies here. All these problems are interconnected. The diplomats we spoke to during the review said that the times when they felt most motivated and effective and that they were really contributing to UK objectives well were normally not when they were in a structure or hierarchy, not when they necessarily knew their place within the organogram, which was very rigid and hierarchical, but when they were working in a project team on these sorts of challenges. We want to shift resource from the organogram into the project teams, which hopefully can then be much more responsive to ministerial priorities.

It is interesting to note, for example, that the Government are now appointing a Minister for loneliness. While we are not going to set up a department for loneliness, we can set up an interesting cross-departmental project team that will try to pull the work together on the issue. I think that a lot of energy in government will go in that direction,

which is probably a positive thing. It is the best response that we can make to the nature of the challenge that you have described.

The Chairman: Professor, we have kept you for an hour and you have painted on a huge canvas around which we still need to construct a huge frame—and a good artist to fill that canvas. You are doing your bit in helping to get the picture straight. Thank you for sharing your thoughts with us. They are very valuable and useful, and we are most grateful to you.

Examination of witnesses

Dr Andrea Calderaro, Dr Madeline Carr and Professor Philip Howard.

Q43 **The Chairman:** I welcome our three witnesses and apologise for the interregnum while we solve the temperature problems in the room. We are very grateful that you are before us. I remind you that these hearings are in public and on the record. Transcripts are available afterwards, which can be adjusted by those involved if they so wish. Committee members' interests have to be declared if they arise and are relevant. I think you are familiar with the broad shape of the inquiry that we are trying to conduct. In the areas we are looking at, you have a special expertise and privileged knowledge to share with us.

I will start with a fairly general question relevant to our inquiry. To what extent have digital technologies changed the challenges and threats facing nation states? I add a codicil: if it is more difficult to establish who the enemy is and where the security threat is coming from, what should be particular nation states' reaction to it? How does that affect the behaviour between nation states and the old pattern of alliances that we inherited from the 19th and 20th centuries?

That is a big question. Please could you give us a general answer at this stage, because we are going to ask some much more specific questions as we go along?

Dr Andrea Calderaro: Thank you for the invitation to be here today. It is a pleasure for me to contribute to the discussion today. I am sure that today's session will be useful to cover the different threats that we are increasingly exposing ourselves to because of our increased connectivity. It is a broad question, and I am sure we will cover different aspects and talk in more depth over the next hour.

The increased connectivity of our critical infrastructure—all our stuff—leads to an enormous number of threats to our infrastructure. For example, the digitalisation of information exposes countries and state Governments to new forms of espionage. When we talk about the challenges, just to kick off the conversation on that, I stress that the main challenge is that the technology evolves more quickly than our capacity to understand the nature of that technology, especially when we need to discuss and identify policy reactions.

It will be complicated, for example, to identify the regulatory frameworks that we need to put in place in order to react as quickly as possible. This is one of the main challenges that we face. Because of that, the state needs to find new ways of collaborating as much as possible with other actors involved in this connectivity-building process, such as civil society organisations and the private sector. Of course, this is one of the main reasons why we are here today, and I hope that we will help to identify how we can react quickly to these digital developments.

Dr Madeline Carr: Thank you for inviting me here today. To some extent, digital technologies introduce a range of new threats and challenges, and opportunities of course, in international relations, but at the macro level there is some continuity and constancy in those threats and challenges.

The challenges of securing borders or providing security for citizens or economic prosperity are perennial. Digital technologies have fundamentally undermined the social nature of international relations because of the capacity for anonymity and the problems that attribution brings. The kinds of mechanisms that we use to address challenges—diplomacy, international law, political conflict—all rest on the fundamental principle that we know who we are engaging with and we understand that there is that social element to international relations.

For me, that difficulty of not knowing who we are interacting with is the most challenging aspect of international relations in the information age.

Professor Philip Howard: Thank you for the invitation to speak. I start off by saying that I am here even though many of my colleagues are currently on strike. As some of you may know, there is a threat to the pension plan. You all have one of the best scholarly communities in the world and you risk losing it. But most academics, most of the time, feel an urge to contribute to public conversations, so I am joining you today while most of my colleagues are on the picket lines.

There are two important challenges that we face now. I think information infrastructure is international relations in a very significant way. Every international relations crisis has an online parallel. Every online social movement now has some offline equivalent that can sometimes result in blood on the streets or bring out large numbers of people to face tear gas. It is difficult to tell the story of any international relations crisis without some room for cyber.

There are two particular challenges that we face in the UK, the first of which is public research. The security services have excellent research capacity. They have great skills at understanding the forms of attack that we face. These are closed systems of intelligence gathering. Industry has some of the best access to the kind of information that we need; Facebook and Twitter know internally much of what we wish we knew. The number of public research organisations that can work with public and open information is limited. Improving that research capacity would be one way of addressing the challenge.

The second challenge that we face is that, at the moment, many of my colleagues certainly are distracted by what happened in November 2016 in the United States or during the conversation about the Brexit referendum here in the UK. Most of the organisations that attack democracies have now moved on from the UK and the US and are attacking our democratic allies in the global south. The crisis has moved from the US and the UK to many of our democratic allies.

The Chairman: Thank you for that overview. If no members of the Committee want to pursue that, we will move on to the next question.

Q44 **Baroness Hilton of Eggardon:** My question follows on directly from what Professor Howard was saying. The issue of cybersecurity seems to have at least two aspects. One is keeping information secret, which traditionally diplomacy has been keen on, and the other is the organised attacks on countries such as Estonia and the difficulty of identifying where these come from.

As we know, and as you say, an anonymous cyber organisation depends on anonymity, and that is a particular problem in knowing whether it is Russia. We keep pointing fingers at Russia and North Korea, but we do not know whether in fact it is they who are setting out to disable us. So there are two aspects: one is the difficulty of maintaining one's own information secure, which may have an inhibiting effect on ambassadors' willingness to commit things to paper, and the other is the organised attacks on a whole nation, as in Estonia.

Dr Andrea Calderaro: I am happy to hear in the question already the assumption that it is incredibly difficult to identify the source of a cyberattack. This is very much the case. We have the capacity to identify from where the attack comes from, but it will always be difficult to prove who is behind a cyberattack, which makes impossible for us to attribute with certainty any responsibilities to a foreign state actor or military body. Indeed, that has major implications for the designing of some diplomatic strategy to react to a cyberattack. The European Union is working a lot on that and has announced that it will soon release the so-called EU cyber diplomacy toolbox, which will be a set of standards and rules that aim to identify how and when it will be possible for the European Union to implement some sanctioning strategies. As we know, sanctioning strategy is a tool often used by the EU in other fields.

The problem, as we just said, is that it is always difficult to identify who is behind an attack. It will therefore always be difficult to start a sanctioning strategy when it is difficult to identify the source of the attack. The only time sanctions have been used in international diplomacy was when the United States sanctioned North Korea as a consequence of the attack against Sony, after the release of a movie that apparently ridiculed the North Korean President. Of course, in that case it was easy for the United States to sanction North Korea, because North Korea has a weak diplomatic capacity. However, it will be complicated in the future to keep pursuing this sanctioning strategy, without the risk to generate diplomatic disasters.

The idea behind this approach so far is that cyberattack is recognised as a violation of Article 2.4 of the United Nations charter, which somehow protects the territoriality and sovereignty of countries—basically, protecting countries from each other. However, the problem with this assumption is that the cyberattack is constantly perceived and treated as a military attack, while this is very much not the case.

What is the solution? It is probably to stop treating cyberattacks as a military attack. We will never be able to develop deterrence strategies based on this approach. We rather need to develop a diplomatic capacity on different innovative levels.

Dr Madeline Carr: One of the challenges for foreign policy and international relations in this context is that it can be very difficult or impossible to attribute cyber incidents conclusively to an actor as opposed to a geography. We are therefore seeing some suggestions that the burden of proof should be lessened so that we can do without conclusive technological proof that can attribute an attack and rely on evidence such as who had the motivation or which actor had the capacity or stood to gain most from such an attack.

I flag up that as a worrying trend, as it leaves us open to these things being spoofed. If we no longer rely on conclusive technological evidence of an attack and rely instead on factors that can be faked, we leave ourselves open to responding to an attack that we should not respond to, in a way that we should not respond to it.

I guess that the goal in these situations, certainly at the international level, should be at all costs to prevent escalation to a kinetic conflict. The goal should be that no cyber incident gets accidentally or intentionally attributed to an actor such that it prompts a response that could lead to a kinetic conflict. That is the risk of these conversations about attribution, where if we cannot find conclusive proof, we just use what we can find and make a best guess.

Professor Philip Howard: There have been several moments when we have got very close to conclusive proof. Industry sits on enormous amounts of data, which is useful for proving these connections. Facebook, for example, only grudgingly revealed what it knew about Russia's involvement in the US after a Senate inquiry, a House inquiry, a Justice Department inquiry and an FBI investigation. We know that firms have this data, and some academic units are getting better at working with civil society groups to do what we call social data science to trace these things. The craft is therefore improving, certainly in democracies.

Lord Reid of Cardowan: I am sure that it is improving, but the point that has just been made is a fascinating one. The difficulties in attribution are huge. Even if you could attribute it to a particular place and a particular group at a particular time, you might find that it is a hospital. In the same way that you can hide artillery pieces in a hospital and launch an attack, you can do it through bots, extensions and the network, and so on.

That raises this question. The doctrine of deterrence on nuclear weapons developed over a number of years, to the extent that it was mutual assured destruction. Michael Quinlan and others in the United Kingdom developed that. However, it more or less developed without a formal treaty. It was the recognition by all parties that if we did X, someone else would do Y. The problem with cyber is, first, attribution, and, secondly, that instead of six, 10 or 12 nations having the capacity, there are now 4 billion people with platforms that can launch an attack, which are as various as a laptop or an iPad, or whatever.

My question is probably an impossible question, but a central one: how do we develop a doctrine that is commonly accepted and understood, short of an international legal agreement, which I do not think we can get—you can get it with two nations, but not with 190 nations—and begin to work towards a doctrine on cybersecurity that will reduce the risks and the possibility of one group of people, sometimes through pirates rather than the state itself, attacking another group of people whose infrastructure is now entirely dependent on industrial operating systems and software? Do you have any idea how to start to approach that question?

Dr Madeline Carr: A good starting point would be not to return repeatedly to these Cold War concepts, which, as you point out, were developed in a very different technological context. Ideas such as deterrence, which made a lot of sense with technology like nuclear weapons, which had very clear implications and very clear uses, are deeply problematic when we are talking about a technology that is interwoven through civil-society infrastructure, the military, governance, communications—everything.

The two aspects that we should focus on are the recognised and growing interdependence that we all have at a systemic level and the resilience of those systems. What is worrying is that when we have these discussions about international relations and international competition in the information age, most of what we are talking about are legacy cybersecurity problems anyway; the legacy of the last generation of cybersecurity problems.

As you have pointed out, we have not done a great job of dealing with them, but we are already looking at emerging problems that have not even really made it on to the table yet. In order to avoid building in the kind of insecurity that we did in the first generation of digital technologies to the next generation, we need to find a way to talk about what is coming along in both the near and the far future.

The Chairman: Before we move on, I have one question to put all of this into perspective. There are people who have written books saying that the cyber threat is a more serious issue for international stability than the nuclear threat for the reasons that Lord Reid has touched on. If we think about the past few years, there have been some global cyberattacks, but they have not killed millions of people and destroyed cities. They have done nothing on the scale of a potential nuclear bomb. What is your

general view? Is the cyber threat greater than the threat of nuclear war? Could you put this into perspective for us?

Professor Philip Howard: It is not greater than the horror of a nuclear attack, but I would say that several Governments have fallen because of social media-led campaigns, some of which may have been false or falsely seeded. There are at least four dictators in north Africa who lost their jobs, if not their lives, during the Arab spring. There are therefore many examples at this point of significant changes in Governments because of either cyberattack or activism in the form of democracy advocacy carried out online.

Lord Reid of Cardowan: Perhaps I can approach the question in a slightly different way. You cleverly referred to the potential of nuclear weapons, but said that cyber had not been used. Of course, apart from Hiroshima and Nagasaki, nuclear weapons have not been used either. The real question is therefore whether a cyberattack has the potential to inflict damage on us that is commensurate with what an atomic bomb could do. That is the real question.

Dr Andrea Calderaro: I do not think so. Of course, technically we are constantly exposed to apocalyptic scenarios that are very much in line with other nuclear apocalyptic scenarios, but at the moment they are just science fiction. That is my personal opinion; I do not know what my colleagues think of it.

We are a long way away from any major damage, especially in terms of casualties. That is why despite the fact that we have been talking about cyberattacks for several years now, we are no closer to that scenario, and so far no one has died because of such an attack. That is my straightforward answer to your question.

Dr Madeline Carr: I have a different straightforward answer, which you find so often in this field. The argument that no one has ever died and there have been no casualties as a result of cyberattacks is what I would call a status quo argument: because something has not happened, we question whether it will ever happen.

One of the things that we are looking at in the near future is the wider implementation of the internet of things, which is very much about the physical dimension. Things will happen in the physical world as a consequence of the analysis of data, including things like autonomous vehicles and implantable health devices.

All these aspects are moving from what in the past in cybersecurity terms were about securing data and networks are now in the physical realm. We can already see the capacity for that. I agree with Dr Calderaro that at this point it is not on the level in our imagination of a nuclear weapon that could annihilate the world in a moment, but certainly the argument that there is no potential for violence or loss of life connected with cybersecurity is already old. We have not seen a death yet, but it is easy to contemplate how that could happen with vehicles or health devices.

Baroness Smith of Newnham: Are we not at risk of comparing apples and oranges here? If you are doing a risk assessment, you might say that a nuclear attack would be absolutely catastrophic, but the chances of it happening are very slight, whereas the chance of a cyberattack is high.

The question then, as Dr Calderaro suggested, is that while we have not necessarily seen any deaths yet, do we know that we have not done so? I ask this, because when the ransomware attacks were made on the NHS, who knows what some of the implications were? There is a whole range of things where the consequences can be severe. They may not be as catastrophic as a nuclear attack, but nevertheless we are perhaps not taking them sufficiently seriously.

Dr Madeline Carr: I would say that that is the case. The risk assessment is exactly of the likelihood and severity. Yes, they are apples and oranges. They are both international relations problems, but they are not the same problem.

Lord Grocott: Is this a conflict of evidence here? No one has died, as Dr Calderaro was saying. I perked up when Professor Howard said that several Governments have fallen as the result of cyberattacks. I would love to hear about a few of the examples. Presumably they were bloodless falls, otherwise there would have been deaths as a result.

Professor Philip Howard: The most dramatic would be Trump's election, which was an example of a significant attack carried out on social media that degraded the quality of information available to the electorate. We saw the content shift from social media into the broadcast media environment of the United States. It was such a large and well-executed move that there was in effect a change of Government.

Lord Grocott: Was that conclusive as far as you are concerned? You are saying that Hillary Clinton would have won—indeed, she did win in the popular vote—were it not for the cyberattacks. Is that what you are saying?

Professor Philip Howard: Yes, if the cyberattack had not been deliberately concentrated on the swing states to move fractional numbers of voters with ridiculous stories about her participation in paedophile rings and in corruption, the outcomes would have been different.

Lord Grocott: Can you give me a few more examples? You mentioned that several Governments have fallen—

Professor Philip Howard: —across borders. The examples also include democracy advocacy. So I would refer to Tunisia, Egypt and Libya during the Arab spring, along with Yemen, where another head of state lost their role because of a campaign that was effectively run over social media by democracy advocates.

Lord Grocott: A lot of people died in Yemen, did they not?

Professor Philip Howard: Yes. I should remind you that elections in India, Pakistan and South Africa are coming along. These are countries where rumours that originate over social media result in blood on the streets, especially during the heightened tensions of an election. If we expect foreign powers to interfere in the elections held by our democratic allies, those would be cases to watch, moments to look for physical casualties.

But I also agree with my colleagues that it does not make sense to draw a parallel between nuclear attack and the deterrence language and what we are talking about now, which is more about quality of life. A sudden loss of electricity infrastructure would have a significant effect on our quality of life, but it would not be comparable to a nuclear holocaust.

Lord Reid of Cardowan: I just want to clarify something. I hope it does not cut across.

I think that for the purpose of our analysis it is worth separating two things. We are talking at cross-purposes. You are talking about the use of social media through the internet to influence people's views and so on. I was talking about a potential cyberattack, not social media, on our infrastructure. In this country, it is now software that lands our planes, moves our trains, protects our water supply, distributes our food and money, and so on: in other words, the essential infrastructure, which any opponent would wish to damage irreparably and bring down the country, which is the purpose of war. We used to use bombs to do that.

What I was actually inquiring about, following on from what Dr Carr said, was that form of attack and the potential for it, because that has a huge significance for international relations. If you can be clever enough to carry out a conflict without actually declaring war, but you have done your reconnaissance and planted the viruses, as somebody did with Iran's Isfahan facilities for developing Iran's own nuclear capacity, that has huge consequences, does it not?

Dr Madeline Carr: It does. In some ways that is the stand-out example. We only have that account from the *New York Times* journalist who wrote about that story. But if we are to believe that account of the Stuxnet incident, in some ways the solution was a very creative and innovative one to an extremely dangerous situation.

Lord Reid of Cardowan: And it was a commonly used industrial operating system developed by Siemens, which is widely used in this country.

Dr Madeline Carr: Yes, exactly, and it demonstrated how that could happen, and states were prompted to consider their own vulnerabilities.

This brings us to the kind of observation that Barack Obama made about this. He called it the paradox of the information age: the states that have integrated digital technologies into their infrastructures most successfully are most vulnerable to the threats that they present. This is in

contravention to our pre-existing ideas about the relationship between technology and power in international relations, which used to be very much that the state with the most advanced technology—weapons technology or communications technology—was most likely to prevail in conflict, so it was regarded as a factor of power.

This comes to the whole purpose of this Committee hearing, I guess. While we understood what technology meant to power in international relationships in the industrial age, in the information age it is very much more complex. Unravelling those pieces is probably the work of a generation.

The Chairman: What Lord Reid's question was leading to is the questioning of all the traditional forms of alliances. If Russia attacks Ukraine over electricity—we have talked about Estonia, and there is the whole Stuxnet saga, which was organised by America and Israel, or so one assumed—this may not necessarily be in the interests of other countries. We hear a lot about our intelligence links with the United States, but if the United States' enemies and interests are different from ours, as they certainly are in some areas, that throws the alliance into question. Are we now looking at a new pattern of co-operation, which the old alliance pattern does not service?

Dr Andrea Calderaro: Are you asking about co-operation?

The Chairman: Yes. What does co-operation mean if we have different enemies and different purposes?

Dr Andrea Calderaro: When we talk about co-operation, which is one of the important strategies that needs to be pursued, especially when we talk about identifying the diplomatic tools that we might put in place, we need to introduce another concept, which I think is important here: cyber capacity-building.

Of course, to discuss co-operation, we need to be sure that we have the right interlocutors out there. We have been working for years on narrowing the digital divide as much as possible. Now we can say that all countries are connected, but not all countries are connected in the same way. Newly connected countries especially do not have the capacity to secure their piece of the network.

It is very important to perceive the network as a whole and not, when we talk about cybersecurity, be concerned wholly with how to secure the infrastructure within the UK but how to secure the infrastructure worldwide, by developing some co-operation and interactions with other countries. So co-operation goes together with capacity-building in order to increase the numbers of interlocutors and potential allies that we have out there. That is very important, especially because most of the threats come from countries that have a weaker capacity to react to cyber threats, and weak networks.

Q45 **Lord Hannay of Chiswick:** To what extent do you feel that the

development of digital technologies, which we have been talking about, has empowered individuals or groups of individuals—subnational organisations—to challenge the monopoly that Governments have had in the past over intergovernmental dealings, and made it difficult for Governments actually to act internationally in the way they were used to doing? I think we had better leave aside the activities of the tweeter-in-chief in the White House, who seems to disrupt his own Government quite frequently.

Professor Philip Howard: There are several examples of subnational identities that are stronger now than they were 20 years ago, because the internet allowed young people to develop their identities online. There are several communities that are closer to one another or that aspire to statehood or at least some level of independence, which they would not have achieved 20 years ago, because of social media and the internet.

When you look at the diffusion of technologies and the change in voting patterns, I do not think this has eroded, in most democracies, the degree of participation in elections. I am not sure that there are examples of Governments who have lost the confidence of their citizenry because of social media.

The Chairman: You do not think that.

Professor Philip Howard: I cannot think of an example, no.

Lord Hannay of Chiswick: So the biggest threat is the one we were discussing earlier, which is Governments either directly interfering in other Governments' business by digital technology or operating under pretty obvious aliases and so on. That is the bigger threat than subnational groups or individuals or groups of individuals.

Professor Philip Howard: I think that is the bigger threat, but I would argue that it will be important for all of us to stop separating the kinds of attacks that we used to associate with military initiatives from the kinds of attacks that we once called soft diplomacy or cultural diplomacy.

Our little group has done a piece of research on how Russia targets US military personnel for misinformation while they are on assignment in the theatre of operations. Now, is this is a classic military attack or is this a form of contemporary cyber/social media diplomacy? It is difficult to know, but the threat is serious and we know that these kinds of social media aggressions go after UK and NATO personnel as well.

The Chairman: This takes us on to the question of whether there is a need for a better international order, better behaviour, otherwise it is all going to be tit for tat; as Lord Hannay says, Governments pretending not to be involved when they are involved. This is very much what Lord Purvis's question is about.

Q46 **Lord Purvis of Tweed:** It is quite interesting, having seen how a group such as Daesh has used technologies and then seeing the coalition partners seeking to deploy similar tactics. That might not be a

cyberoffensive by targeting some of their infrastructure, but cyberwarfare has certainly been deployed by coalition forces. We now have a virtual army of strategic communications officers, whose entire role is to do that, which is quite interesting.

Let us separate out for a moment the military use or weaponisation of cyber by proxy from what might have to be a rules-based system to take into consideration the greater use of cyber. I was interested to read in the G7 communiqué from Italy last year: "To increase predictability and stability in cyberspace, we call on States to publicly explain their views on how existing international law applies to States' activities in cyberspace to the greatest extent possible in order to improve transparency and give rise to more settled expectations of State behavior".

It seems as though that is moving quite slowly, and I wondered whether you are aware that that work is being carried out and whether Governments are publishing how they themselves define the use of offensive cyberactivity covered by international law, and if there are gaps. The Secretary-General of the UN said last week in Lisbon that he believes that the UN is the best platform for starting to write new norms of international law, whether that is equivalent to the Geneva convention on cyber. He said in his speech that if it operates under the normal UN mechanisms of how member states operate, it could take a very long time, and it is urgent.

Can you inform us of whether activities are being carried out apace, and whether you think the UN is the right body to create these new international norms?

Dr Madeline Carr: I will comment on that, because I have been involved in the UN GGE, including working with the FCO on briefings prior to the GGE meetings of the last round, where these questions of what defines responsible state behaviour in cyberspace are raised and debated.

The fact is that states have agreed that international law applies in cyberspace, but, as you pointed out, they have been unable to agree how to apply it. There has been no consensus on what constitutes the use of force or an armed attack, in part because cyberspace does not have this physical dimension. We are working now on bringing together a working group that will look at those questions in the context of the internet of things, because it has that physical dimension and we feel that there is some capacity to move forward those very slow-moving discussions about cyber norms, as we call them.

There are other problems in addition to working out how international law might apply in cyberspace. There are also problems of ascertaining why actors would be motivated to adhere to international law—going back to this question of attribution and anonymity. It is not that actors would see less value in international law but that they may then be able to pursue other foreign policy goals while still appearing to adhere to international law. So it is both the application of the law—how to apply it—and what motivates actors to adhere to it if we can work out how to apply it.

As regards international organisations, it is difficult for the UN to move rapidly on that. We have just finished a study in which we looked at the activity taking place in other international organisations on emerging technology issues. Part of the idea behind the working group is to bring global cybersecurity policymakers into conversation with people from the technical community who are interested in and conversant with policy problems, with the international organisations—the World Economic Forum has emerged as an active organisation in this space—and with other academics who are working on understanding these problems in the future.

Again, in many of these forums we are talking about old, existing cybersecurity problems with no capacity to understand the future problems that are either imminent or in the near future. The UN is probably not agile enough to deal with those foresight problems. We will therefore look at some possible solutions to support the policy community to do that better.

Professor Philip Howard: I work at the Oxford Internet Institute, and we have had a little more success collaborating with NATO and the EU on these kinds of issues. The UN is of course a wonderful institution, but some of the processes involving media and information policy have been hijacked over the years, because they become moments where authoritarian regimes can use the same kinds of instruments to justify their choices internally. Regional groups of like-minded democracies may be another level of relationship that would be productive.

Q47 **Lord Hannay of Chiswick:** Can you comment on whether there is a useful distinction in this international discussion between what in the jargon is normally called soft law and hard law, given that the chances of the United Nations or anyone else being able to negotiate hard law in this area are very slight, and the chances of soft law, which is more like what we would call rules of the road, being a more useful way?

Secondly, to follow the professor's last intervention, I am sure it is easier to get a common approach with NATO, the European Union, or something like that, than with the United Nations, but is it at all useful when you are dealing with technologies that are global, not regional?

Dr Madeline Carr: I will comment quickly on the hard law versus soft law issue. Since 1998, Russia and later China have been calling for an international treaty, arguing that there is a need for some hard law and agreement on what is acceptable state behaviour in cyberspace. But that view has not been shared more widely. It is currently confined to the Shanghai Cooperation Organisation group of states.

The expectation or ambition is that by agreeing these cyber norms through the UN process, eventually they will become identifiable as customary law over time. However, part of the problem is that, again, this is where attribution poses another challenge. It is not clear, if we cannot conclusively attribute behaviour in cyberspace, when we would see these behaviours becoming evident as customary law. It is not clear

how we would ever recognise when these things develop into an approach to the extent that they could be understood as customary international law. Phil, you probably have some comments on that.

Professor Philip Howard: We have had the most success in understanding the problems and what is going on when we collaborate well with security agencies, other academics and investigative journalists. In an important way, this is an advantage that democracies have, because many of us working to make attribution are also interested in open attribution systems. So even if our security services can make determinations that they cannot share with the public, there are often things that we can assemble from qualitative, quantitative and computational research that let us point fingers, make some determinations, and contribute to a public conversation about who is attacking our democratic institutions and why.

Q48 **The Chairman:** I come finally to something that we have so far not discussed. Many people feel that this cyber world of information and disinformation is dominated by the giant global information companies, which transmit fake news, disrupting news, pornography, crime, terrorism, and so on.

As a result of that, these institutions are under attack by individual Governments and Governments working collectively, in a big way. Give us your take on that. Will this ever be controlled, or is this is the next big threat: the domination by these giant global systems of our entire information pattern?

Dr Madeline Carr: The general data protection regulation, for example, is a very exciting development and a step forward in protecting exactly the kinds of human rights that we have seen systematically abused over the past four decades by the information giants. While there are big questions about how the GDPR will be implemented and the kinds of problems that we will see arise from that, thinking much more critically and carefully about what rights we wish to protect in cyberspace, and how to do that, will be really important in decades to come. We are coming to accept that the idea that these things will be successfully managed by a market-led approach has not been the case and has not eventuated, and that it does require some government intervention.

Lord Reid of Cardowan: At the risk of keeping you here for another day and a half, where is all this going? We are just getting to grips—well, some of us are trying to get to grips—with revolutionary change. We are on the verge of artificial intelligence: quantum, which will change the whole game again, and combinations of some of these technologies. We all now know about drones; we did not five years ago. We know about facial recognition, which can be put in drones, thus allowing them to lock on and follow you. We know about the dissemination of viral warfare. If you combine them, you have a drone that can lock on to a target, follow it indefinitely, and target people with a virus.

I do not want to frighten us all to death, but as we are grappling with the

existing cyber problems, these are already being developed. Where do you see the biggest threats to and opportunities for international relations—global relations, I suppose—from the developments that are already occurring but which we have not caught up with yet?

Dr Andrea Calderaro: I will try to end this meeting on a positive note. You mentioned artificial intelligence. We have been discussing cybersecurity for the past hour. Let us say that artificial intelligence will be a great opportunity. So far, cybersecurity strategies—the ways in which we have used them to protect our critical infrastructure—have been a static approach, meaning that we have been interested in developing cyber-hygiene norms or firewalls.

But these are static strategies, and at the same time we have attackers who have a dynamic way of attacking our critical infrastructure. In other words, they adapt their attacks; they use their tools based on how our systems are designed. Artificial intelligence will give lots of opportunities to design a dynamic way of securing our critical infrastructure. It will allow us to react based on the kind of attack that will be made. To leave you with a positive note, artificial intelligence is a great opportunity.

Dr Madeline Carr: If we look at the big picture of where all this is going, we know from observing technological change that it has huge implications. When we think back even to the changes that the Industrial Revolution brought about, at that time we did not have the understanding that we do now of the implications that technology can have. Now we know that through this technological revolution, and it would be a real shame if we did not apply that knowledge to thinking through the problems that we are facing now.

One thing that we understand from digital technologies is that states that lead in developing technologies can to a certain extent set the agenda and the rules of engagement—the rules of the road, as Lord Hannay said. In the first generation of digital technologies, that was certainly the United States. To a large extent, the United States' values, norms and interests were embedded in the way digital technologies developed. That was good for the UK, because our interests were very closely aligned with those of the US.

In the next generation of digital technologies, it is most likely that that power will not be located so explicitly in the US but will be shared, specifically with China, which is leading in a number of fundamental technologies now. It is important for the UK to understand China's ambitions and intentions for the development of technology and for innovation, so that we understand how our national interests will fit into that. It needs to be developed in a way that maximises the opportunities that will be there but that mitigates the challenges.

Q49 **The Chairman:** That is an interesting note on which to end. I have just one reflection and a final question.

Democracies have favoured and prided themselves on free speech, free

exchange, free transmission, a free press and so on, and authoritarian countries have said, "No, we must try to close all this down—filter, curate, limit and restrict". Looking into the near future, could we see a convergence of views here such that both the free nations and the authoritarian nations are more interested in combining control of what appears to be uncontrollable at present in the way of information and knowledge and fake information and fake knowledge disturbing and undermining our societies? Would you allow me that final reflection, or is it ridiculous?

Professor Philip Howard: I will try. I agree with you that there are some new breeds of authoritarian regimes that take advantage of these technologies. We sometimes call them soft authoritarian regimes. These are countries in which there are elections but they are rigged through the media and information infrastructure by people who need only 60% of the popular vote instead of 90%.

There are several soft authoritarian regimes that I think we will see be stronger and more resilient than we might have expected in the past. I also agree that many of these technologies, such as the internet of things and AI, give us some opportunities to build new institutions. Some creative tool-building can allow civil society groups and universities to protect our democracies in creative ways.

The Chairman: This is a note on which we can end. We have moved into vast new areas, but the rather chilling thing is that they may be closer than we think. Everything is moving so fast. You have been very helpful to us and given us a lot to think about. I am most grateful to all three of you for attending this morning in this rather unpleasant weather. Thank you very much.